ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

ДОКТОР, ПРОФЕССОР Г.ЦОГБАДРАХЫН НЭРЭМЖИТ

“МЭДЭЭЛЭЛ, ХОЛБООНЫ САЛБАРЫН ХӨГЖИЛД БИДНИЙ ГҮЙЦЭТГЭХ ҮҮРЭГ”

2024-2025 ОНЫ ХИЧЭЭЛИЙН ЖИЛИЙН ХАВРЫН УЛИРЛЫН ЭРДЭМ ШИНЖИЛГЭЭНИЙ ХУРЛЫН ЭМХЭТГЭЛ

№25(06)353

УЛААНБААТАР ХОТ

2025 ОН

ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛИЙН

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

ДОКТОР, ПРОФЕССОР Г.ЦОГБАДРАХЫН НЭРЭМЖИТ “МЭДЭЭЛЭЛ, ХОЛБООНЫ САЛБАРЫН ХӨГЖИЛД БИДНИЙ ГҮЙЦЭТГЭХ ҮҮРЭГ-2025”

ЭРДЭМ ШИНЖИЛГЭЭНИЙ БҮТЭЭЛИЙН ЭМХЭТГЭЛ

№ 25(06)353

УЛААНБААТАР ХОТ
2025 ОН

ISSN 1560-8794

Бүтээлийн эмхэтгэл хянан магадалсан:

Эмхэтгэсэн: Н.Даваасүрэн
Хуудасны хэмжээ: А4
Бодит хэвлэлийн хуудас: 8.33 х.х
Үсгийн гарнитур: Times New Roman
Хэвлэсэн тоо: Онлайн
Улаанбаатар хот

MONGOLIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

SCIENTIFIC TRANSACTIONS

№25(06)353

ULAANBAATAR 2025

Өмнөх үг

Мэдээлэл, Холбооны Технологийн Сургуулийн 2024/2025 оны хичээлийн жилийн хаврын улирлын бакалавр, магистр, доктор оюутнуудын судалгаа шинжилгээний ажлын үр дүнг тусгасан эрдэм шинжилгээний өгүүллийг энэхүү эрдэм шинжилгээний бичигт эмхэтгэн гаргаж байна. 2024/2025 оны хичээлийн жилийн хаврын улирлын бакалавр, магистр, доктор оюутны хурлыг "Мэдээлэл Холбооны салбарын хөгжилд бидний гүйцэтгэх үүрэг-2025" сэдвийн хүрээнд зохион байгуулсан бөгөөд салбаруудын ЭШХ-д хэлэлцэгдсэн илтгэлээс шалгарсан бакалавр оюутны 14, магистр оюутны 14, доктор оюутны 2 илтгэлийг 2-р шатанд хэлэлцүүлж доктор (Ph.D), дэд профессор Х.Загарзүсэм, доктор (Ph.D) П.Ууганбаяр, доктор (Ph.D) Р.Баярмаа, доктор (Ph.D), дэд профессор Б.Долгорсүрэн, доктор (Ph.D), дэд профессор Б.Дорж, доктор (Ph.D) Д.Бямбадорж нар бакалавр оюутнуудын илтгэлийг сонсож Х.Загарзүсэм, доктор (Ph.D) П.Ууганбаяр, доктор (Ph.D), дэд профессор Я.Дашдорж, доктор (Ph.D), дэд профессор Б.Долгорсүрэн, доктор (Ph.D), дэд профессор Б.Дорж, доктор (Ph.D) Р.Баярмаа, доктор (Ph.D) Ж.Оргил нар магистр, доктор оюутны илтгэлүүдийг сонсож, тус бүр 3 байр шалгаруулав. Хурлын өгүүллийн редакцаар доктор (Ph.D) Х.Загарзүсэм, доктор (Ph.D), дэд профессор Ч.Мөнхнасан, доктор (Ph.D), дэд профессор И.Цэрэн-Онолт, доктор (Ph.D) , дэд профессор Д.Золзаяа, доктор (Ph.D), дэд профессор Д.Сарангэрэл, доктор (Ph.D) Л.Одончимэг, доктор (Ph.D) Б.Дорж, доктор (Ph.D), дэд профессор Ж.Жавзансүрэн, доктор (Ph.D), дэд профессор Б.Туяацэцэг нар ажиллан тунгаан дүгнэлт өгсний дагуу өгүүллүүдийг засварлан эмхэтгэв.

ДОКТОР ОЮУТНЫ АНГИЛАЛД:

I байр **"Resource allocation for D2D communications underlay 5G networks using reinforcement learning"**
Илтгэгч: Ө.Буянхишиг */Утасгүй холбоо мэргэжлийн докторант/*
Удирдагч: Доктор (Ph.D), профессор Б.Отгонбаяр */ХС-ын профессор/*

II байр **"Монгол улсад хиймэл дагуулын холбооны радио долгионы тархалтад үүлнээс үүсэх унтралтын нөлөөллийг ITU-r загварчлалаар үнэлэх нь"**
Илтгэгч: Ю.Отгонбаатар */ Утасгүй холбоо мэргэжлийн докторант/*
Удирдагч: Доктор (Ph.D), дэд профессор З.Буянхишиг */ХС-ын эрхлэгч/*

МАГИСТР ОЮУТНЫ АНГИЛАЛД:

I байр **"Context-free grammar for mongolian, some results"**
Илтгэгч: Jonathan Sande */ Программ хангамжийн инженерчлэлийн магистрант/*
Удирдагч: Доктор (Ph.D), дэд профессор Б.Туяацэцэг */КУС-ын ахлах багш/*

II байр **"Бараа материалын нөөц төлөвлөлтийн ухаалаг системийн хөгжүүлэлт"**
Илтгэгч: Ө.Азамат */ Программ хангамжийн инженерчлэлийн магистрант /*
Удирдагч: Доктор (Ph.D), дэд профессор Б.Туяацэцэг */КУС-ын ахлах багш/*

III байр **"Микроскопын дүрснээс enterobius vermicularis-ийн өндгийг гүн сургалт ашиглан илрүүлэх нь"**
Илтгэгч: Т.Түвшинсайхан */ Өгөгдлийн ухаан хөтөлбөрийн магистрант /*
Удирдагч: Доктор (Ph.D) Б.Долгорсүрэн */МТС-ын дэд профессор/*

БАКАЛАВР ОЮУТНЫ АНГИЛАЛД:

I байр **"Эмийн жор бичээч ухаалаг систем"**
Илтгэгч: Ү. Мөнхтуяа, Г.Магван - Эрдэнэ / Мэдээллийн систем хөтөлбөрийн III-р курс /
Удирдагч: Доктор (Ph.D) Б.Долгорсүрэн */МТС-ын дэд профессор/*

II байр **"Монгол хэл дээрх текстийг оновчтой хураангуйлах аргын судалгаа"**
Илтгэгч: Б.Амартүвшин, Н.Гантөмөр / Компьютерын ухаан хөтөлбөрийн 2-р курс /
Удирдагч: Доктор (Ph.D) Б.Золзаяа */МТС-ын дэд профессор/*

III байр **"Карго тээврийн бичгээс мэдээлэл гарган авах ухаалаг систем"**
Илтгэгч: М.Түмэн-Аюуш, Ч.Мичидгоо, С.Батмөнх /Мэдээллийн технологи хөтөлбөрийн 4-р курс/

Удирдагч: Доктор (Ph.D) С.Өлзийбаяр /МТС-ын ахлах багш/

III байр **“Аюултай ачаа тээврийн маршрутыг граф бүтэц ашиглан оновчлох нь”**

Илтгэгч: Х.Ариунзаяа /Мэдээллийн систем хөтөлбөрийн 4-р курс/

Удирдагч: Доктор (Ph.D) Б.Долгорсүрэн / МТС-ын дэд профессор/

Цаг заваа гарган мэргэн шүүсэн эрхэм багш нартаа болон өгүүллийн редакц хийсэн гишүүддээ хурал зохион байгуулагчдын зүгээс талархлаа илэрхийлье.

НОМЫН ЦАГААН БУЯН ДЭЛГЭРЭХ БОЛТУГАЙ

ГАРЧИГ

ДОКТОР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

МАГИСТР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

БАКАЛАВР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

RESOURCE ALLOCATION FOR D2D COMMUNICATIONS UNDERLAY 5G NETWORKS USING REINFORCEMENT LEARNING

Buyankhishig ULZIINYAM[1], Otgonbayar BATAA[1], Dae-ki Hong[2]

[1]*Department of Communications, School of Information and Communication Technology, MUST, Ulaanbaatar, Mongolia*

[2]*Department of System Semiconductor Engineering, Sangmyung University, Cheonan, Korea*

Email: buyankhishig.o@must.edu.mn[1], otgonbayar_b@must.edu.mn[1], hongdk@smu.ac.kr[2]

***Abstract*: Device-to-Device (D2D) technology is becoming increasingly significant for boosting spectral utilization in emerging wireless networks. With the exponential rise in interconnected devices, Fifth-Generation (5G) networks must provide greater data rates accompanied by extremely low latency. To achieve this objective, this study focuses on optimizing total throughput for cellular and D2D links simultaneously within a cell using resource allocation methods, where several D2D pairs concurrently access a single cellular channel. Thus, we introduce an efficient Q-learning-based channel allocation strategy for D2D communications operating alongside cellular networks. For developing the proposed Q-learning mechanism, an emulator was built to mimic the wireless network environment. The simulation results illustrate marked improvements in system throughput and energy efficiency (EE).**

Keywords: D2D, 5G, gNB, resource allocation, RL, throughput

I. INTRODUCTION

The advent of Fifth-Generation (5G) mobile networks has significantly enhanced network connectivity among multiple mobile devices by leveraging low uplink and downlink latency and higher bandwidth. In recent years, the number of connections and volume of multimedia content in mobile communications have expanded rapidly [1-2]. This massive connectivity has led to a substantial increase in network traffic at the gNodeB. Therefore, offloading traffic from the Base Station (BS) and improving the overall system performance have become essential. Device-to-Device (D2D) communication is a key approach for offloading network traffic and enhancing spectrum efficiency [3].

Various resource allocation methods have been analyzed and researched, particularly focusing on centralized channel assignment for D2D communication in 3G mobile networks. With the increasing number of interconnected devices, 5G networks require higher data rates with minimal latency [4]. However, implementing D2D communication within an underlay heterogeneous cellular network introduces two significant issues. The first is managing interference between cellular users and D2D pairs, which directly impacts overall system efficiency. The second is maintaining adequate Quality of Service (QoS) for both cellular and D2D users. Effective resource allocation is essential for improving D2D communication capabilities in upcoming 5G and 6G networks. Moreover, the sharp increase in the number of connected devices demands substantial spectral resources to accommodate diverse applications, adding considerable pressure on base stations [5].

Several studies have explored methods to improve spectrum efficiency, coverage, and traffic offloading [6], effectively alleviating wireless spectrum resource pressure and enhancing the capacity of heterogeneous networks. However, these solutions also introduce significant interference challenges [7]. To address these issues, this paper proposes a deep learning (DL)-based hybrid resource allocation framework for optimizing multi-channel D2D communication. Our proposed approach targets maximizing the aggregate data rate of D2D User Equipment (DUE), ensuring QoS by effectively controlling interference levels affecting cellular users [8].

Multiple research works have investigated resource allocation using reinforcement learning approaches in 5G mobile networks supporting D2D communication, aiming to increase overall capacity and reduce interference. Our approach integrates the Multi-Player Multi-Armed Bandit (MPMAB) model and a multi-agent reinforcement learning framework with Proximal Policy Optimization. This combined approach ensures efficient and fair resource distribution, preventing resource wastage and starvation. Additionally, staggered training improves learning efficiency, while decentralized execution enhances scalability and robustness. The proposed approach maximizes throughput and SINR performance while preserving low complexity in computation, particularly when dealing with a limited number of D2D user pairs. [9-10].

Multiple researchers have investigated resource allocation and interference mitigation techniques for D2D communications in heterogeneous cellular systems of 5G and beyond. A common approach involves using Deep Q-Networks (DQN) for reinforcement learning to optimize spectrum allocation and power control, maximizing throughput while ensuring QoS and improving spectrum efficiency. The proposed machine learning-based approach enhances interference

mitigation and outperforms existing solutions, as confirmed through simulations [11].

To address these challenges, this paper investigates maximizing total system throughput for both cellular and D2D connections in a single cell through resource allocation schemes, where cellular channels can be shared by multiple D2D links. We propose an efficient channel assignment method for D2D communications in 5G networks, based on the Q-learning algorithm. To train the Q-learning model, we develop an environment for spectrum sharing in a single-cell environment, where an evolved 5G Base station (gNB) coexists with multiple Cellular User Equipment (CUEs) and DUE pairs. Based on resource allocation strategies, we propose an iterative resource allocation approach utilizing Q-learning, which achieves superior efficiency compared to traditional optimization techniques. The Q-learning algorithm enables the system to dynamically learn and adapt to network environments by leveraging the advantages of an iterative model. The proposed resource allocation approach utilizing Q-learning assigns resources to D2D devices instantaneously, considering dynamically varying network conditions, including cellular users, D2D locations, and co-channel interference.

In this paper, we present a solution addressing interference management, while ensuring acceptable Quality of Service (QoS). For this purpose, we propose a resource allocation mechanism based on machine learning, targeting throughput maximization and compliance with minimum QoS requirements for active cellular and D2D users. Initially, we focus on formulating the spectrum allocation as a resource optimization problem. As this optimization is classified as an integer nonlinear programming task, we implement a Q-learning algorithm to enhance resource allocation efficiency within the described setting. The introduced Q-learning model is trained using a decision-making strategy, enabling optimal outcomes in terms of spectral efficiency, computational time, and overall throughput.

The paper is structured as follows: Section 2 provides an overview of relevant literature. Section 3 introduces the system model, the developed Q-learning-based channel assignment framework, and the agent's training method. Performance evaluation of the proposed D2D resource allocation strategy, including detailed simulation results demonstrating its efficiency, is presented in Section 4. Finally, conclusions are drawn in Section 5.

II. ANALYSIS OF THE RELATED WORKS

D2D communication, whether implemented with or without network infrastructure, enables the connection of more devices while enhancing data rates and reducing latency. D2D is regarded as a key technology for addressing the challenges of 5G wireless networks across various industries. The next generation of mobile communication—Beyond 5G (B5G) and 6G systems—is expected to be deployed between 2027 and 2030. These systems will integrate advancements such as massive Multiple-Input Multiple-Output (MIMO) and millimeter-Wave (mm Wave) technologies.

Even with these improvements, beyond 5G (B5G) still faces crucial issues requiring solutions, including the demand for greater capacity, faster data transmission, minimized latency, heightened security, and improved Quality of Service (QoS) relative to 5G. In this paper, we examine the potentials of future 6G wireless communication by focusing on critical network needs and difficulties, specifically in terms of millimeter-wave (mm Wave), terahertz-based communication, and massive MIMO system deployments.

Extensive research has been conducted on D2D technology within cellular networks, with numerous studies exploring and advancing D2D communication. Recently, deep learning (DL) and reinforcement Learning (RL) have attracted considerable interest from diverse research areas. DL has become extensively utilized for tasks like optimization, system modeling, recognition, and classification in a variety of applications, particularly within wireless and mobile communication domains. RL, on the other hand, is a learning paradigm in which agents determine optimal actions or strategies to maximize rewards through trial-and-error exploration.

Deep Reinforcement Learning (DRL) combines the strengths of DL and RL, enabling agents to make intelligent decisions from unstructured input data. In the context of D2D communication, RL-based resource allocation algorithms have been extensively studied. Table 1 summarizes key RL-based resource allocation algorithms applied to D2D communication.

TABLE 1. RESOURCE ALLOCATION ALGORITHMS IN D2D COMMUNICATION

№	Learning algorithm	References	System Model	Description
1	Joint DQN, Multiagent DQN	[12]	Node B, K CUE, M D2D	• A centralized multi-agent DRL based resource allocation method is introduced to minimize computational complexity • The RA approach aims at optimizing the accumulated average throughput for cellular and D2D users within a cell
2	SARSA-State-Action-Reward-State-Action algorithm	[13]	Node B, K CUE, M D2D	• Reinforcement learning based SARSA-State-Action-Reward-State-Action algorithm is used to improve overall system throughput • Distributed device centric RA method is to reduce the traffic burden on the base station and lower the overall system latency.

3	Distributed Multiagent DQN algorithm	[14]	Macro base station, small base station, K CUE, M D2D	• To solve the channel assignment and mode selection challenge, a distributed multi-agent Deep Q-Network (DQN) algorithm is introduced. • The optimization task focuses on maximizing overall system sum-rate under the constraints of maintaining the Quality of Service (QoS) for each user.
4	Game theory-based algorithm, DNN (Deep neural network) based method	[15]	M D2D	• A game-theoretic algorithm employing iterative channel assignment and power control is presented. • The proposed algorithm based on game theory addresses the problem of maximizing the total sum-rate of the system. • Additionally, two resource allocation methods utilizing Deep Neural Networks (DNN) for D2D networks are introduced.
5	Centralized and distributed DNN model	[16]	BS, 2 CUE, 2 D2D	• Channel selection and discrete transmit power levels
6	Multi-Player Multi-Armed Bandit (MPMAB) reinforcement learning scheme	[17]	Node B, K CUE, M D2D	• The issue can be modeled using a preference matrix to enable efficient greedy resource assignment. • A fair resource distribution scheme is implemented to maintain equity, minimize resource misuse, and prevent user starvation.
7	Double-deep Q-network (DDQN) algorithm	[18]	BS, K CUE, M D2D	• Our aim is to optimize the aggregate data rate for all D2D pairs within the system. • A joint optimization problem involving combined uplink–downlink subcarrier assignment and power allocation for D2D pairs is formulated.

III. THE PROPOSED RESOURCE ALLOCATION MODEL

A. *System Model*

Let us consider a single-cell scenario, where a gNB, multiple CUEs, and DUE pairs coexist. There are two types of users: CUEs and DUEs. Each DUE operates in pairs, consisting of a D2D Transmitting User Equipment (DTUE) and a D2D Receiving User Equipment (DRUE). All CUEs and DUEs are uniformly distributed within the cell.

When CUEs and DUEs share the same frequency resources, additional interference is introduced. In this study, we assume that each cellular user selects only one subchannel, while each D2D user reuses the same subchannel allocated to a cellular user.

To enhance D2D communication performance, we propose a method to increase overall system capacity. To ensure the QoS of User Equipment (UEs), the SINR must be maintained above a predefined SINR threshold.

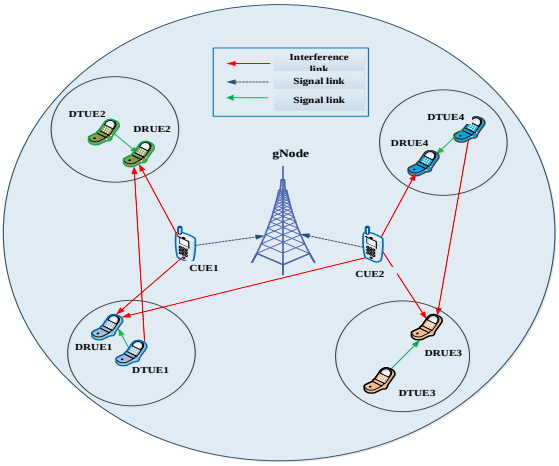


Fig 1. System model of D2D communications underlay 5G networks

Therefore, SINR of CUE I [19] for uplink period is determined by:

$$\beta_i = \frac{P_i / r_i^{\alpha}}{\sum_{k \in R_i} \left(\frac{P_T}{d_k^{\alpha}} \right) + N_0} \qquad (1)$$

where P_i denotes the CUE i's transmitting power, r_i^{α} is the distance from CUE i to the gNB, P_T denotes the DTUE k's transmitting power, d_k is the distance from DTUE k to the gNB, α is the path loss exponent, and N_o is the noise power.

Similarly, the SINR of DRUE j for the uplink period is given by:

$$\gamma_i = \frac{P_i / l_i^{\alpha}}{\left(P_m / d_{m,j}^{\alpha} \right) + \sum_{k \in R_m \, k \notin m} \left(\frac{P_T}{d_{k,j}^{\alpha}} \right) + N_0} \qquad (2)$$

where l_j^{α} is the distance from DTUE j to the DRUE j, $d_{m,j}^{\alpha}$ is the distance from CUE m to the DRUE j, $d_{k,j}^{\alpha}$ is the distance from DTUE k to the DRUE j, and R_m denotes the set of the equipment which share the mth subchannel.

The total capacity consists of two components: CUEs and DUE pairs. Therefore, the capacity function is expressed as:

$$C = B\sum_{i=1}^{N} log_2(1+\beta_i) + B\sum_{j=1}^{M} log_2(1+\gamma_j) \quad (3)$$

where B represents the one subchannel bandwidth.

The average transmission power of CUEs is determined by:

$$P_{average} = \frac{\sum_{i=1}^{N}\left(\sum_{k\in\mathcal{R}_i}\left(\frac{P_T}{d_k^{\alpha}}\right)+N_0\right)\cdot\tau\cdot r_i^{\alpha}}{N} \quad (4)$$

where τ denotes the SINR threshold.

Finally, the Energy Efficiency (EE) is given by:

$$EE = \frac{C(U_x)}{\sum_{i=1}^{N}P_i + \sum_{j=1}^{M}P_T} \quad (5)$$

B. Architecture of Q learning based channel allocation

Recent research has focused on developing an efficient channel allocation method for 5G gNB and D2D communications in licensed bands, utilizing Q-Networks. The primary objective of RL in this context is to enhance the agent's decision-making capability in resource allocation, ultimately improving user throughput and optimizing resource utilization in 5G networks. To achieve this, we propose a complex training environment that incorporates a deployed gNB, CUEs, and DUE pairs. Within this environment, we assume that the gNB operates under conditions where CUEs and DUEs are not densely deployed. The agent is responsible for centrally managing resource allocation for both DUEs and CUEs, using the current state of the environment as a basis for decision-making.

The state of the environment evolves dynamically and is affected by multiple factors, including the locations of users, the distance from CUE i to the gNB, the distance from DTUE k to the gNB, the distance from DTUE j to the DRUE j, the distance from CUE m to the DRUE j, and the channel state during each episode. Additionally, the agent's parameters are updated continuously throughout all episodes, allowing it to learn and refine its ability to select optimal actions based on the observed state at each time step.

Given the dynamic nature of the environment, achieving optimal channel allocation for the gNB, CUEs, and DUEs presents a significant challenge. In order to resolve this, we propose a Q-learning algorithm for channel assignment, designed to enhance user throughput compared to traditional methods [12]. Optimal channel allocation plays a crucial role in maximizing user capacity by reducing interference and improving overall throughput. In our approach, the Q-network agent is trained to learn all possible channel assignment patterns corresponding to various observed states in the environment. Once trained, the agent can effectively determine and implement efficient channel allocation strategies within the system.

To formulate the channel allocation problem, we apply the Q-learning algorithm within the Markov Decision Process (MDP) framework [13]. The primary goal of MDP is to define a policy that enables the agent to maximize the rewards obtained from interactions with the environment. In this context, the channel allocation problem, as illustrated in Fig. 2, is modeled as an MDP consisting of a state space S, an action space A, a transition probability p (St+1|St, At), and a reward function Rt (St, At). The agent functions as the decision-maker, utilizing an action-value function to estimate the expected return associated with executing action At in the state St.

Fig 2. Agent-environment interactions

In our research, the agent determines channel allocations to maximize system capacity by appropriately assigning channels to the gNB, CUEs, and DUEs. By associating the impact of its actions within specific environmental states with the executed actions, the agent aims to maximize a numerical reward. This relationship, defined by policy rules, governs the behavior of the learning agent [14]. Within this environment, a variable number of CUEs and DUEs connect to the gNB at different locations in each episode. To facilitate the training process, we developed a Python-based simulator for resource allocation in 5G networks supporting D2D communication, which serves as the agent's testbed. During the training of the Q-network agent, the simulator computes the average throughput to derive rewards, thereby providing the agent with essential feedback for learning.

As a result, throughout the model training process, the agent gradually learns to identify optimal channel assignment patterns for every possible state of the environment. The state information, as detailed in Table 2, is extracted from the developed simulator and serves as input data for training the Q-network agent. In this scenario, the state space is discrete and defined by four key elements: the number of CUEs connected to the gNB, their respective locations, the number of CUEs associated

with D2D pairs, and their locations along with the states of the assigned channels.

TABLE 2. STATE INFORMATION (INPUT DATA) OF THE Q-NETWORK

CUE location	DUE pair location	Number of CUEs	Number of DUEs	Assigned channel
463.313, 280.425	98.376, 277.133; 93.351, 271.698	25	10	9
-384.687, -422.017	278.758, 345.211; 297.702, 349.051	18	16	23
174.891, 122.987	-517.590, -300.967; -520.364, -293.375	7	22	5
564.123, -389.836	508.678, -297.667; 525.360, -292.687	19	38	18
-222.516, 85.197	62.432, -229.875; 76.561, -219.994	20	26	8
599.825, 189.416	572.069, -148.828; 577.647, -160.043	2	18	3
589.369, 187.178	-327.685, -487.034; -333.186, -502.26	11	8	19

C. Training Q-learning Agent

A single-agent Q-learning-driven RL method is introduced to tackle the challenge of efficient channel allocation within the network.

a) Environment Setup

States: Represent the current status of channels. The state may include whether a channel is available or occupied, interference levels, and signal quality.

Actions: The action space is composed of discrete elements and described as the set of available channels, where $A_t \in A = \{0,1,2\}$.

In this approach, optimal channel allocation patterns are determined using the epsilon-greedy algorithm, where ε=1 represents random actions, and ε=0 corresponds to greedy actions. This method is applied to the gNB, CUEs, and DUEs in the environment. Consequently, the optimal policy is derived by choosing the action with the highest value in every episode, based on optimal values such as maximum capacity or throughput. The proposed channel allocation method using Q-learning is composed of two main components: the environment and the Q-Network agent. These components interact by exchanging state, action, and reward information to train the desired model, as illustrated in Fig. 2.

The input of the proposed model is the observed state from the environment, denoted as S_t, as presented in Table 1. The training dataset was generated using our developed simulator.

This dataset includes the locations of CUEs and D2D pairs, maximum capacity for the gNB, CUEs, and DUEs, user throughput, assigned channels, user location information, and overall system capacity. During every time step, the agent forms its state based on the gathered data from the simulated environment. It then applies the epsilon-greedy method to select an action for the gNB, CUEs, and DUEs in the given episode.

Based on the selected action and its impact on the environment, a reward function R_{t+1}(St, A) is calculated. The higher the reward, the greater the probability that this action will be selected in subsequent iterations [15]. The output of the Q-Network is the expected action for channel allocation corresponding to each given state.

Agent: The decision-making agent chooses actions according to a policy obtained from its Q-table.

Reward: In this research, the reward function is designed to optimize channel assignment within the assumed environment. A discrete reward function is employed, providing a real-valued reward equivalent to the average throughput, which is obtained from the environment acting as an emulator.

The process of channel allocation involves transitioning from a given state St to a new state St+1, with a transition probability defined as:

$$p(S_{t+1}, R_t | S_t, A_t) = P_r\{S_t = S_{t+1}, R_t = R_{t+1} | S_{t-1} = S_t, A_{t-1} = A_t\} \quad (6)$$

Every episode ends with a channel allocation step, followed by resetting the average throughput, which is utilized in reward calculation, for the next trial.

Due to variations in user locations and channel states, the agent's target shifts throughout the trial as it refines its strategy based on previously learned objectives. These targets are learned by the Q-Network agent as it simulates actions, interacts with the environment, and collects corresponding rewards. Therefore, the agent's ability to adaptively explore new targets is crucial for assigning optimal channels to each CUE and DUE pair. As a result, the trained agent efficiently assigns channels depend on the total number of users and their location data, improving overall network performance.

Consequently, the trained agent effectively allocates channels by considering user count and location data, leading to enhanced network performance.

b) The Channel Allocation Procedure Based on Q Networks

Initially, during the first episodes, the channel state (assigned channel) information for the gNB, CUEs, and DUE pairs is set to zero. It is important to note that only

one channel state for the gNB, CUEs, and DUE pairs is updated in each episode. In other words, the state data in the modeled environment determines the transition probability p ($S_{t+1}|S_t,\ A_t$), mapping each state in S to the likelihood of taking specific actions in A within the MDP framework.

Consequently, the number of users connected to the gNB, their location information, and the assigned channels are treated as random variables in this environment.

The number of time steps per episode is set to 1000, depending on the deployment of gNBs, CUEs, and DUEs in the defined area. The action A is selected using the epsilon-greedy strategy during each episode. The selected channels (actions) are subsequently passed to the simulator.

In the simulation environment, the reward for the chosen actions in the present state of an episode is computed. This reward R_t and the next state S_{t+1} information is then transferred to the Q-Network agent. The differences between S_t and S_{t+1} by the number of users, their location area information, and the channel state at each time step. This flowchart represents an implementation of Q-learning in Fig. 3.

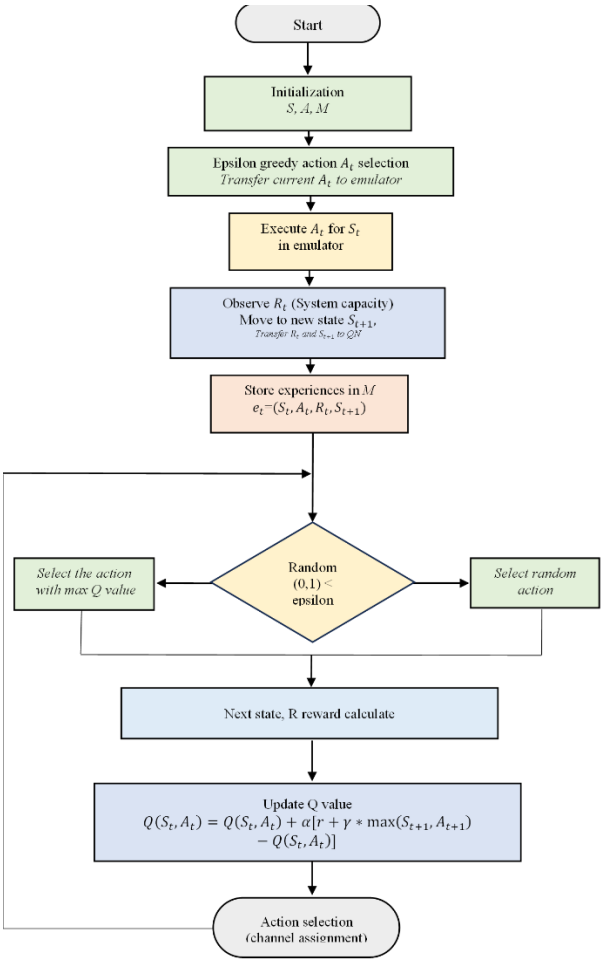


Fig 3. Channel assignment flowchart based on Q-learning

The learning process of each agent across several time steps and episodes is outlined below and visually summarized in Fig. 4.

Q-learning Algorithm
Initialization:
Initialize experience replay memory M, state S_t, action A_t, reward R_t at time step t and Q value

for all training steps **do**
Initialize and preprocess: state S_1 for the new episodes at time step 1000
repeat
Select action according to Epsilon Greedy Strategy: random action when ε =1 and greedy action with ε=0.01,
$A_t = \text{argmax}_A (Q (S_t, A, R))$
Execute action A_t in a state S_t in emulator
then move to a new state S_{t+1}, observe R,
Transfer R_t and $s_{t+1}$to QN
Store experience: e_t= (S_t, A_t, R_t,S_{t+1}) in M
Sample mini batch of N transitions e_k from M
Update the Q-values as:
$Q(S_t, A_t) = Q(S_t, A_t) + \alpha[r + \gamma * \max(S_{t+1}, A_{t+1}) - Q(S_t, A_t)]$
until episode terminates (reach a certain number of iterations or when all Q-values have converged)
end for

Fig 4. Algorithm of Q-Network for channel allocation

IV. PERFORMANCE EVALUATION

Channel allocation is a critical task in wireless communication systems, involving the assignment of frequency channels, time slots, or codes to different users or devices to optimize network performance. Advanced channel allocation algorithms aim to maximize system capacity, minimize interference, and ensure fairness among users.

To address these challenges, we have utilized the following parameters for the simulation system environment (Table 3) and the parameters used in the Q-learning algorithm (Table 4) in our research.

Table 3. Simulation parameters for D2D communications underlay cellular networks

Simulation Parameters	Value
Cell radius, *R*	600m
Distance D2D pair transmitter and receiver, *L*	20m
Path loss factor, α	4
SINR threshold, β	4.6 db
Noise, *No*	-90 dbm
The number of DUE pairs	8
The number of CUEs	3
The maximum transmission power of CUEs	2 W
The transmission power of DTUEs	0.01 W
The bandwidth of the subchannel *B*	0.15 MHz

Table 4. Hyperparameters for Q learning

Simulation Parameters	Value
Learning rate,	0.1
Discount factor	0.6
Exploration rate	0.01
Number of episodes, *E*	1000
Experience replay memory	2000

To maximize system capacity, we implemented the proposed Q-learning algorithm, which allocated optimal channels for 5G networks. Fig. 4 illustrates the total capacity performance of the trained Q-Network model, where the x-axis represents the number of steps and the y-axis denotes the maximum capacity. Once the maximum reward stabilizes, it indicates that the agent has successfully learned the environment and is capable

of selecting optimal actions (i.e., channel allocation) in any given state. At each step, the algorithm used Q-tables from previous steps to calculate the optimal channel allocation based on maximum capacity. The results, as shown in Fig. 5, illustrate the optimal outcomes of the simulation.

At 200 steps, the maximum capacity in the given environment was 31.5. As the steps increased to 600, the capacity rose to 32.0, reaching its maximum value at 700 steps. From 700 to 1000 steps, the capacity stabilized at 32.4, confirming 32.4 as the optimal capacity in this environment.

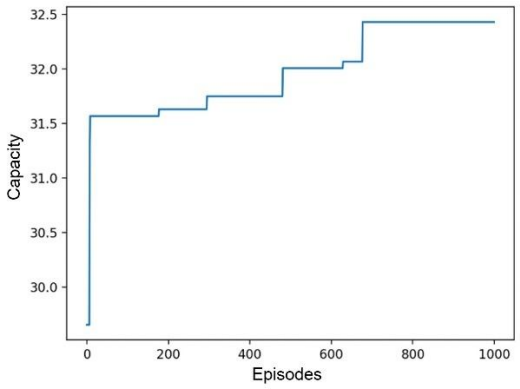


Fig 5. System capacity performance of the resulting Q-Network model

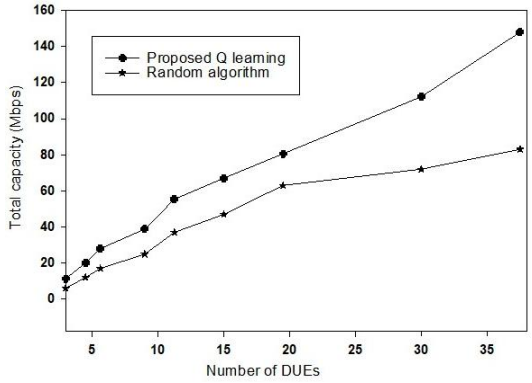


Fig 6. The Analyzed performance of the total capacity when DUEs and CUEs numbers ratio is 1.5

The results presented in Fig. 6 clearly indicate that the proposed Q-learning algorithm achieves significantly higher total capacity compared to the random algorithm across different numbers of DUEs:

• When the number of DUEs is 5, the total capacity using Q-learning is approximately 15 Mbps, whereas the random algorithm achieves only 8 Mbps.

• As the number of DUEs increases to 10, Q-learning reaches around 40 Mbps, while the random algorithm remains lower at 30 Mbps.

• At 20 DUEs, the proposed Q-learning method achieves about 80 Mbps, whereas the random algorithm only reaches 60 Mbps, showing a 33% performance improvement.

• For 35 DUEs, the gap becomes even larger, with Q-learning achieving over 140 Mbps, whereas the random algorithm stagnates at approximately 90 Mbps, demonstrating a more than 50% improvement in total capacity.

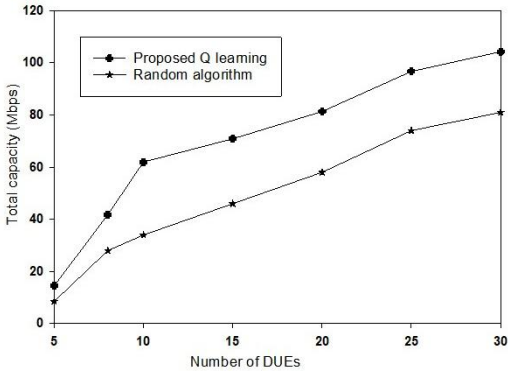


Fig 7. The Analyzed performance of the total capacity when DUEs and CUEs numbers ratio is 2.5

Fig. 7 compares the total capacity (Mbps) achieved by the proposed Q-learning algorithm and the random algorithm as the number of DUEs increases. The results clearly show that the Q-learning method consistently outperforms the random approach in all cases:

- When the number of DUEs is 5, Q-learning achieves about 12 Mbps, whereas the random algorithm reaches only 5 Mbps.
- At 10 DUEs, the total capacity with Q-learning rises sharply to 60 Mbps, while the random algorithm only achieves 35 Mbps, indicating a 71% improvement.
- When 15 DUEs are considered, the Q-learning method reaches 75 Mbps, whereas the random algorithm stays at 50 Mbps, showing a clear advantage.
- For 20 DUEs, Q-learning achieves 85 Mbps, while the random algorithm reaches 65 Mbps, highlighting a 30% higher performance.
- When 25 DUEs are present, Q-learning results in 100 Mbps, whereas the random algorithm remains lower at 80 Mbps.
- Finally, at 30 DUEs, the proposed Q-learning approach reaches 110 Mbps, while the random algorithm stagnates at 90 Mbps, demonstrating an approximately 22% improvement in total capacity.

The simulation results confirm that the Q-learning algorithm consistently outperforms the random algorithm in all tested scenarios. The performance gains are particularly pronounced at higher numbers of DUEs, indicating that Q-learning effectively adapts to increasing network demands. By dynamically optimizing resource allocation, the proposed approach significantly enhances system performance, making it a promising solution for future wireless communication networks.

CONCLUSION

In this paper, we presented an overview of the challenges associated with D2D networks and discussed methods for solving the optimal resource allocation problem with minimal mutual interference under given power constraints, addressing the demands of future 5G and B5G communication networks. We conducted a survey of existing techniques related to key aspects of D2D communication, including interference management and resource allocation. Additionally, we explored the use of RL to enhance resource allocation in D2D networks.

To address these challenges, we proposed a Q-learning algorithm for resource allocation, aimed at enhancing system capacity in D2D-enabled 5G networks. The developed DRL algorithm employs a single-agent decision-making policy to obtain an optimal solution concerning computational efficiency, spectral usage, and overall throughput. System performance was assessed using a Python-based simulator, and the outcomes confirmed that the proposed Q-learning method surpasses conventional techniques by delivering greater total capacity for both CUEs and DUE pairs. In addition, the approach improves system performance while adhering to the minimum QoS standards required by all users. These findings offer contributions to advancing 5G and B5G systems and provide useful direction for applying Q-learning-based resource allocation to ensure reliable throughput and QoS.

The simulation results demonstrate that the proposed Q-learning algorithm achieves significantly higher total capacity compared to a random allocation algorithm as the number of DUEs increases. In Fig.5, the Q-learning algorithm reaches a capacity of approximately 140 Mbps with 35 DUEs, while the random algorithm achieves only 80 Mbps when the DUE-to-CUE ratio is 1.5. Similarly, in Fig. 6, for up to 30 DUEs, the Q-learning algorithm attains around 100 Mbps, whereas the random algorithm remains below 80 Mbps when the DUE-to-CUE ratio is 2.5. These results confirm that the Q-learning algorithm effectively adapts to an increasing number of devices, demonstrating its ability to optimize resource allocation and improve system performance in wireless networks.

ACKNOWLEDGEMENT

This research was supported by “Capacity Building Project for School of Information and Communication Technology at Mongolian University of Science and Technology in Mongolia” (Contract No. P2019-00124) funded by KOICA (Korea International Cooperation Agency).

REFERENCES

[1] Rafay Iqbal Ansari, Syed Ali Hassan, Jonathan Rodriguez and Joel J. P. C. Rodrigues, “5G D2D Networks: Techniques, Challenges, and Future Prospects,” pp.1937-9234, 2017 IEEE, http://doi.org/doi:10.1109/JSYST.2017.2773633.

[2] Xiaohu Ge, Yuanwei Liu, Minghua Chen and Lajos Hanzo, “A Survey on Resource Allocation for 5G Heterogeneous Networks: Current Research, Future Trends and Challenges,” pp.1553-877, IEEE Communications Surveys & Tutorials, vol.23, pp.668–695, 2021, http://doi.org/doi: 10.1109/COMST.2021.3059896.

[3] Bin Zhong, HeHong Lin, Liang Chen and Zhongshan Zhang, “Performance Improvements for Device to Device Users in Underlay Cellular Communication Networks ”, KSII Transactions on Internet and Information Systems, vol.18, No.9, Sep 2024, http://doi.org/10.3837/tiis.2024.09.017.

[4] Tejal Rathod, Sudeep Tanwar, “AI-based resource allocation techniques in D2D communication: Open issues and future directions,” ELSEVIER, Physical Communication, vol.66, October 2024, http://doi.org/doi:10.1016/j.phycom.2024.102423.

[5] Steffi Jayakumar, Nandakumar S, “A review on resource allocation techniques in D2D communication for 5G and B5G technology,” Peer-to-Peer Networking and Applications 2021, pp.14:243–269, http://doi.org/doi:10.1007/s12083-020-00962-x.

[6] Ibrahim Attar, Nor Muzlifah Mahyuddi, “Joint mode selection and resource allocation for underlaying D2D communications: matching theory,” Telecommunication Systems 87(3), pp.663-678, August 2024, http://doi.org/doi:10.1007/s11235-024-01206-6.

[7] Jianli Xie, Lin Li, Cuiran Li, “A joint resource optimization allocation algorithm for NOMA-D2D communication,” IET communications, February 2024, http://doi.org/doi:10.1049/cmu2.12741.

[8] Shaik Ahmed Pasha, Vnoor Mohammed, “A modified LSTM with QoS aware hybrid AVO algorithm to enhance resource allocation in D2D communication,” EURASIP Journal on Wireless Communications and Networking 2024(1), March 2024, http://doi.org/doi:10.1186/s13638-024-02339-7.

[9] Fang-Chang Kuo, Hwang-cheng Wang, Chih-Cheng Tseng, “D2D Resource Allocation based on Reinforcement Learning and QoS,” Mobile Networks and Applications, http://doi.org/doi: 10.1007/s11036-023-02145-3.

[10] Kwame Opuni-Boachie Obour Adyekun, Alex Yaw Boakye, “Resource Allocation in D2D-Enabled 5G Networks using Multiagent Reinforcement Learning,” Journal of Computer Networks and Communications, June 2024, http://doi.org/doi: 10.1155/2024/2780845.

[11] Md Kamruzzaman, Nurul Sarkar, Jairo Gutierrez, “Machine Learning-Based Resource Allocation Algorithm to Mitigate Interference in D2D-Enabled Cellular Networks,” November 2024, http://doi.org/doi: 10.3390/fi16110408.

[12] Seoyoung Yu and Jeong Woo Lee, “Deep Reinforcement Learning Based Resource Allocation for D2D Communications Underlay Cellular Networks,” Sensors 2022, special issue Deep Reinforcement Learning in Communication Systems and Networks, December 2022, https://doi.org/10.3390/s22239459.

[13] Steffi Jayakumar, S. Nandakumar, “Reinforcement learning based distributed resource allocation technique in device to device (D2D) communication,” Wireless Networks, vol. 29, pp.1843–1858, February 2023, https://doi.org/10.1007/s11276-023-03230-x.

[14] Yuan Zhi, Jie Tian, Xiaofang Deng, Jingping Qiao and Dianjie Lu, “Deep Reinforcement Learning Based Resource Allocation for D2D Communications in heterogeneous cellular networks,” Digital Communications and Networks, vol.8, Issue.5, pp.834–842, October 2022, https://doi.org/10.1016/j.dcan.2021.09.013.

[15] Zhe Zheng, Yingying Chi , Guangyao Ding and Guanding Yu, “Deep-Learning-Based Resource Allocation for Time-Sensitive Device-to-Device Networks,” Sensors 2022, Trustworthy Sensing with Human-and-Environment-in-the-Loopun, February 2022, https://doi.org/10.3390/s22041551.

[16] Woongsup Lee and Robert Schober, “Deep Learning-based Resource Allocation For Device-to-Device Communication,” IEEE Transactions on Wireless Communications, vol. 21, pp.5235-5250, July 2022, http://doi.org/doi:10.1109/TWC.2021.3138733.

[17] Fang-Chang Kuo, Hwang-Cheng Wang, Chih Cheng Tseng, Jung-Shyr Wu, Jia-Hao Xu and Jieh-Ren Chang, “D2D Resource

Allocation Based on Reinforcement Learning and QoS," Mobile Networks and Applications, vol. 28, pp.1076–1095, July 2023, http://doi.org/doi: 10.1007/s11036-023-02145-3.

[18] Caihong Kai, Xiaowei Meng, Linsheng Mei and Wei Huang, "Multi-agent reinforcement learning based joint uplink–downlink subcarrier assignment and power allocation for D2D underlay networks," Wireless Networks, vol. 29, pp.891–907, November 2022, http://doi.org/doi: 10.1007/s11276-022-03176-6.

[19] Xujie Li, Lingjie Zhou, Xing Chen, Ailin Qi, Chenming Li and Yanli Xu, "Resource Allocation Schemes Based on Intelligent Optimization Algorithms for D2D Communications Underlaying Cellular Networks," Hindawi: Mobile Information Systems, vol.2018, pp.10, December 2018, https://doi.org/10.1155/2018/7852407.

МОНГОЛ УЛСАД ХИЙМЭЛ ДАГУУЛЫН ХОЛБООНЫ РАДИО ДОЛГИОНЫ ТАРХАЛТАД ҮҮЛНЭЭС ҮҮСЭХ УНТРАЛТЫН НӨЛӨӨЛЛИЙГ ITU-R ЗАГВАРЧЛАЛААР ҮНЭЛЭХ НЬ

Ю. ОТГОНБААТАР[1,2] , З. БУЯНХИШИГ[2], Ш.ГАНБОЛД[2]

[1] Монгол улс, Улаанбаатар, Хүрээ МХТДС, Мэдээллийн технологи, харилцаа холбооны тэнхим

[2] Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Холбооны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: otgonbaatar@huree.edu.mn[1], zbuya@must.edu.mn[2], sh_ganbold@must.edu.mn[2]

***Хураангуй*: Дэлхийн улс орнууд эрэлт хэрэгцээндээ тулгуурлан төрөл бүрийн хиймэл дагуулыг сансрын уудамд хөөргөж, харилцаа холбооны систем болон нийгмийн бүхий л салбартаа өргөн хүрээнд ашиглаж байна. Хиймэл дагуулын холбоо нь улс орнуудын үндэсний аюулгүй байдал, нийгэм, эдийн засгийн хөгжилд стратегийн өндөр ач холбогдолтой. Монгол улс ч мөн адил улс орны онцлог, төрөл бүрийн салбарын хэрэглээндээ тулгуурлан 2030 онд өөрийн орны үндэсний хиймэл дагуулыг хөөргөж, ашиглах чиглэлээр улсын их хурал, засгийн газар, мэдээллийн технологи, харилцаа холбооны салбар хамтран үндэсний хэмжээний цогц бодлогын баримт бичгийг боловсруулан баталж, үе шаттай хэрэгжүүлж эхлээд байна. Олон Улсын Цахилгаан Холбооны Байгууллагаас манай улсад сансрын "Geostationary" буюу Гео тогтонги байрлалд сансрын холбооны суурин үйлчилгээнд 113.6 Е зүүн уртрагийн байрлалд, өргөн нэвтрүүлгийн үйлчилгээнд 74 Е байршлыг тус тус хуваарилсан байдаг.**

Энэхүү судалгааны ажлаар Монгол орны нутаг дэвсгэрт байрших сансрын холбооны газрын станцын нэвтрүүлэх, хүлээн авах антены чиглэх өнцөг, хиймэл дагуул газрын станц хоорондоо долгион тархах зай, түүнд нөлөөлөх атмосферийн давхаргын үүлний массын нөлөөгөөр үүсэх дохионы унтралтыг бүс бүрээс төлөөлөх нийслэл, аймгийг сонгон авч, нэвтрүүлэх, хүлээн авах станц бүрийн хувьд тооцоолон, харьцуулсан дүн шинжилгээ хийж, үр дүнг гаргахыг зорилоо.

Түлхүүр үгс: Геометр хэмжигдэхүүн, радиозонд станцын өгөгдөл

I. УДИРТГАЛ

Дэлхийн агаар мандалд тухайн эгшинд $1.4*10^{16}$ кг буюу 10 их наяд илүү тонн усны молекул буюу устөрөгчийн исэл оршин байдаг. Үүнээс хэсэгхэн эзлэхүүнийг сонгон авч судлахад түүний найрлагад 78.08% хувь нь азот-(N_2), 20.95% хувь нь хүчил төрөгч-(O_2), 0.93% хувь нь аргон (Ar), үлдэх хувь нь бусад олон янзын хийнүүд байх бөгөөд эдгээрээс хамгийн их агууламжтай нь нүүрстөрөгчийн давхар исэл (CO_2) байдаг. Агаар мандлын устөрөгчийн ислийн гол онцлог нь ердийн даралт, температурын нөхцөлд 3 төрлийн цогц төлөвт оршин байдаг ганц бодис юм. Энэ нь хийн төлөв байдлыг нь уур, шингэн төлөвийг нь ус, хатуу төлөвийг нь цас, мөс гэж нэрлэнэ.

Үүл манан бол жижигхэн усан тусал, мөсөн талстуудын агаар дахь их хэмжээний бөөгнөрөл юм. Өөрөөр хэлбэл газрын гадаргаас дээш тодорхой өндөрт хуримтлагдсан усан дусал, хэт хөрсөн тусал, хатуу биет мөсөн талстын бөөгнөрлийн нэгдэл юм.

Газрын гадарга орчмын агаарт манан үүсэх бөгөөд энэ нь газар тогтсон үүл юм. Үүл манан хоёрын хооронд мэдэгдэхүйц ялгаа байхгүй бөгөөд эдгээр нь зөвхөн орших өндрөөрөө ялгардаг. 1940 онд гаргасан олон улсын атласт зөвшөөрөгдсөнөөр оорчих мандлын үүлсийг дотоод бүтэц, өндрийн хэмжээ, гадаад хэлбэр дүрсээс нь хамааараад 10 ангилалд авч үздэг ба хэвтээ чиглэлийн хөгжлийн гаралтай буюу давхраат хэлбэрийн 8 төрлийн үүлс, босоо хөгжлийн гаралтай буюу бөөн хэлбэрийн 2 төрлийн үүлс багтдаг байна.

Хэвтээ чиглэлийн давхраат хэлбэрийн үүлс нь ихээхэн том талбай эзэлдэг бөгөөд (10-1000 км)-ийн хэмжээний нутаг дэвсгэр хамарсан, хэдэн зуун метрийн зузаантай үүлс байдаг. Энэ хэлбэрийн үүлс тогтвортой оршин тогтнодог, үндсэндээ бүтэн хоногоор хадгалагддаг. Хэвтээ чиглэлийн үүлсийг өндрийн түвшингээс хамаарч доод, дунд, дээд мандлын үүлс гэж 3 ангилна.

ҮҮЛНИЙ ТӨРӨЛ

1-Р ХҮСНЭГТ

Физик үзүүлэлт	Доод мандал	Дунд мандал	Дээд мандал
Суурийн өндөр	0.4-1 км хүртэл	2-5 км	6-10 км
Усны агууламж	0.5-6 г/м^3	0.1-0.3 г/м^3	0.001-0.05 г/м^3

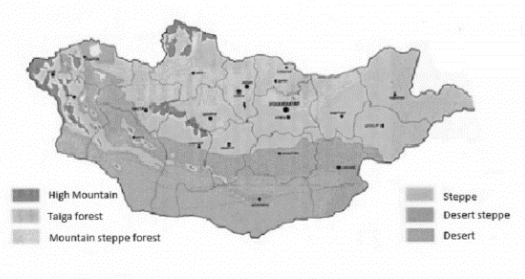
Доод мандлын үүл ихэнхдээ усан дусал, дээд мандлын үүл бүхэлдээ мөсөн талстаас, дунд мандлын үүлс усан дусал, мөсөн талстын холимгоос тогтно.

Босоо чиглэлийн үүлс нь хэвтээ чиглэлд хамрах талбайн хэмжээ багатай байдаг. (хэдхэн км-ээс хэдэн

арван км) боловч босоо чиглэлд зузаан нь 10 км, заримдаа бүр давхраат мандалд хүрсэн байдаг.

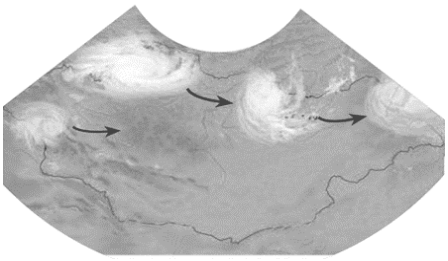
II. МОНГОЛ ОРНЫ УУР АМЬСГАЛ БА ҮҮЛШИЛТ

Монгол орны уур амьсгал дэлхийн бусад улс орнуудтай харьцуулахад нэлээд ялгаатай байдаг. Монгол улс дэлхийн бөмбөрцгийн хойд хагас, эх газрын хүйтэн сэрүүн бүсэд оршдог бөгөөд далай тэнгисээс алслагдсан байрлалтай тул эх газрын эрс тэс, хатуу ширүүн уур амьсгалтай. Жилийн ихэнх хугацаанд хасах хэмтэй өдрүүд давамгайлдаг. Улирлын хувьд эрс ялгаатай дөрвөн улиралтай бөгөөд зун, намар, өвөл, хаврын улирлууд ээлжилдэг онцлогтой. Газарзүйн тогтцын хувьд манай орон **Алтай, Хангай, Хөвсгөл, Хэнтийн** уулсын нурууд болон Их нууруудын хотгор зэрэг томоохон уулс, хотгор гүдгэр бүхий бүс нутагт байрладаг онцлогтой. Монгол орны газарзүйн бүтцийн ерөнхий байршлыг 1-р зурагт үзүүлсэн болно.



1-р зураг. Монгол орны газарзүйн бүтэц

Монгол орны өвлийн улирал нь нэлээн хүйтэн ширүүн уур амьсгалтай. Энэ улиралд агаар мандлын үйл явц, салхины урсгал гол төлөв баруун, хойд, баруун хойноос орж ирдэг. Хэрэв салхи хойд талаасаа урсгалтай байвал хойд мөсөн далай болон Сибирийн хүйтэн эх газрын нөлөөгөөр туйлын хүйтэн агаар Монгол орны нутаг дэвсгэрийн бүхэлд нь бүрхдэг..



2-р зураг. Монгол орны агаарын урсгалын ерөнхий чиглэл.

2-р зурагт монгол орны агаарын урсгалыг ерөнхий чиглэлийг харуулав. Дэлхийн агаар мандлын доод давхаргад халсан агаарын нягт сийрэгжиж дээш хөөрөх бөгөөд дээшлэх тутам температур нь буурах ерөнхий зүй тогтолтой. Гэвч монгол орны хувьд хойноос болон баруун хойноос орж ирж байгаа хүйтэн агаарын урсгал нь хэдэн мянган диаметр бүхий **хүйтэн агаарын тогтцыг** үүсгэдэг. Энэ нь хүйтний улиралд **температурын урвуу үзэгдэл инверсийг** үүсгэдэг. Хаврын улирлын нэг онцлог нь шороон шуурга ихээр тохиолддог явдал юм. Үүний гол шалтгаан нь өвлийн улиралд тогтсон томоохон хүйтэн агаарын тогтоц гуравдугаар сараас эхлэн задарч, сарнихтай холбоотойгоор шороон шуурга үүсэх нөхцөл болдог.

Зуны улиралд баруун талаасаа агаарын масс урсаж ирэхдээ Атлантын далайн чийглэг агаар замдаа каракумын цөлд хур тунадас, чийгээ алдаад, тэндхийн их хэмжээний дулаан агаарын шигээж Монголд ирнэ. Энэ нь зуны улирал олон хоног үргэлжилсэн халуун болдог.

ЦУОШГ-аас Монгол орны үүлний бүрхэлтийг 137 станц, 181 харуулын станцаар, 3 цаг тутамд өдөрт 8 удаа хэмжилт хийж, үр дүнг цаг, өдөр, сар, жилийн алхамтай тооцоолон гаргадаг. 2-р хүснэгтэд Монгол орны үүлшилтийн эзлэх хувийг харуулав.

МОНГОЛ ОРНЫ ҮҮЛШИЛТИЙН ЭЗЛЭХ ХУВЬ

2-Р ХҮСНЭГТ

№	Name	Доод мандал	Дунд мандал	Дээд мандал
A	Төвийн бүс			
1	Улаанбаатар	27.5 %	39.3 %	33.2 %
2	Төв	24.6 %	38.6 %	36.8 %
3	Өвөрхангай	41.1 %	41.9 %	17 %
4	Архангай	30.2 %	41.9 %	27.9 %
5	Баянхонгор	30.1 %	31.7 %	38.2 %
B	Хойд бүс			
6	Сэлэнгэ	30.3 %	38.2 %	31.6 %
7	Дархан-Уул	23 %	49.6 %	27.3 %
8	Орхон	30.5 %	37.8 %	31.8 %
9	Булган	27.2 %	40.7 %	32.1 %
10	Хөвсгөл	31 %	37.9 %	31.1 %
C	Баруун бүс			
11	Говь-Алтай	42.1 %	32.7 %	25.2 %
12	Завхан	31 %	36.6 %	32.3 %
13	Увс	33.4 %	42.4 %	24.2 %
14	Ховд	28.9 %	46.7 %	24.4 %
15	Баян-Өлгий	38.4 %	36.8 %	24.8 %
D	Өмнөд бүс			
16	Говьсүмбэр	27.3 %	37 %	35.7 %
17	Дорноговь	20.4 %	37.7 %	41.9 %
18	Дундговь	28.7 %	33 %	38.3 %
19	Өмнөговь	18.9 %	42.7 %	38.4 %
E	Зүүн бүс			
20	Хэнтий	25.2 %	40.5 %	34.3 %
21	Сүхбаатар	27.2 %	41.8 %	31 %
22	Дорнод	28.4 %	32.5 %	39.2 %

Эх сурвалж: (Цаг уур орчны шинжилгээний газар)

2-р хүснэгтээс харахад Монгол орны нутаг дэвсгэрт доод, дунд, дээд мандлын бүх төрлийн үүлшилт байна. Мөн үүлний эзлэх хувийг харьцуулан харахад манай оронд доод болон дунд мандлын үүлний төрөл ихэнх хувийг нь эзэлж байна.

III. ОУЦХБ-ААС БОЛОВСРУУЛСАН ҮҮЛНИЙ УНТРАЛТ ТООЦООЛОХ ITU-R ЗАГВАРЧЛАЛ

Рэйлингийн тархалтад суурилсан математик загварт усны диэлектрик нэвтрүүлэх чадвар ε (f)-г Дебэй загвараар илэрхийлснээр 1000 ГГц хүртэлх давтамжийн мужид (K_i) коэффициентыг тооцоолох боломжтой.

$$K_i = \frac{0.819f}{\varepsilon^{"}(1+\eta^2)} \text{ (дБ/км)/(гр/м}^3\text{)} \quad (1)$$

Энд

K_i-Давтамж температураас хамаарсан коэффициент

f-Радио долгионы давтамж-[ГГц]

$$\eta = \frac{2+\varepsilon^{`}}{\varepsilon^{"}} \quad (2)$$

Комплекс диэлектрик нэвтрэлтийн коэффициент

$$\varepsilon^{"}(\mathrm{f}) = \frac{\mathrm{f}(\varepsilon_0-\varepsilon_1)}{f_p\left[1+(\frac{f}{f_p})^2\right]} + \frac{\mathrm{f}(\varepsilon_1-\varepsilon_2)}{f_s\left[1+(\frac{f}{f_s})^2\right]} \quad (3)$$

$$\varepsilon^{`}(\mathrm{f}) = \frac{(\varepsilon_0-\varepsilon_1)}{\left[1+(\frac{f}{f_p})^2\right]} + \frac{(\varepsilon_1-\varepsilon_2)}{\left[1+(\frac{f}{f_s})^2\right]} + \varepsilon_2 \quad (4)$$

Энд

$$\varepsilon_{(0)} = 77.6+103.3(\theta-1) \quad (5)$$

$$\varepsilon_{(1)} = 5.48 \quad (6)$$

$$\varepsilon_{(2)} = 3.51 \quad (7)$$

$$\theta = 300/T \quad (8)$$

Т-Температур бөгөөд Кельвинээр илэрхийлнэ

Үндсэн болон хоёрдогч давтамжуудыг дараах томьёогоор илэрхийлнэ.

$$f_p = 20.09 - 142\,(\theta-1) + 294\,(\theta-1)^2 \quad (9)$$

$$f_s = 590 - 1500\,(\theta-1) \quad (10)$$

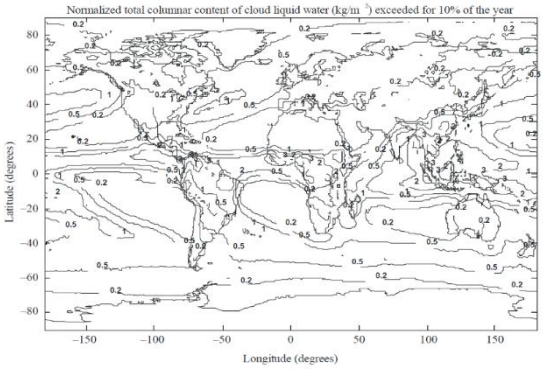
Үүлний нөлөөгөөр үүсэх унтралтыг дараах томьёогоор илэрхийлнэ.

$$A = \frac{MK_i}{\sin\theta} \text{ [dB] for } 90^0 \geq \theta \geq 5^0 \quad (11)$$

Энд:

- A-Үүлний нөлөөгөөр үүсэх унтралт
- θ-Антены босоо чиглэлийн өнцөг
- K_i-Давтамж температураас хамаарсан коэффициент
- M-Үүлэн дэх усны агууламж

ОУЦХБ-аас боловсруулсан ITU-R P.840-5 загварт дэлхийн атмосферийн шингэн усны агууламжийн жилийн 0.1%, 0.5%, 1%, 5%, 10%, 20%-хувиар тус тус тооцож, статистикийг харуулсан дижитал газрын зураг байдлаар боловсруулсан байдаг. 3-р зурагт ОУЦХБ-ын ITU-R P.840-5 загварт боловсруулсан дижитал газрын зургийг харуулж байна.



3-р зураг. Дэлхийн атмосферийн шингэн усны агууламжийн дижитал газрын зураг.

Монгол улсын нутаг дэвсгэрт хиймэл дагуулын холбооны долгион тархалтад нөлөөлөх үүлнээс үүсэх унтралтыг тооцоолохдоо үүлний усны агууламжийн хэмжээг тус статистик үзүүлэлтийн өгөгдөлд үндэслэн тооцоолно.

ДЭЛХИЙН АТМОСФЕРИЙН ШИНГЭН УСНЫ АГУУЛАМЖ

3-Р ХҮСНЭГТ.

Хамрах хүрээ		Жилийн хувь				
		0.1 %	0.5 %	1 %	5 %	10 %
		[гр/м^2]				
Уртраг	70-120 E	2	2	1	0.2	0.2
Өргөрөг	40-60 N					

ОУЦХБ-аас боловсруулсан атмосферийн давхаргын үүлний шингэн усны агууламжийг дэлхийн өргөргийн $+80^0$-аас (-80^0), уртрагийн $+150^0$-аас (-150^0) хүртэлх хязгаарт тооцоолсон байдаг. 3-р хүснэгтэд Монгол улсын нутаг дэвсгэрт хамаарах зүүн уртрагийн (75^0-120^0 E) болон хойд өргөргийн (40^0-60^0 N) бүсэд хамаарах тоон статистик өгөгдлийг харууллаа.

IV. ХИЙМЭЛ ДАГУУЛЫН РАДИО ДОЛГИОНЫ ТАРХАЛТАД ҮҮЛНЭЭС ҮҮСЭХ УНТРАЛТ ТООЦООЛОХ АРГАЧЛАЛ

Сансрын холбооны сүлжээний системийн найдвартай ажиллагааг үнэлэхэд антены чиглэлийн өнцгийн тооцоолол, ашиглах радио долгионы давтамж өндөрсөх дутам атмосферийн цаг уурын

элементүүдийн нөлөөлөл, өөрчлөлт зэргийг авч үзэх шаардлагатай байдаг. Бид үндсэн судалгааны ажилдаа Монгол орны нутаг дэвсгэрийн байршлаас хамаарсан сансрын холбооны газрын станцын нэвтрүүлэх, хүлээн авах антены хэвтээ, босоо чиглэлийн өнцөг болон тухайн цэгээс зүүн уртрагийн 113.6 E зурваст байрлах хиймэл дагуул руу долгион тархах налуу замын урт буюу зайг нийслэл, аймаг бүрээр тооцоолсон.

Энэхүү судалгааны ажилдаа нутаг дэвсгэрийн бүсчлэл бүрээс нэг аймгуудыг сонгон авч хураангуйлан загварчилж, тооцоолсон үр дүнг оруулаа. Монгол орны баруун бүсээс Баян-Өлгий аймаг, төвийн бүсээс Улаанбаатар хот, зүүн бүсээс Дорнод аймаг, Хойд бүсээс Хөвсгөл аймаг, Өмнөд бүсээс Өмнөговь аймгуудыг тус тус сонгон авч сансрын холбооны газрын станцын нэвтрүүлэх, хүлээн авах антены хэвтээ, босоо чиглэлийн өнцөг болон тухайн цэгээс зүүн уртрагийн 113.6^0 E зурваст байрлах хиймэл дагуул руу долгион тархах налуу замын урт буюу зайг тооцоолон гаргаж, тооцоолсон үр дүнг 4-р хүснэгтээр үзүүлэв.

САНСРЫН ХОЛБООНЫ ГЕОМЕТР ШУГАМЫН ГЕОМЕТР ХЭМЖИГДЭХҮҮНИЙГ ТООЦООЛСОН ҮР ДҮН

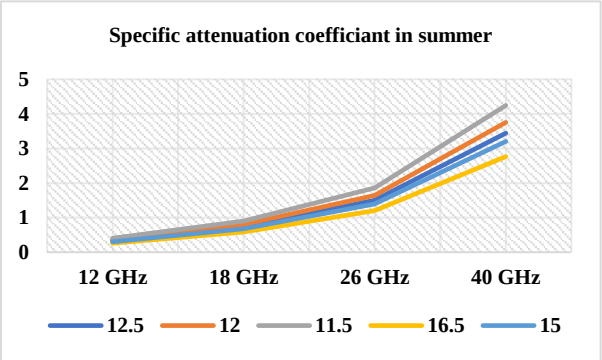
4-Р ХҮСНЭГТ .

Нийслэл, аймгуудын нэр	Налуу замын урт [км]	Антены чиглэх өнцөг	
		Хэвтээ өнцөг	Босоо өнцөг
Улаанбаатар	38213	171.04^0	34.5^0
Хөвсгөл	38463	162.6^0	31.6^0
Баян-Өлгий	38662	150^0	28^0
Өмнөговь	37865	166.8^0	40^0
Дорнод	38196	181.26^0	35^0

Газрын станцын антены босоо чиглэлийн өнцгийн хэмээ 5^0 градусаас бага тохиолдолд хиймэл дагуулын холбооны системд ашигладаггүй. 4-р хүснэгтэд тодорхойлсон техникийн үзүүлэлтээс харахад сансрын суурин үйлчилгээний зүүн уртрагийн 113.6^0E хиймэл дагуулын байрлал дээр монгол орны харьяалагдаж байгаа уртраг, өргөргийн аль ч цэгт нэвтрүүлэх, хүлээн авах антены босоо чиглэлийн өнцөг нь (28^0-40^0) градус байгаа нь хиймэл дагуулаас сигнал хүлээн авч, нэвтрүүлэхэд хамгийн тохиромжтой болох нь харагдаж байна.

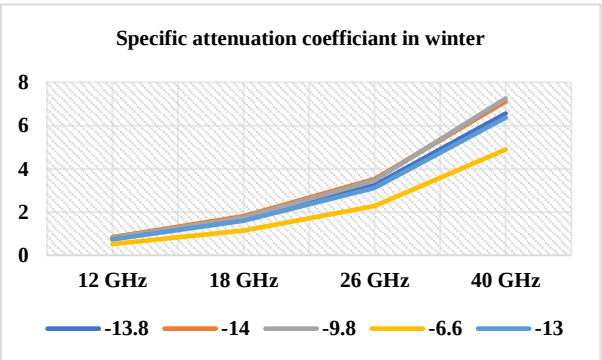
А. Ki коэффициент тооцоолсон үр дүн

Сансрын холбоонд ашиглагддаг радио долгионы давтамж нэмэгдэхийн хэрээр цаг агаарын хүчин зүйлсийн нөлөө нэмэгддэг. Тухайлбал Ku болон Ka зэрэг 10 ГГц-ээс дээш давтамжийн зурвасыг ашиглах тохиолдолд тухайн орчны цаг уурын нөхцөл байдал нь дохионы унтралт болон энергийн алдагдалд оруулах нөхцөл үүсгэдэг. Иймээс эдгээр хүчин зүйлийг зайлшгүй харгалзан үзэх шаардлагатай. Монгол орны нөхцөлд хиймэл дагуулын холбооны радио долгион тархалтад үүлнээс үүсэх унтраалтын нөлөөг үнэлэхдээ цаг уур орчны шинжилгээний газар (ЦУОШГ)-ын ажиглалтын 1999-2024 оны хооронд хийсэн 30 жилийн хугацааны агаарын температурын өөрчлөлтийн өгөгдөл ашигласан. Судалгаанд бүсчлэл бүрээс сонгогдсон нийслэл, аймгуудын цаг агаарын мэдээлэлд үндэслэн давтамж температураас хамаарсан усны диэлектрик нэвтрүүлэх коэффициентыг зун өвлийн улирлаар тооцоолж үр дүнг 4-р зураг, 5-р зургаар харуулав.



4-р зураг. Зуны улиралд давтамж температураас хамаарсан Ki коэффициентийн тооцоолсон үр дүн.

Монгол орны зуны улиралд Ku, Ka давтамжийн шууд болон гэдрэг чиглэлд температураас хамаарсан Ki коэффициентын үр дүнгээс харахад давтамж нэмэгдэх дутам Ki коэффициентын утга өсөж байна.



5-р зураг. Өвлийн улиалрд давтамж температураас хамаарсан Ki коэффициентийн тооцоолсон үр дүн.

Өвлийн улиралд Ku, Ka давтамжийн шууд болон гэдрэг чиглэлд температураас хамаарсан Ki коэффициентын үр дүнгээс харахад зуны улирлын үр дүнтэй адил давтамж нэмэгдэх дутам Ki коэффициентын утга өсөж байна.

B. Үүлнээс үүсэх унтралт тооцоолсон үр дүн

Монгол орны нөхцөлд ITU-R P.840-5 загварыг ашиглан үүлний унтралтыг тооцоолохдоо газарзүйн байршлаар ялгаатай бүс нутгуудыг төлөөлүүлэн нийслэл болон зарим аймгуудыг сонгон авч, тухайн бүс нутагт байрлах сансрын холбооны газрын станцын босоо чиглэлийн өнцгийг тооцоолсон. Мөн давтамж болон температурын хамаарлаар Ki коэффициентыг сонгосон нийслэл аймаг бүрийн хувьд тооцоолсон.

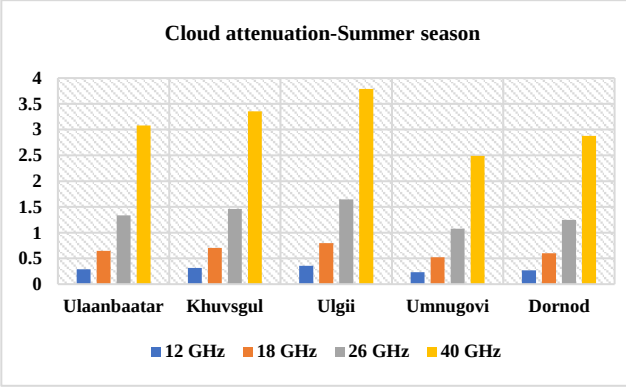
Тооцоололд үүлэн дэх усны агууламжийн хэмжээг 2 гр/м^3 гэж үзэн өвөл болон зуны улиралд С давтамжийн хувьд шууд ба гэдрэг чиглэлд тооцоолж үр дүнг 5-р хүснэгтээр үзүүлсэн болно.

САНСРЫН ХОЛБООНЫ С ДАВТАМЖИЙН ШУУД БА ГЭДРЭГ ЧИГЛЭЛД ҮҮЛНИЙ УНТРАЛТ ТООЦООЛСОН ҮР ДҮН

5-Р ХҮСНЭГТ.

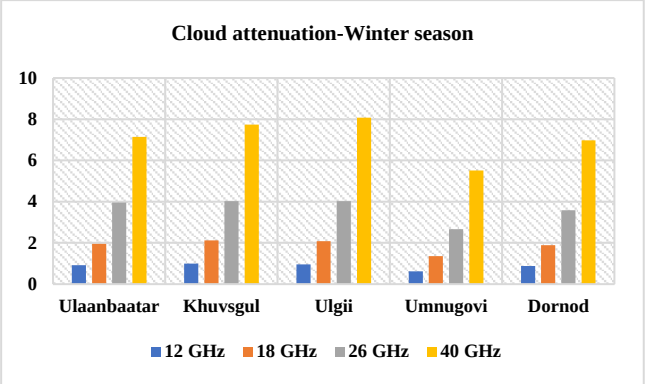
Аймгуудын нэр	Босоо өнцөг	Давтамж	
		4 ГГц	6 ГГц
		Үүлний унтралт-[дБ]	
Зуны улиралд			
Улаанбаатар	34.5^0	0.036	0.0819
Хөвсгөл	31.6^0	0.0398	0.089
Баян-Өлгий	28^0	0.0451	0.101
Өмнөговь	40^0	0.029	0.0651
Дорнод	35^0	0.034	0.076
Өвлийн улирал			
Улаанбаатар	34.5^0	0.088	0.197
Хөвсгөл	31.6^0	0.0957	0.214
Баян-Өлгий	28^0	0.091	0.203
Өмнөговь	40^0	0.0586	0.131
Дорнод	35^0	0.084	0.188

Ku ба Ka давтамжийн хувьд шууд чиглэлд нарийвчилсан тооцоо хийсэн болно. Тооцоолсон үр дүнг 6-р зураг болон 7-р зургаар үзүүлэв.



6-р зураг. Зуны улиралд хиймэл дагуулын радио долгионы тархалтад үүлнээс үүсэх унтралт тооцоолсон үр дүн

Зуны улиралд үүлний унтралт тооцоолсон үр дүнгээс харахад Баян-Өлгий аймагт бүх давтамжийн зурваст үүлний унтралт 0.404-4.244 дБ-ийн хооронд байна. Харин Өмнөговь аймагт энэ үзүүлэлт 0.2598-2.765 дБ- ийн хооронд байгаа нь илүү бага унтраалттай байгааг харуулж байна. Баян-Өлгий аймагт үүлнээс үүсэх унтралт бусад нийслэл аймгуудтай харьцуулахад харьцангуй өндөр байгааг илэрхийлж байна.



7-р зураг. Өвлийн улиралд хиймэл дагуулын радио долгионы тархалтад үүлнээс үүсэх унтралт тооцоолсон үр дүн.

Өвлийн улиралд үүлний унтралт тооцоолсон үр дүнгээс харахад Баян-Өлгий аймагт үүлнээс үүсэх унтралт 0.799-7.255 дБ-ийн хооронд хэлбэлзэж байна.. Харин Өмнөговь аймагт энэ үзүүлэлт 0.519-4,893 дБ- ийн хооронд байгаа нь харьцангуй бага унтраалттай байгааг харуулж байна. Харин Баян-Өлгий аймагт үүлнээс үүсэх унтралт бусад нийслэл болон аймгуудтай харьцуулахад өндөр түвшинд байгааг илэрхийлж байна. 6-р зураг болон 7-р зургуудын үр дүнгээс харахад өвлийн улиралд нийт нутгийн хэмжээнд үүлнээс үүсэх унтралт өндөр байгаагаас гадна бүс нутгийн ялгаа ч тод ажиглагдаж байна.

ДҮГНЭЛТ

Үүлнээс үүсэх унтралтыг нийслэл, аймгийн төвүүд, бүс нутгийн хэмжээнд сансрын холбооны С, Ku, Ka давтамжийн шууд чиглэлд тооцоолж дараах үр дүнг гаргалаа.

- Монгол орон газарзүйн байршил, тогтоц, бүтэц, уур амьсгалын нөхцөл нь дэлхийн бусад улс орнуудаас нэлээд өөр байдаг. Улирлын ялгаа ихтэй бөгөөд ялангуяа өвлийн улиралд агаарын урвуу инверс үүсдэг нь сансрын холбооны радио долгионы замчлалд нөлөөлдөг тул үүлний унтралт тооцоолоход өвлийн агаарын температур, төлөв байдлыг анхаарч үзэх шаардлагатай.

- ЦУОШГ-ын ажиглалтын станцын мэдээнээс үзэхэд манай орны ихэнх нутаг жилийн 4 улирлын туршид үүлшилттэй байдаг нь сансрын холбооны найдвартай ажиллагаанд үүлнээс үүсэх нөлөөллийг анхаарч тооцоолох шаардлагатайг харуулж байна.
- Сэрүүн бүсийн Монгол орны хувьд халуун болон хүйтний улирлын турш үүлнээс үүсэх унтралтыг нийслэл аймаг бүрээр тооцоолсон үр дүнгээс харахад өвлийн улиралд Баян-Өлгий аймагт бүх давтамжийн зурваст хамгийн их унтралт ажиглагдсан бөгөөд (0.799-7.255 дБ) байна. Зуны улиралд мөн адил Баян-Өлгий аймагт хамгийн их унтраалттай бөгөөд (0.404 дБ-4.244 дБ) хооронд байна. Харин өвөл зуны аль ч улиралд Өмнөговь аймагт хамгийн бага унтраалттай байгаа нь тогтоогдсон.
- Энэхүү судалгааны ажилд тооцоо хийх аргачлал, улирлын ялгаатай байдлыг тодорхойлон гаргасан.

Судалгааны үр дүн нь хиймэл дагуулын системийн ажиллах энергийн нөөцийг оновчтой тооцоолох, техник тоног төхөөрөмжийг зөв сонгох, системийн найдвартай ажиллагааг төлөвлөхөд техник эдийн засгийн ач холбогдолтой. Түүнчлэн Монгол улс үндэсний хиймэл дагуул хөөргөх зорилтыг шинжлэх ухааны үндэслэлтэйгээр хэрэгжүүлэхэд хувь нэмрээ оруулах, цаашдын инженерийн нарийвчилсан шийдэл гаргахад онол практикийн чухал ач холбогдолтой юм.

НОМ ЗҮЙ

[1] Л. Нацагдорж, Г. Сарантуяа, “Үүл агаар мандлын үзэгдлүүд”, 2020 он

[2] ITU-R, Recommendation ITU-R P.840-5: *Attenuation due to clouds and fog*, Radiocommunication Sector of ITU, 2012

[3] OMaps of World, “Mongolia latitude and longitude,” Digital World Maps, [Online]. Access: https://www.mapsofworld.com

[4] “Монгол улсын үндэсний хиймэл дагуул хөтөлбөр” online access www.legalinfo.mn

[5] “Сансрын холбооны үндэсний хиймэл дагуул төсөл”, Communication and Information Technology Authority, 2020.08.11, Online access www.cita.gov.mn

[6] Г. Баярсүрэн, Хөдөө орон нутагт зайн сургалт, теле-эмнэлэгийн үйлчилгээг нэвтрүүлэх боломж. ЭШӨ

[7] Харилцаа холбооны тусгай зөвшөөрөлтэй үйлчилгээ эрхлэгчдийн үндсэн үзүүлэлтүүд-2023.12.31, Харилцаа холбооны зохицуулах хороо, online access www.crc.gov.mn

[8] Ю. Отгонбаатар, “System Design & Analysis of Hybrid Terrestrial and Satellite Networks, Its Simulation of Propagation Effect for Mongolia”, магистрийн диссертаци, Энэтхэг улс, 2021 он.

[9] Y. Igarashi, H. Fujiwara, and D. Jugder, “Change of the Asian dust source region deduced from the composition of anthropogenic radionuclides in surface soil in Mongolia,” ResearchGate, Jul. 20, 2011. [Online]. Accsess: https://www.researchgate.net

[10] R. N. Mutagi, Satellite Communication: Principles and Applications, 1st ed. 2016, pp. 42–48, 185–187.

КИБЕР АЮУЛГҮЙ БАЙДАЛ ДАХЬ ХЭШ ФУНКЦИЙН ХЭРЭГЛЭЭНИЙ ТУХАЙ

Болдбаатарын ЗОРИГТ[1], Бат-Эрдэнийн МӨНХБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ, аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: Dino010400@gmail.com[1], munkhbayar.b@must.edu.mn[2]

Хураангуй: **Аж үйлдвэрийн Дөрөвдүгээр хувьсгал, мэдээллийн технологийн эрин зуун дахь хүн төрөлхтний хөгжлийн үе шатанд "Мэдээлэл"-ийн нийгэмд эзлэх байр суурь өдөр тутмын амьдралын нэг хэсэг болсон. Мэдээлэл чухал байхын хэрээр түүний аюулгүй байдлын асуудал мөн хөндөгдөнө. Одоо үед МАБ-ыг ханган, цахим орчинд аюулгүй ажиллах нь нэн тэргүүний чухал асуудлын нэг бөгөөд хувь хүний төдийгүй геополитикийн, улс төрийн хүрээнд яригдаж байна. Энэхүү судалгааны ажлаар МАБ болон КАБ-ыг хангах аргууд, тэр дундаа мэдээллийг нууцлан дамжуулахад ашиглагддаг "HASH функц"-ийн талаар судалгаа, туршилтын ажлыг гүйцэтгэлээ. "HASH функц" нь мэдээллийг нэг чиглэлд хувиргаж, тухайн өгөгдлийг дахин анхны байдалд нь оруулах боломжгүй болгох процесс юм.**

I. УДИРТГАЛ

Монгол Улсад хүчин төгөлдөр мөрдөгдөж буй хууль тогтоомжид "кибер аюулгүй байдал" гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг хэлнэ хэмээн заажээ. Кибер аюулгүй байдлыг хангахад хэш функцүүд олон төрлийн чухал үүрэг гүйцэтгэдэг бөгөөд түүнийг password protection (нууц үгийн хамгаалалт), data integrity checks (мэдээллийн уялдаа холбоог шалгах), digital signatures (цахим гарын үсэг), system auditing (системийн аудит), blockchain security (крипто блокчэйний аюулгүй байдал) зэрэг олон талын хамгаалалтад ашигладаг.[1] Хэшлэлт нь нууцлал, мэдээллийн аюулгүй байдал, хакерын халдлагаас хамгаалах хамгийн үр дүнтэй арга хэрэгслүүдийн нэг юм. Хэш функц нь шифрлэлттэй харьцуулбал, шифрлэлт нь хоёр талын процесс байдаг. Үүний утга нь өгөгдлийг нууцлах, буцааж авах боломжтой байдлаар шифрлэх бол харин хэш функц нь зөвхөн нэг чиглэлээр, өгөгдлийг "хэшлэх" үйлдлийг хийнэ. Тиймээс, хэш функц нь шифрлэлт гэж тооцогддоггүй. Жишээ нь: MD5, SHA-1, SHA-256 гэх мэт хэш функцүүд нь өгөгдлийг тодорхой нэг урттай хэш код болгон хувиргадаг. Эдгээр кодыг "буцааж" гаргаж авах боломжгүй тул тэдгээр нь зөвхөн өгөгдлийн баталгаажуулалт, шинжилгээ болон хөрвүүлэлтэд ашиглагддаг. [2] Анх 1991 онд 128bit урттай MD-5 функцийг Файл шалгах, нууц үг хадгалах, өгөгдлийн бүрэн бүтэн байдлыг шалгах зориулалттай бүтээсэн ч аюулгүй байдлын шаардлага хангаагүй тул 1995 онд АНУ-ын "NSA" 160 bit урттай SHA-1 функцийг зохиосон. Гэвч уг функц нь MD-5-тай мөн адил аюулгүй байдлын шаардлага хангаагүй тул 2001 оноос SHA-2 функцийг өнөөг хүртэл нийтлэг ашиглаж байна.

"Мэдээлэл хамгаалагдаагүй бол үнэ цэнгүй" гэх Кибер аюулгүй байдлын үндсэн зарчимд тулгуурлан үндсэн аргууд, шифрлэлтийн төрлүүд болон Хаш (Hash) функц ашиглан өгөгдлийг шифрлэх талаар судаллаа.

II. ОНОЛЫН ХЭСЭГ

Мэдээллийн аюулгүй байдлыг хангахад дараах 3 дүрмийг баримтлан ажилладаг. [3]

- Нууцлагдсан байдал: "Confidentiality"
- Бүрэн бүтэн байдал: "Integrity"
- Хүртээмжтэй байдал: "Availability"

1. Нууцлагдсан байдал

Мэдээлэл зөвхөн эрх бүхий этгээдэд хүртээмжтэй байх ёстой гэсэн зарчим юм. Энэ нь зөвшөөрөлгүй хандах оролдлогоос хамгаалах зорилготой. Хэрэгжүүлэх арга хэмжээ:

- Шифрлэлт (Encryption) – Мэдээллийг шифрлэж, зөвхөн хүлээн авагч нь унших боломжтой болгох.
- Нэвтрэх хяналт (Access Control) – Эрх бүхий хэрэглэгчдэд л мэдээлэлд хандах эрх олгох.
- Нууц үг болон хоёр шатлалт баталгаажуулалт (MFA, 2FA) – Ашиглагчийн мэдээлэлд зөвхөн баталгаажсан хүмүүс хандах боломжтой болгох.

2. Бүрэн бүтэн байдал

Мэдээлэл өөрчлөгдөхгүй, зөв, найдвартай байх ёстой гэсэн зарчим юм. Өөрөөр хэлбэл, зөвхөн эрх бүхий хүмүүс мэдээллийг засварлах ёстой бөгөөд гадны халдлага, техникийн алдаанаас үүдэн мэдээлэл гажилтгүй байх ёстой. Хэрэгжүүлэх арга хэмжээ:

- Хяналтын дүн шинжилгээ (Checksums, Hashing) – Мэдээлэл өөрчлөгдөөгүйг баталгаажуулах.
- Өгөгдлийн хяналт (Data validation) – Оролтын мэдээллийг шалгаж, зөв эсэхийг тодорхойлох.
- Хандалтын хяналт (Access Control Lists, ACLs) – Хэн мэдээлэлд өөрчлөлт оруулж болохыг тодорхойлох.
- Нөөцлөлт (Backup & Versioning) – Алдаатай, халдлагад өртсөн тохиолдолд мэдээллийг сэргээх боломжтой байх.

3. Хүртээмжтэй байдал

Мэдээлэл зөвшөөрөгдсөн хэрэглэгчдэд хэрэгтэй үед нь хүртээмжтэй байх ёстой гэсэн зарчим юм. Өөрөөр хэлбэл, сервер унтарсан, сүлжээний доголдол гарсан, халдлагад өртсөн үед мэдээлэлд

хандах боломжгүй болох эрсдэлийг багасгах хэрэгтэй.

Хэрэгжүүлэх арга хэмжээ:

- Системийн найдвартай байдал (Redundancy, Load Balancing) – Серверүүдийг дэмжих олон нөөц систем ашиглах.
- DDoS халдлагаас хамгаалах (Firewall, Anti-DDoS tools) – Сүлжээг хэт ачааллаас сэргийлэх.

Нөөц сервер (Backup Servers, Cloud Storage) – Систем доголдсон үед мэдээллийг сэргээх.

Хэш функц ажиллах үндсэн үе шат болон зураглал: Зураг 1

1. Оролтын өгөгдөл – Дурын хэмжээтэй өгөгдөл (текст, файл, тоон өгөгдөл г.м.).
2. Оролтын боловсруулалт. Үүнд:
   - Өгөгдлийг блокоор хуваах
   - Padding (нэмэлт бит оруулах)
   - Тогтмол эхлэх утгуудыг (initialization vector) тохируулах
3. Хэш алгоритмын боловсруулалт
   - Блок бүрд битийн арифметик болон логик үйлдлүүд хийх (XOR, AND, OR, NOT, SHIFT)
   - Дотоод төлөвийн шинэчлэлт
4. Гаралтын хэш утга – Тогтмол урттай хэш код үүсэх (MD5=128 бит, SHA-256 = 256 бит).

Диаграмм 1: Hash функцийн ажиллагаа

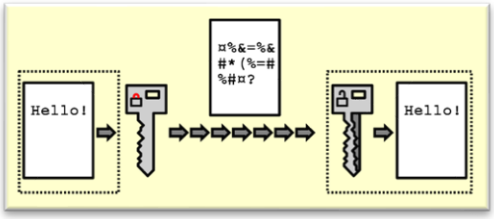
III. НУУЦЛАЛЫГ ХАНГАХ АРГА ЗАМУУД

Цахим орчинд мэдээллийн нууцлалыг хангахын тулд дараах гол аргуудыг ашигладаг.[4]

1. Шифрлэлт (Encryption) ашиглах
2. Хандалтын хяналт (Access Control) хэрэгжүүлэх
3. 2FA/MFA зэрэг баталгаажуулалтын аргыг нэвтрүүлэх
4. Кибер аюулгүй байдлын бодлогыг баримтлах

1. Шифрлэлт (Encryption)

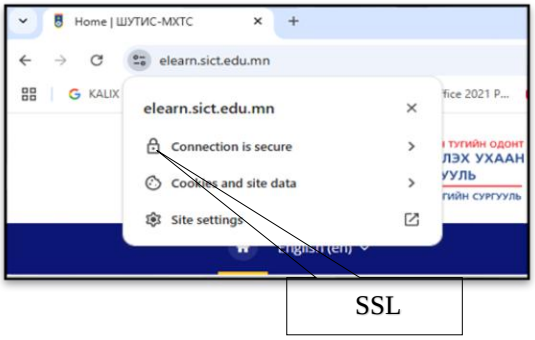
Шифрлэлт нь Зураг 1-т үзүүлснээр тухайн мэдээллийг тусгай тэмдэгт бүхий тэмдэгтээр баяжуулах процесс юм. Үндсэн 2 төрлийн шифрлэлтийн аргыг түлхүү хэрэглэдэг.



1-р зураг: Шифрлэлтийн дүрслэл

1. Symmetric Encryption (Нэг түлхүүртэй шифрлэлт) – Илгээгч болон хүлээн авагч нэг ижил түлхүүр ашиглан мэдээллийг шифрлэж, тайлдаг.[5]
2. Asymmetric Encryption (Хоёр түлхүүртэй шифрлэлт) – Илгээх болон тайлахад өөр өөр түлхүүр ашигладаг.

Нууцлалын нэг төрөл болох E2EE буюу End-to-end encryption нь тухайн өгөгдөл, мэдээллийг зөвхөн илгээгч, хүлээн авагчид хандах боломжтой ба гуравдагч этгээд хандах боломжгүй бөгөөд “Social Communication” платформуудад өргөн ашиглагддаг.[5] /Facebook messenger, X, Viber, Telegram, Whatsapp etc/. Бидний өдөр тутмын үйл ажиллагаанд ашиглагддаг цахим хуудас нь SSL/TLS шифрлэлт ашиглан HTTPS протоколоор мэдээллийг дамжуулдаг.



2-р зураг: SSL-ийг цахим хуудсан хэрэгжүүлсэн байдал

2. Хандалтын хяналт (Access Control)

Тухайн мэдээлэлд хэн, ямар эрх хэмжээгээр хандах эрхтэй, ямар түвшинд ашиглаж болохыг тодорхойлох юм. *Хандалтын хяналтын төрлүүд нь:*[6]

a. MAC (Mandatory Access Control) Төвлөрсөн удирдлагатай системийн загвар бөгөөд зөвхөн байгууллагын бодлогоор тогтоосон эрх бүхий хүмүүс мэдээлэлд хандах эрхтэй. (Засгийн газар, цэрэг арми мэт өндөр нууцлалтай мэдээлэл, мөн хувь хүний нууцтай холбоотой банк санхүү, эрүүл мэндийн байгууллагуудад өргөн ашиглагддаг.)

b. DAC (Discretionary Access Control) Тухайн файл, мэдээллийн эзэмшигч нь ACL /Access Control List/ буюу хандах эрхийн жагсаалтын дагуу мэдээлэлд хэн хандахыг шийдэх боломжтой загвар юм.

c. RBAC (Role-Based Access Control) Үүрэгт суурилсан хандалтын хяналт нь тухайн албан хаагчийн байгууллага дахь албан тушаал,

мэргэжлээс хамааран хандалтын түвшнийг тогтоох загвар юм. (Жишээ нь: Нягтлан бодогч нь зөвхөн санхүүгийн мэдээлэлд хандах эрхтэй гэх мэт)

d. PAM (Privileged Access Management)

Давуу эрхтэй хандалтын менежмент нь үүрэгт суурилсан хандалтын хяналтын нэг төрөл бөгөөд "credentials" алдагдахаас хамгаалах зорилготой загвар юм. Энэ загвараар шаардлагатай тохиолдолд тухайн ажилтан, албан хаагчдын үүрэг зорилгоос хамааран түр зуурын хандалтын эрх олгох боломжтой. Facebook, Google, Microsoft гэх мэт компаниуд OAuth 2.0 ашиглан хэрэглэгчийн эрхийг баталгаажуулдаг.

Байгууллагын мэдээлэл зөвхөн VPN ашиглан дотоод сүлжээгээр хандах боломжтой байхаар тохируулдаг.

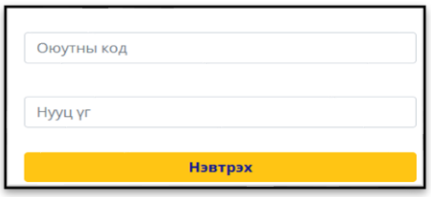
3. *Танилт ба баталгаажуулалт* *(Authentication & Verification)*

Тухайн мэдээлэлд хандах, нэвтрэх эрх бөгөөд танилт ба баталгаажуулалтын арга юм. Танилт ба баталгаажуулалтын арга нь 1, 2 болон олон шатлалт байх бөгөөд одоо үед ихэнх платформууд аюулгүй байдлаа илүү өндөр түвшинд хангахын тулд 2 ба түүнээс дээш баталгаажуулалтын аргыг ашиглаж байна.[7]

Баталгаажуулалтын төрлүүд: [8]

1. Нэг шатлалт баталгаажуулалт (Single-Factor Authentication – SFA)

Зөвхөн нууц үг, PIN код гэх мэт нэг аргаар хэрэглэгчийг баталгаажуулдаг.

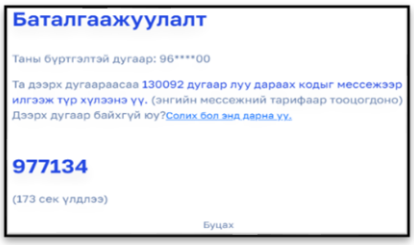


3-р зураг: SFA ашиглан хандах цахим хуудас

2. Хоёр шатлалт баталгаажуулалт (Two-Factor Authentication – 2FA)

Хэрэглэгч өөрийгөө хоёр төрлийн мэдээллээр баталгаажуулдаг.

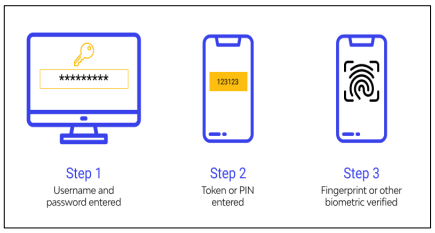
E-Mongolia систем нь 2FA нууц үг + OTP код ашиглах.



4-р зураг: 2FA ашиглан хандах систем

3. Олон шатлалт баталгаажуулалт (Multi-Factor Authentication – MFA)

3 ба түүнээс дээш баталгаажуулалтын аргыг хослуулдаг. Нууц үг + SMS OTP + Хурууны хээ ашиглан системд нэвтрэх.



5-р зураг: MFA ашиглан хандах цахим хуудас

Google, Microsoft, Apple зэрэг компаниуд 2FA ашиглахыг хэрэглэгчдэд зөвлөдөг.

Биометр танилт (Face ID, Fingerprint) нь зөвхөн тухайн хүн мэдээлэлд хандах боломжтой болгож, аюулгүй байдлыг өндөр түвшинд хангадаг.

4. *Мэдээллийн нууцлалыг хадгалах бодлого* *(Data Privacy Policy)*[9]

Улс орон, шат шатны байгууллагууд нь иргэд, ажилтан, албан хаагчид болон хэрэглэгчдийн мэдээллийг хамгаалахын тулд тодорхой бодлого, эрх зүйн акт, баримт бичгүүд боловсруулдаг. Үүнд:

- General Data Protection Regulation (GDPR) [10] - Европын холбооны мэдээлэл хамгаалах журам
- California Consumer Privacy Act (CCPA) [11] – АНУ-ын хэрэглэгчийн мэдээлэл хамгаалах хууль
- Монгол Улсын "Хувь хүний мэдээлэл хамгаалах тухай", "Нийтийн мэдээллийн ил тод байдлын тухай хууль", "Кибер аюулгүй байдлын тухай хууль" гэх мэт.

Эдгээр хууль, эрх зүйн баримт бичгүүд нь ард иргэд, олон нийтийн хувийн мэдээллийг хамгаалах, Кибер аюулгүй байдлыг хамгаалах зорилгоор боловсруулагдсан эрх зүйн баримт бичгүүд бөгөөд Facebook, Google, Apple зэрэг дэлхийн хэмжээний компаниуд хэрэглэгчийн мэдээллийг GDPR-ын дагуу, харин Монгол Улсад үйл ажиллагаа эрхэлж буй компани, ААН-үүд, цахим платформууд нь хэрэглэгчийн мэдээллийг зөвшөөрөлгүй задруулахгүй байх нууцлалын бодлого боловсруулан, мөрдөх үүрэгтэй гэх мэт.

Хэрэв мэдээллийн нууцлал алдагдвал [12]:

1. Хувийн мэдээлэл хулгайд алдагдах (Identity Theft)
2. Компанийн санхүүгийн мэдээлэл задарч өрсөлдөгчдөд ашиглагдах.
3. Төрийн нууц мэдээлэл алдагдаж үндэсний аюулгүй байдалд заналхийлэх.
4. Кибер халдлага, хакерын дайралтад өртөх зэрэг төрөл бүрийн эрсдэл үүснэ.

5. *Нууцлал* *(Confidentiality)* [13]

Нууцлал нь кибер аюулгүй байдлын хамгийн чухал бүрэлдэхүүн хэсэг бөгөөд зөвхөн эрх бүхий хүмүүс мэдээлэлд хандах боломжийг бүрдүүлэх, хязгаарлах арга хэмжээний цогц юм. Аж үйлдвэрийн дөрөвдүгээр хувьсгал, мэдээллийн технологийн эрийн зуун хэмээн нэрлэгдсэн одоо үед мэдээллийн аюулгүй байдлыг сахих нь хувь хүн, байгууллага төдийгүй улс орны түвшинд нэн тэргүүний асуудал болоод байна. "Мэдээлэл хамгаалагдаагүй бол үнэ цэнгүй" гэсэн зарчмыг улс орнууд, дэлхийн хэмжээний корпорац, компаниуд, олон улсын байгууллагууд урьтал болгон хэрэгжүүлж байна.

Бид энэхүү өгүүллийн гуравдугаар хэсэг буюу Нууцлалыг хангах арга замууд хэсэгт нууцлалыг хэрэгжүүлэх, шифрлэлтийн талаар цухас дурдсан бөгөөд энэ хэсэгт шифрлэлтийн аргууд болон “Hash” функцийн талаар дэлгэрүүлэн тайлбарлаж, “Hash” функцийн энгийн туршилтыг оруулъя.

5.1 Шифрлэлтийн үндсэн төрлүүд

Шифрлэлт (Encryption) нь мэдээллийн аюулгүй байдлын хамгийн чухал бүрэлдэхүүн хэсэг бөгөөд аливаа системийн нууцлал (Confidentiality)-ыг хангадаг.

1. Симметрик шифрлэлт (Symmetric Encryption)
2. Ассимметрик шифрлэлт (Asymmetric Encryption)
3. Хаш (Hash) функц ба нэг чиглэлийн шифрлэлт

5.1.1 Симметрик шифрлэлт (Symmetric Encryption)

Симметрик шифрлэлд нэг түлхүүр ашигладаг. Илгээгч болон хүлээн авагч хоёул адилхан түлхүүртэй байх ёстой бөгөөд тухайн түлхүүрийг хакердаж чадвал мэдээлэл задрах эрсдэлтэй.

1. Алгоритмууд: AES, DES, 3DES, Blowfish
2. Давуу тал: Хурдан, бага нөөц ашиглана.
3. Сул тал: Түлхүүрийг аюулгүй дамжуулах шаардлагатай. Үүнд:
   - Wi-Fi хамгаалалт (WPA2, WPA3) нь AES симметрик шифрлэлт ашигладаг.
   - Засгийн газрын өндөр хамгаалалттай мэдээллүүд нь AES-256 алгоритмаар шифрлэгддэг. [14]

5.1.2 Ассимметрик шифрлэлт (Asymmetric Encryption)

Ассимметрик шифрлэлд нээлттэй түлхүүр (Public Key) болон хаалттай түлхүүр (Private Key) гэсэн 2 төрлийн түлхүүрийг ашигладаг байна. [15]

1. Алгоритмууд [16] : RSA, ECC, Diffie-Hellman, ElGamal
2. Давуу тал: Илүү аюулгүй, түлхүүрийг дамжуулах шаардлагагүй.
3. Сул тал: Илүү их тооцооллын нөөц шаарддаг (удаан). Хэрэглээ:
   - SSL/TLS (HTTPS) – Вебсайтуудын нууцлалтай холболтод RSA шифрлэлт ашиглагддаг.
   - И-мэйл шифрлэлт (PGP, S/MIME) – И-мэйлийг ассимметрик шифрлэлтээр хамгаална.
   - Cryptocurrency (Bitcoin, Ethereum) – Хэрэглэгчийн хэтэвч (wallet) public-private **key** ашигладаг.

5.1.3 Хаш (Hash) функц ба нэг чиглэлийн шифрлэлт

Hashing гэдэг нь мэдээллийг нэг чиглэлд хувиргаж, тухайн өгөгдлийг дахин анхны байдалд нь оруулах боломжгүй болгох процесс юм. [17]

1. Алгоритмууд: MD5, SHA-1, SHA-256, SHA-512 [18]
2. Давуу тал: Хурдан, нэг чиглэлтэй тул хакердах боломжгүй.
   - Нууц үг хадгалах – Вебсайтууд хэрэглэгчийн нууц үгийг SHA-256 алгоритмаар хаш хийж хадгалдаг.
   - Блокчейн технологи – Hash функц ашиглан өгөгдлийг баталгаажуулдаг**.** [19]

5.2 Шифрлэлт хаана ашиглагддаг вэ?

Шифрлэлт нь бидний өдөр тутмын амьдралд дараах байдлаар хэрэглэгддэг. Хүснэгт 1-д Hash функцийн хэрэглээг харуулав.

ХҮСНЭГТ 1: HASH ФУНКЦИЙН ХЭРЭГЛЭЭ

Ашиглагдах талбар	**Шифрлэлт ашиглах арга**
Интернэт харилцаа	HTTPS (SSL/TLS)
Мессенжер, чат	End-to-End Encryption (WhatsApp, Messenger)
Файлын хадгалалт	BitLocker (Windows), FileVault (Mac)
Wi-Fi хамгаалалт	WPA2, WPA3 (AES шифрлэлт)
Блокчейн, криптовалют	Public-Private Key (Bitcoin, Ethereum)
И-мэйл хамгаалалт	PGP, S/MIME
Нууц үгийн хамгаалалт	Hashing (SHA-256, bcrypt)
Банк, санхүүгийн систем	AES-256, RSA шифрлэлт

5.3 Шифрлэлтийн давуу болон сул талууд

ХҮСНЭГТ 2-Д МЭДЭЭЛЛИЙГ ШИФРЛЭХИЙН ДАВУУ БОЛОН СУЛ ТАЛУУД

Давуу тал	**Сул тал**
Мэдээллийг зөвхөн зөвшөөрөгдсөн хэрэглэгч унших боломжтой.	Зарим алгоритмууд өндөр тооцоолол шаарддаг.
Хакер, халдлагад өртөх эрсдэлийг бууруулдаг.	Шифрлэлтийн түлхүүр алдвал мэдээлэл сэргээх боломжгүй.
Кибер аюулгүй байдлыг сайжруулдаг.	Хуучирсан алгоритмууд (MD5, DES) хэрэглээнээс гарч байгаа.
GDPR, HIPAA зэрэг хууль эрхзүйн шаардлагыг хангана.	Шифрлэлтийн аргыг хакерууд ашиглан хууль бус үйлдэл хийх боломжтой.

- Симметрик шифрлэлт – Хурдан, бага нөөц ашиглана (AES, DES).
- Ассимметрик шифрлэлт – Илүү аюулгүй, түлхүүр солилцоонд ашиглана (RSA, ECC).
- Hash функц – Нууц үг хадгалах, өгөгдлийг баталгаажуулахад хэрэглэнэ (SHA-256).

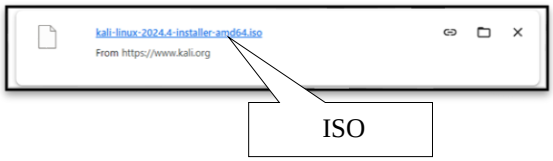
5.4 Туршилт

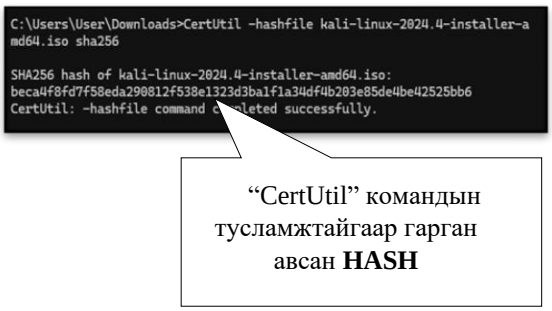
Энэхүү өгүүллийг бэлдэх явцдаа “Hash” функцийн талаар судлан интернэт орчинд байршуулсан файлыг ашиглан энгийн туршилт хийсэн.

5.4.1 Интернэт орчинд байршуулсан Kali Linux ISO файлын HASH - Зураг 6

6-р зураг: Туршилт

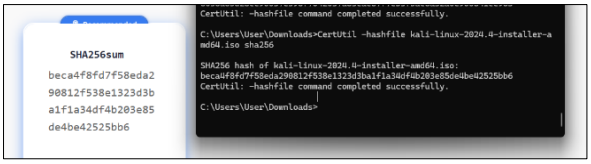
5.4.2 Kali Linux ISO файлыг татан "Windows" үйлдлийн системийн орчинд "CertUtil" командын тусламжтайгаар гарган авсан HASH-тай харьцуулан шалгасан. Зураг 7





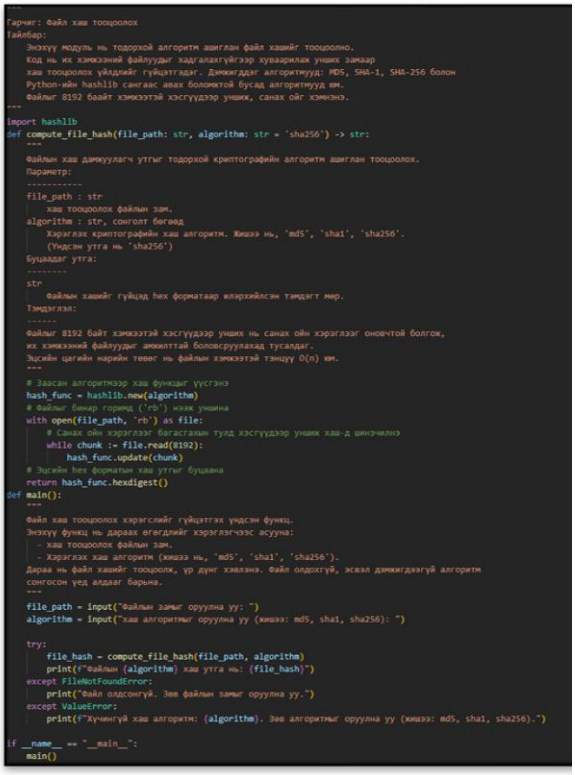
7-р зураг: Туршилт

Туршилтаар вэбсайт дээрх HASH болон гарган авсан HASH нь хоорондоо таарсан бөгөөд ISO файл нь ямар нэгэн хакер, гуравдагч этгээдийн халдлагад өртөөгүй татагдсан байна. Зураг 8



8-р зураг: Харьцуулсан шалгалт

5.5 Файл HASH-лэх Python код. Зураг 9

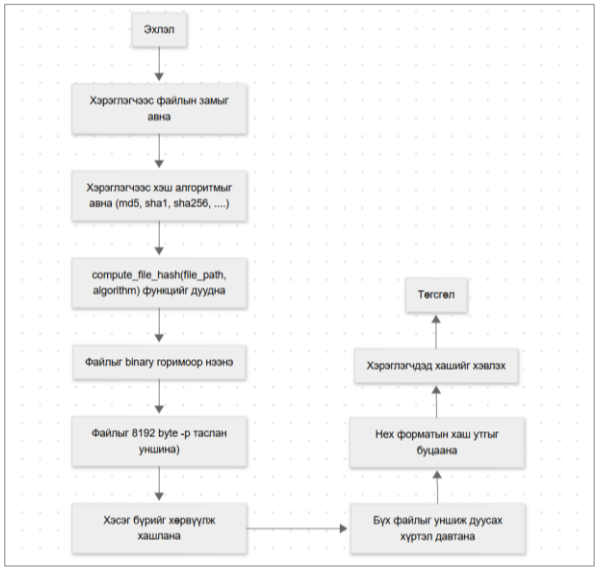


```
Гарчиг: Файл хэш тооцоолох
Тайлбар:
    Энэхүү модуль нь тодорхой алгоритм ашиглан файл хэшийг тооцоолно.
    Код нь их хэмжээний файлуудыг хадгалахгүйгээр хуваарилах унших замаар
    хэш тооцоолох үйлдлийг гүйцэтгэдэг. Дэмжигдэх алгоритмууд: MD5, SHA-1, SHA-256 болон
    Python-ийн hashlib сангаас авах боломжтой бусад алгоритмууд юм.
    Файлыг 8192 байт хэмжээтэй хэсгүүдээр уншиж, санах ойг хэмнэнэ.
"""
import hashlib
def compute_file_hash(file_path: str, algorithm: str = 'sha256') -> str:
    """
    Файлын хэш дамжуулагч утгыг тодорхой криптографийн алгоритм ашиглан тооцоолох.
    Параметр:
    ----------
    file_path : str
        хэш тооцоолох файлын зам.
    algorithm : str, сонголт бөгөөд
        Хэрэглэх криптографийн хэш алгоритм. Жишээ нь, 'md5', 'sha1', 'sha256'.
        (Үндсэн утга нь 'sha256')
    Буцаадаг утга:
    --------
    str
        Файлын хэшийг гүйцэд hex форматаар илэрхийлсэн тэмдэгт мөр.
    Тэмдэглэл:
    ------
    Файлыг 8192 байт хэмжээтэй хэсгүүдээр унших нь санах ойн хэрэглээг оновчтой болгож,
    их хэмжээний файлуудыг амжилттай боловсруулахад тусалдаг.
    Эцсийн цагийн нарийн төвөг нь файлын хэмжээтэй тэнцүү O(n) юм.
    """
    # Зааасан алгоритмээр хэш функцыг үүсгэнэ
    hash_func = hashlib.new(algorithm)
    # Файлыг бинар горимд ('rb') нээж уншина
    with open(file_path, 'rb') as file:
        # Санах ойн хэрэглээг багасгахын тулд хэсгүүдээр уншиж хэш-д шингээлнэ
        while chunk := file.read(8192):
            hash_func.update(chunk)
    # Эцсийн hex форматын хэш утгыг буцаана
    return hash_func.hexdigest()
def main():
    """
    Файл хэш тооцоолох хэрэгслийг гүйцэтгэх үндсэн функц.
    Энэхүү функц нь дараах өгөгдмөл хэрэглэгчээс асууна:
      - хэш тооцоолох файлын зам.
      - Хэрэглэх хэш алгоритм (жишээ нь, 'md5', 'sha1', 'sha256').
    Дараа нь файл хэшийг тооцоолж, үр дүнг хэвлэнэ. Файл олдохгүй, эсвэл дэмжигдээгүй алгоритм
    сонгосон үед алдаат барьна.
    """
    file_path = input("Файлын замыг оруулна уу: ")
    algorithm = input("Хэш алгоритмыг оруулна уу (жишээ: md5, sha1, sha256): ")

    try:
        file_hash = compute_file_hash(file_path, algorithm)
        print(f"Файлын {algorithm} хэш утга нь: {file_hash}")
    except FileNotFoundError:
        print("Файл олдсонгүй. Зөв файлын замыг оруулна уу.")
    except ValueError:
        print(f"Хүчингүй хэш алгоритм: {algorithm}. Зөв алгоритмыг оруулна уу (жишээ: md5, sha1, sha256).")

if __name__ == "__main__":
    main()
```

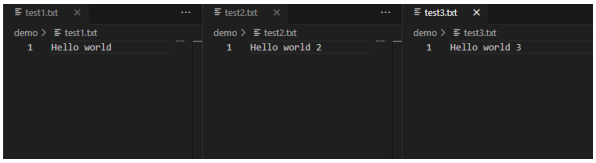
9-р зураг: Турших зорилгоор зохиосон код

Туршилтын явцад файл Hash-лэх энгийн Python кодыг зохион туршсан бөгөөд программыг ажиллуулах үед файлын байршил, нэр болон Hash-лэх алгоритмыг сонгон үүсгэнэ.

5.6 Python кодын блок диаграмм. Зураг 10

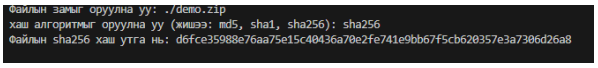


10-р зураг Python кодын хялбарчилсан диаграмм



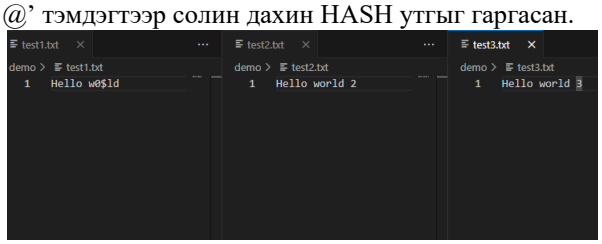
11-р зураг: Hash утгын өөрчлөлт. Үүсгэсэн файл /өөрчлөөгүй/

Энэ туршилтад 3ш файлыг нэгтгэн 1ш **compressed** буюу .zip файл үүсгэсэн бөгөөд эхний файлын HASH утга:

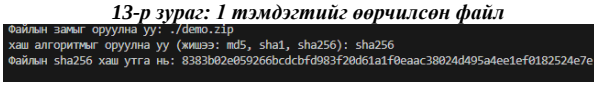


12-р зураг: Үүсгэсэн файл HASH утга

1 файлын “Hello world” гэсэн утгын ‘o’ үсгийг ‘@’ тэмдэгтээр солин дахин HASH утгыг гаргасан.



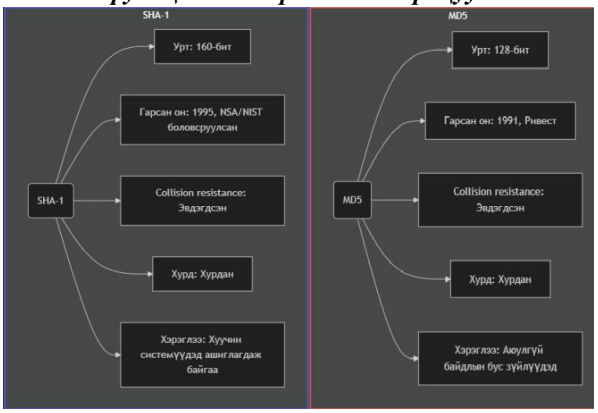
13-р зураг: 1 тэмдэгтийг өөрчилсөн файл



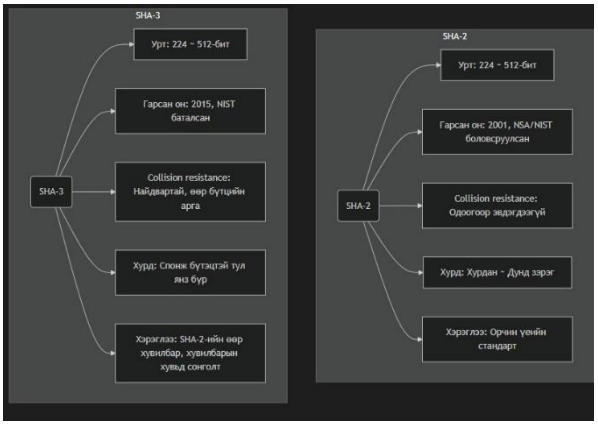
14-р зураг: 1 тэмдэгтийг өөрчилсөн файлын HASH утга

Туршилтаас харахад Zip файл доторхооc test1.txt-н 2 үсгийг солиход HASH утга солигдож байгаа нь тухайн файлыг дамжуулах явцад анхны агуулгыг нь өөрчилсөн эсэхийг шалгахад файлыг HASH-лах нь чухал ач холбогдолтойг харуулж байна.

5.7 HASH функцийн алгоритмын харьцуулалт



***15-р зураг:* /SHA1 болон MD5/**



16-р зураг: /SHA-2 болон SHA-3/

Дээрх хүснэгтүүдийг /Зураг 15, 16/ харьцуулан харахад SHA-1 болон MD5 функцүүд нь “Collision resistance” буюу давхцахаас сэргийлэх чадамжууд нь эвдэгдсэн харагдаж байна. Харин SHA-2 болон SHA-3 функцүүд нь одоогийн байдлаар эвдэгдээгүй, найдвартай харагдаж байна.

ДҮГНЭЛТ

Хэш функц нь мэдээллийн аюулгүй байдал, нууцлал, өгөгдлийн бүрэн бүтэн байдлыг хангах чухал ач холбогдолтой бөгөөд энэхүү өгүүллийг боловсруулах явцад хэш алгоритмуудын онцлог, хэрэглээ, давуу болон сул талуудыг судалсан болно. Судалгааны явцад хэш функцийн криптографийн аюулгүй байдлыг хангах хүчин зүйлс, учирч болох эрсдэл, түүнээс сэргийлэх арга замуудыг нарийвчлан авч үзсэн.

Мөн орчин үеийн мэдээллийн аюулгүй байдлын системд хэш алгоритмуудын гүйцэтгэх үүргийг судалж, (MD5, SHA-1, SHA-2, SHA-3 гэх мэт)-ийн үр ашиг, аюулгүй байдал, ашиглалтын онцлогийг харьцуулан судлав. Үүнээс гадна, хэш функцийн алгоритмуудын сул тал, боломжит халдлагуудын эсрэг хамгаалах аргачлалыг тодорхойлж, ирээдүйн судалгааны чиг хандлагыг тодорхойлох оролдлого хийсэн.

Олон улсад мэдээллийн аюулгүй байдлын шинжээчид (MD5) нь Pre-image болон Birthday Attack (Хүчтэй тооцоолох чадалтай төхөөрөмж ашиглан өгөгдлийн анхны утгыг сэргээх) гэх халдлагуудад сул талтай байгаа тул өнөө үед ашиглаж байгаа SHA-2, ирээдүйн чиг хандлагад зориулан бүтээсэн SHA-3, BLAKE2 зэрэг алгоритмуудыг хэрэглэхийг зөвлөж байгаа юм байна.

Энэхүү судалгааны үр дүнд хэш функцийн онол, практик хэрэглээний талаарх ойлголт хүргэхийг зорьсон ба ирээдүйд шинэ технологи буюу (Quantum Computer)-ийн тооцоолох чадварын эрин үед үргэлжлүүлэн ашиглах боломжтой эсэхийг судлах, цаашид шинэ арга зам эрэлхийлэх нь зүйтэй гэж дүгнэлээ.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] https://fidelissecurity.com/cybersecurity-101/learn/what-is-hashing/
[2] https://medium.com/@erdenebayr.d/hash-function-af3a930506ea
[3] https://www.fortinet.com/de/resources/cyberglossary/cia-triad#:~:text=The%20three%20letters%20in%20%22CIA,equipped%20to%20handle%20threat%20incidents.
[7] https://sumadi.net/difference-between-authentication-and-verification/#:~:text=Authentication%20vs.,digital%20key%2C%20or%20biometric%20identification
[8] https://regulaforensics.com/blog/types-of-authentication/#:~:text=all%20three%20stages.-,Types%20of%20authentication%20explained,needed%20to%20complete%20the%20authentication
[9] https://termly.io/resources/templates/privacy-policy-template/
[10] https://gdpr-info.eu/
[11] https://oag.ca.gov/privacy/ccpa
[12] https://www.f-secure.com/en/articles/why-do-hackers-want-your-personal-information
[13] https://cpdonline.co.uk/knowledge-base/safeguarding/what-is-confidentiality
[14] https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard
[15] https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/
[16] https://www.ssl2buy.com/wiki/diffie-hellman-rsa-dsa-ecc-and-ecdsa-asymmetric-key-algorithms
[17] https://www.crowdstrike.com/en-us/cybersecurity-101/data-protection/data-hashing/#:~:text=Hashing%20use%20cases%20in%20cybersecurity,File%20and%20document%20management
[18] https://certera.com/blog/sha1-vs-sha2-vs-sha256-vs-sha512-hash-algorithms-know-the-difference/#:~:text=of%20SHA%2D256.-,What%20Distinguishes%20SHA%2D1%2C%20SHA%2D2%2C%20SHA%2D,newly%20issued%20SSL/TLS%20certificates.
[19] https://www.scalingparrots.com/en/blockchain-hash-what-is-it/#:~:text=A%20Blockchain%20hash%20is%20a,together%20chronologically%20using%20hash%20values.
- https://catalog.must.edu.mn/
- https://chatgpt.com/
- https://legalinfo.mn/mn

УНШИЖ СУДАЛСАН ЭРДЭМ ШИНЖИЛГЭЭНИЙ БҮТЭЭЛҮҮД

[20] Эрдэнэбат Чулуун, Сигнатурт тулгуурласан сүлжээний халдлага илрүүлэх систем хөгжүүлэх нь, хурлын өгүүлэл, 2014
[21] Hongjun Wu, The Hash Function JH 1 2011
[22] Heiko Knospe, A Course in Cryptography 2019, American Mathematical Society.
[23] Bart Preneel, Cryptographic hash funtions, 1994
[4] https://www.titanfile.com/blog/3-methods-to-ensure-confidentiality-of-information/#:~:text=What%20are%205%20ways%20to,information%20and%20mitigate%20potential%20risks.
[5] https://us.norton.com/blog/privacy/what-is-encryption
[6] https://www.syteca.com/en/blog/mac-vs-dac#:~:text=Mandatory%20access%20control%20(MAC)%20is,for%20information%20before%20gaining%20access.

ИХ ӨГӨГДЛИЙН САН ДАХЬ ХУВИЙН МЭДЭЭЛЛИЙГ ХАМГААЛАХ АРГАЧЛАЛ

Буянжаргалын БАТЦЭЦЭГ[1], Аюушийн АЛТАНГЭРЭЛ[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбоо Технологийн Сургууль, Мэдээлэл технологийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: j.it20e056@must.edu.mn[1], a.altangerel@must.edu.mn[2]

Хураангуй: **Хувийн мэдээллийг хамгаалах аргуудыг судалснаар төрийн болон хувийн байгууллагуудад тус тусын өгөгдлөө хуулийн хүрээнд нэгтгэн төрийн үйлчилгээ ,бизнесийн чадвараа өргөжүүлэх боломж нээгдэнэ.**

Түлхүүр үг: Хамгаалах арга,Data privacy,Date security,Data Breach, Re-identification attacks

I. УДИРТГАЛ

Монгол Улсад интернэт албан ёсоор 1996 оны 01 сарын 17 нд Датаком ХХК нэвтрүүлснээр Азийн 10 дах интернэтэд холбогдсон улс болж дижитал өгөгдөл үүсэх эхлэл тавигдсан. Улмаар интернэтийн хэрэглээ нэмэгдэж сошиал медиа, цахим худалдаа, үйлчилгээ хөгжиж их хэмжээний өгөгдөл бий болж эхэлсэн. Мөн үүрэн холбооны операторууд байгуулагдаж хэрэглэгч нэмэгдэхийн хэрээр холбооны өгөгдөл, байршлын өгөгдөл зэрэг их өгөгдлийн хэсгийг үүсгэж эхэлсэн.

Монгол улсад их өгөгдөл нь технологийн хөгжилтэй уялдан аажмаар үүссэн бөгөөд 2010 аад оноос эрс нэмэгдэж, улмаар Монгол улс төрийн үйлчилгээг бүрэн цахимжуулах “Цахим монгол” зэрэг томоохон төслүүдийг 2020 оноос хэрэгжүүлж байгаа нь цахим мэдээллийн сангууд ихээр үүсэхэд дэмжлэг болж өгсөн. Түүнчлэн 2023 оны 11 сарын 8-нд Монгол улс засгийн газраас “Их өгөгдлийн сан” үүсгэх тогтоол гарч салбар бүрийн өгөгдлийг нэгтгэх ажил өрнөж байна.

Өнөөгийн тус тусдаа байгаа өгөгдлийн сан нь тухайн байгууллагын шийдвэр гаргалтад нөлөөлдөг бол их өгөгдлийн сан үүссэнээр улс эх орны хөгжил дэвшилд бодитой хувь нэмэр оруулна гэж Монгол улсын ЦХХХЯ нь 2025 оны 03 сарын 12-ны өдрийн Их өгөгдөл хиймэл оюун ухаан (Data+AI)-ы үндэсний стратеги хэлэлцүүлгийн үеэр онцлов.

Их өгөгдөл нэгтгэх үйл явцын хүрээнд хуулиар хамгаалагдсан хувь хүний хувийн болон эмзэг мэдээллийг хэрхэн нууцлах, хамгаалах, дамжуулах асуудлууд хурцаар тавигдаж байна. Хувь хүний мэдээлэл болон эмзэг мэдээллийг алдахад хууль эрхзүйн, нийгмийн, эдийн засгийн , кибер зэрэг олон төрлийн аюул тулгардаг. Иймээс зайшгүй их өгөгдлийн санд хэрэглэгчийн хувийн мэдээллийг хамгаалан хэрэглэгчийг тодорхойлох боломжгүй болгох шаардлага тулгарч байна.

Өнөө үед их өгөгдлийн санд
- Хэрэглэгчийн хувийн мэдээллийг хамгаалах нууцлалын асуудал
- Өгөгдлийн алдагдал болон кибер халдлагаас урьдчилан сэргийлэх аюулгүй байдлын асуудал
- Мэдээллийн үнэн зөв, найдвартай байдлыг хангах өгөгдлийн чанарын асуудал
- Их хэмжээний өгөгдлөөс ашигтай мэдээлэл гаргаж авах үр дүнтэй аргуудыг хөгжүүлэх боловсруулалтын асуудлууд ихээхэн анхаарал татаж байна .

Энэхүү судалгааны ажлаараа эхний асуудлыг судалж их өргөдлийн сан дахь хувийн мэдээлэл, болон эмзэг мэдээллүүдийг хамгаалах өгөгдөл хамгаалах аргуудаас шууд танигдах боломжтой өгөгдлийг устгах, бүдгэрүүлэх (Anonymization,K-Anonymity, L-Diversity), бодит өгөгдлийг кодчилох (Pseudonymization), Шифрлэлт (AES, RSA, Homomorphic Encryption) ашиглах зэрэг өгөгдөл хамгаалах алгоритм, Differential Privacy загвар үр дүн технологийн ялгаг гарган тухайн өгөгдлийг ямар аргаар боловсруулбал дээр вэ гэдгийг санал болгох болно.

II. ИХ ӨГӨГДЛИЙН АЮУЛГҮЙ БАЙДЛЫН ҮНДСЭН ОЙЛГОЛТ

Энэ хэсэгт бид өгөгдлийн нууцлал (data privacy), өгөгдлийн аюулгүй байдал (data security), өгөгдөлд суурилсан халдлагууд (Data Breach, Re-identification attacks) талаар судлах болно.

Үндсэн ойлголт

А) Өгөгдлийн нууцлал (data privacy)

Энэ нь өгөгдлийн хэрхэн цуглуулах , хадгалах, удирдах, гуравдагч этгээдтэй хуваалцах, түүнчлэн холбогдох нууцын хуулиудыг дагаж мөрдөхөд чиглэнэ. Өгөгдлийн нууцлал нь хувь хүний хувийн мэдээллээ хянах эрхийг чухалчилдаг. Монгол улс нь хувийн мэдээлэл болон эмзэг мэдээллийг тодорхойлон хуульчилсан байдаг.

Өгөгдлийн нууцлалын гол бүрэлдэхүүн хэсэг нь байгууллага, хувь хүмүүсийн итгэлийг хадгалах,дүрэм журмыг дагаж мөрдөх юм. Байгууллага нь өгөгдлийн нууцлалыг хэрэгжүүлснээр хэрэглэгчдээ (хувь хүн) итгэлцлийг бий болгоно.

Өгөгдлийн нууцлалын жишээ

- Нууц мэдээлэлд зөвхөн эрх бүхий ажилтнууд хандуулах

- Зөвшөөрөлгүй хандалтаас сэргийлэхийн тулд өгөгдлийг шифрлэх

- Хувийн мэдээллийг цуглуулах, ашиглахыг зөвхөн шаардлагатай зүйлээр хязгаарлах

- Хэрэглэгчдэд өөрсдийн хувийн мэдээллээ устгах ,өөрчлөх гэх мэт хувийн мэдээллээ хянах боломжийг олгох

- Хувийн мэдээлэл хамгаалах нууцлалтай холбоотой холбогдох хууль тогтоомжийг дагаж мөрдөх (GDPR, CCPA, бүс нутгийн хуулиуд...)

Хувийн мэдээллийг цуглуулах, ашиглахыг зөвхөн шаардлагатай эрхээр хязгаарлах нь мэдээллийн нууцын өөр нэг чухал тал юм. Энэ нь байгууллагуудад зөвхөн тодорхой зорилгоор шаардлагатай хувийн мэдээллийг цуглуулж ашиглах ёстой бөгөөд шаардлагатай хэмжээнээс илүү мэдээлэл цуглуулахгүй байх ёстой гэсэн үг юм.

Б) Өгөгдлийн аюулгүй байдал (data security)

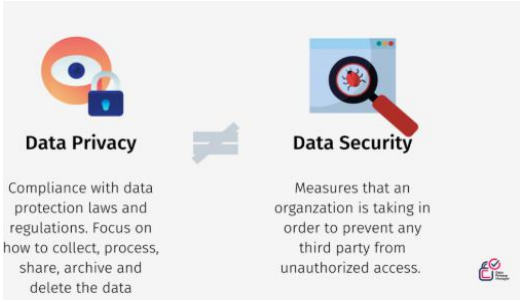
Энэ нь гуравдагч этгээдийн зөвшөөрөлгүй хандалт, өгөгдөл өөрчлөх, устгахаас хамгаалах техникийн болон зохион байгуулалтын арга хэмжээг хэлнэ. Энэ нь нууцлал, өгөгдлийн бүрэн бүтэн байдал, хүртээмжтэй байдлыг хангахыг эрмэлздэг.

Өгөгдлийн аюулгүй байдал нь ихэвчлэн өгөгдлийн санд хадгалагдсан мэдээллийг хамгаалахад чиглэсэн.

Өгөгдлийн аюулгүй байдал нь шифрлэлт, өгөгдлийг далдлах зэрэг аргуудыг ашиглаж, өгөгдлийг зөвшөөрөлгүй нэвтрэхээс хамгаалдаг.

Өгөгдлийн аюулгүй байдал нь ихэвчлэн өгөгдлийн сангийн хэрэглээнд чиглэсэн байдаг. Өгөгдлийн аюулгүй байдал нь өгөгдлийг дамжиж буй эсвэл хөдөлгөөнгүй байх үед хамгаалах процессуудыг хэлнэ.

1- р зураг өгөгдлийн нууцлал болон өгөгдлийн аюулгүй байдал хоёрын ялгааг харуулав.



1-р зураг .Өгөгдлийн нууцлал болон өгөгдлийн аюулгүй байдлын ялгаа

В) Өгөгдөлд суурилсан халдлагууд (Data Breach, Re-identification attacks)

Өгөгдлийн аюулгүй байдлыг хамгаалах нь өнөөдрийн дижитал эринд чухал асуудал болоод байна. Өгөгдлийн алдагдал (Data Breach) гэдэг нь зөвшөөрөлгүй хэрэглэгчид өгөгдөлд хандах, ашиглах, задруулах, өөрчлөх, устгах зэрэг үйлдлүүдийг хийхэд хүргэдэг аюул юм. Энэ нь ихэвчлэн сүлжээний аюулгүй байдлын сул талыг ашиглан хийгддэг бөгөөд дотоод болон гадна халдлагаар хийгдэж болно.

Том компаниуд, эрүүл мэндийн байгууллагууд өгөгдлөө алдах үед хэвлэл мэдээллийн салбарынхны анхаарлыг ихэд татдаг . Энэ нь сүлжээний болон протоколын сул тал,ажилтны хайхрамгүй байдлыг ашиглан хэн нэгэн зөвшөөрөлгүй этгээд нэвтэрч зөрчил гаргадаг үйлдэл юм.

Дахин таних халдлага (Re-identification attacks) нь тодорхойлох боломжгүй болгосон өгөгдлийг дахин идэвхжүүлэн, хувийн мэдээллийг нээхийг хэлнэ. Энэ нь өгөгдлийг нууцлах зорилгоор нууцалсан байсан ч, халдагчид тухайн хүний талаарх мэдээллийг ашиглан дахин идэвхжүүлэх санаатай үйлдэл юм.

Дахин таних халдлага нь прокурорын аюул (prosecutor risk), сэтгүүлчийн аюул (journalist risk), маркетерын аюул (marketer risk) гэсэн гурван төрөл байна. Прокурор болон сэтгүүлчийн хувилбарт хоёуланд нь халдлага үйлдэгч тодорхой зүйлийг дахин тодорхойлохыг оролддог бол маркетерийн хувилбарт халдагч нь аль болох олон хүнийг дахин тодорхойлохыг хүсдэг.

Дахин таних халдлага нь зөвхөн халдлагад өртсөн байгууллагад төдийгүй хувийн мэдээлэл нь алдагдсан хувь хүмүүст ноцтой эрсдэл учруулдаг. Хэрэв нэг хүн өгөгдлийн санд танигдвал түүнтэй холбоотой шинэ мэдээллийг илрүүлэх боломжтой болдог. Жишээлбэл, эрүүл мэндийн мэдээлэл алдагдсанаар нийгэмд ялгаварлан гадуурхаж болох юм.

Халдлагыг үйлдэгчид янз бүрийн шалтгаанаар дахин танихыг (Re-identification attacks) оролддог:

- Сониуч зангаасаа
-Хувийн ашиг хонжоо олохын тулд
-Чадвараа харуулахын тулд

энэ төрлийн халдлагыг хийдэг.

Дахин танигдах эрсдэлийг ойлгохын тулд тухайн өгөгдлийн өвөрмөц байдал (data’s uniqueness) болон боломжит халдлагын төрлүүдийг мэдэх шаардлагатай.Зөвхөн энэ халдагыг судалсан цуврал судалгааны ажил ч нийтлэгдсэн байна.

III . ХУВИЙН МЭДЭЭЛЛИЙН ТУХАЙ ,ХУУЛЬ ЭРХЗҮЙ ОРЧИН

Энэ бүлэгт бид хувийн мэдээлэл болон эмзэг мэдээлэл тухай ,түүнийг хэрхэн хамгаалах хууь эрхзүйн хүрээг авч үзнэ.Ингэсэнээр ямар мэдээллүүдийг хамгаалах ёстойгоо мэдэж авна.

Үндсэн ойлголт

А) Монгол улс болон бусад улсын хууль эрхзүй

Өнөө үед хувийн мэдээллийг хамгаалах 2 үндсэн арга байдаг. Эхний арга бол технологи ашиглан

хувийн мэдээллийг шифрлэх, масклах, шуум нэмэх,танигдахгүй болгох , хоёрдох арга нь хууль эрхзүй, бодлого журмаар зохицуулах арга юм . Зарим техник технологиор шийдэх боломжгүй асуудлыг хууль эрхзүйн аргаар зохицуулалт хийдэг. Хууль эрхзүй нь техник технологи цаг үетэйгээ зэрэгцэн шинэчлэгдэж байх шаардлагатай.

Монгол улсад 2021.12.17 өдөр батлагдсан “Хүний хувийн мэдээлэл хамгаалах тухай” хуулиар хүний хувийн болон эмзэг мэдээллийг цуглуулах, боловсруулах, ашиглах, аюулгүй байдлыг хангахтай холбогдсон харилцааг зохицуулж байна .

Харин олон улсын хамгийн алдартай өгөгдлийн хамгаалалтын

-Европын холбооны хууль “Ерөнхий мэдээллийг хамгаалах” хууль (GDPR),

-Калифорний мужийн “Хэрэглэгчийн нууцлалын тухай” хууль (CCPA),

-АНУ-ын “Хувийн эрүүл мэндийн мэдээллийн нууцлал тухай” хууль (PHI)

- АНУ-ын “Аюулгүй байдлыг зохицуулах” хууль (HIPAA) зэрэг хууль дүрэм бодлого журам хэрэгжиж байна.

Их өгөгдлийг үүсгэхдээ тэр дундаа хэрэглэгчийн хувийн мэдээлэл , хэрэглэгчийн эмзэг мэдээллийг ашиглах, боловсруулах, цуглуулахдаа “Нийтийн мэдээллийн ил тод байдлын тухай”, “Статистикийн тухай”, ”Гүйцэтгэх ажлын тухай хууль”, ”Хувь хүний мэдээлэл хамгаалах тухай ” болон салбарын хуулиудыг дагаж мөрдөж ажиллах шаардлага тулгарч байна .

Б) Хүний хувийн болон эмзэг мэдээллийн тухай

Монгол улс “Хүний хувийн мэдээллийг хамгаалах ” тухай хуулийн 4 дүгээр зүйлд хүний хувийн мэдээллийг дараах байдлаар тодорхойлсон байна. Үүнд:

- "хүний хувийн мэдээлэл" гэж хүний эмзэг мэдээлэл болон хүний эцэг /эх/-ийн нэр, өөрийн нэр, төрсөн он, сар, өдөр, төрсөн газар, оршин суугаа газрын хаяг, байршил, иргэний бүртгэлийн дугаар, хөрөнгө, боловсрол, гишүүнчлэл, цахим тодорхойлогч, хүнийг шууд болон шууд бусаар тодорхойлох, эсхүл тодорхойлох боломжтой бусад мэдээллийг;
- "хүний эмзэг мэдээлэл" гэж хүний үндэс, угсаа, шашин шүтлэг, итгэл үнэмшил, эрүүл мэнд, захидал харилцаа, генетик болон биометрик мэдээлэл, тоон гарын үсгийн хувийн түлхүүр, ял эдэлж байгаа болон ял эдэлсэн эсэх, бэлгийн болон хүйсийн чиг баримжаа, илэрхийлэл, бэлгийн харьцааны талаарх мэдээллийг
- "цахим тодорхойлогч" гэж хүнийг цахим орчинд тодорхойлох мэдээллийн системийн нэвтрэх нэр, цахим шуудан, нийгмийн сүлжээ, харилцаа холбооны утастай болон утасгүй технологийн хаяг, бусад төрлийн төхөөрөмж, мэдээллийн систем дэх мэдээллийг;
- "эрүүл мэндийн мэдээлэл" гэж хүний бие махбод, сэтгэцийн эрүүл мэнд болон эрүүл мэндийн тусламж, үйлчилгээ авсан тухай мэдээллийг гэж тус тус тодорхойлжээ.
- "хүнийг тодорхойлох боломжгүй болгох" гэж мэдээллийг тухайн хүнд хамааруулах боломжгүй болгохыг хэлнэ гэж хуульчилжээ.

Хүний болон хуулийн этгээдийн хувийн мэдээллийг тодорхойлох нь хүний хувийн мэдээллийг бүрдүүлдэг өгөгдлүүд болон аж ахуйн нэгж зэрэг хуулийн этгээдтэй холбоотой өгөгдлийг тодорхойлох явдал юм.

Монгол улсын хүний хувийн мэдээлэл хамгаалах тухай хуульд заасны дагуу хүнд хамаарах мэдээллийг 1-р хүснэгтээр тодорхойллоо.

***1**-Р ХҮСНЭГТ ХҮНИЙ ХУВИЙН МЭДЭЭЛЭЛД ХАМААРАХ ӨГӨГДӨЛ*

№	Ерөнхий мэдээлэл	Нарийвчилсан мэдээлэл
1	Хүний эцэг /эх/-ийн нэр	
2	Өөрийн нэр	
3	Төрсөн он, сар, өдөр	
4	Төрсөн газар	
5	Оршин суугаа газрын хаяг	-Гудамжны хаяг -Хот, аймаг -Дүүрэг, сум -Зип код
6	Байршил	- GPS координат - Байршлыг хянах өгөгдөл
7	Иргэний бүртгэлийн дугаар	- Регистрийн дугаар - Цэргийн бүртгэлийн дугаар - Татвар төлөгчийн дугаар - Сонгогчийн бүртгэлийн мэдээлэл
8	Хөрөнгө	- Банкны дансны дугаарууд - Зээлийн картын дугаарууд - Орлого, татварын мэдээлэл - Санхүүгийн гүйлгээний түүх
9	Боловсрол	- Боловсролын түвшин - Дүнгийн мэдээлэл
10	Гишүүнчлэл	- Улс төрийн үзэл бодол

11	Цахим тодорхойлогч	- IP хаяг - MAC хаяг - Нийгмийн мэдээллийн хэрэглийн хэрэглэгчийн нэр - Нэвтрэх итгэмжлэл - Хэрэглэгчийн нэр - Нууц үг - Аюулгүй байдлын асуулт, хариулт
12	Хүний үндэс, угсаа	
13	Шашин шүтлэг	
14	Итгэл үнэмшил	- Гүн ухааны итгэл үнэмшил
15	Эрүүл мэнд	- Эмнэлгийн бүртгэл - Эрүүл мэндийн даатгалын мэдээлэл - Эмийн жорын мэдээлэл - Эмчилгээний түүх
16	Захидал харилцаа	
17	Генетик	- Генетик мэдээлэл
18	Биометрик мэдээлэл	- Хурууны хээ - Нүүр царай таних өгөгдөл - Торлог бүрхэвч - Дууны өгөгдөл - ДНХ өгөгдөл
19	Тоон гарын үсгийн хувийн түлхүүр	
20	Эрүүгийн бүртгэл	- Ял эдэлж байгаа болон ял эдэлсэн эсэх
21	Бэлгийн болон хүйсийн чиг баримжаа	
22	Бусад	- Гэрэл зураг - Видео - Аудио бичлэг - Тээврийн хэрэглийн таних дугаар - Автомашины улсын дугаарын

“Нийтийн мэдээллийн ил тод байдлын тухай” хуульд нийтийн мэдээллийг нээлттэй, хязгаарлалттай, хаалттай гэж ангилсан. Тус хуулийн 7.3-т “Танилцах, ашиглахад хуулиар хязгаарлалт тогтоосон албаны нууц болон хүн, хуулийн этгээдэд хамаарах мэдээллийг хязгаарлалттай мэдээлэл гэж үзнэ.” гэж заасан нь "Хүний хувийн мэдээлэл хамгаалах тухай” хуульд тодорхойлсон хүний хувийн мэдээлэл нь энэхүү хязгаарлалттай мэдээлэлд хамаарч байна.

III. ӨГӨГДӨЛ ХАМГААЛАХ АРГУУД

Энэ хэсэгт бид хувийн мэдээллийг хамгаалах аргуудыг судлан өгөгдлийн эзнийг тодорхойлох боломжгүй болгох нууцлалын аргуудыг судална .

Үндсэн ойлголт

Өгөгдлийн эзнийг тодорхойлох боломжгүй болгоход анонимизаци (anonymization), псевдонимизаци(pseudonymization) гэсэн хоёр үндсэн аргыг ашигладаг. Эдгээр аргуудыг товч тайлбарлая.

А) Анонимизаци (anonymization) *хийх аргууд*

Анонимизацийн аргууд нь *х*увь хүнийг таних боломжгүй болгохын тулд хувийн мэдээллийг эргэлтгүйгээр устгах эсвэл өөрчлөх үйл явц юм.Зорилго нь мэдээллийг бүрэн аноним болгож, нууцлалын талаар санаа зовохгүйгээр чөлөөтэй ашиглах боломжтой болгох явдал юм.

1. Криптографын аргууд:
Нууц мэдээллийг эргэлтгүйгээр хувиргахын тулд криптографын хаш функцийг (SHA-256) ашиглах

SHA-256 нь оролтын өгөгдлөөс тогтмол хэмжээтэй 256 битийн хэш утгыг үүсгэдэг криптограф хэш функц юм. Өгөгдлийн талбаруудын хэшийг үүсгэхэд ашигладаг бөгөөд энэ нь өгөгдлийн нууцлал, бүрэн бүтэн байдлыг хангахын зэрэгцээ өгөгдлийг эзнийг таних боломжгүй болгоно.

2. Ерөнхийлөх (Generalization)

Энэ нь тодорхой утгуудыг илүү ерөнхий утгаар солихыг хэлнэ. Энэ аргыг нас, гэрийн хаяг, шашин шүтлэг зэрэг мэдээлэлд ашиглахад тохиромжтой.
Жишээ нь УБ, Налайх дүүргийн 1р хороо гэсэн хаягийг “Улаанбаатар” болгож харуулна.

3. *Маскинг (Masking)*

Өгөгдлийн зарим хэсгийг нуух, жишээлбэл нэр, регистрийн дугаар зэргийг хасах эсвэл өөрчлөх; Жишээ: "Батцэцэг" -> "Б**г"

4. Хуурмаг нэр ашиглах (Obfuscation)

Өгөгдлийн утгыг өөрчлөх замаар жинхэнэ өгөгдлийг илрүүлэх боломжийг бууруулах,өгөгдөл хамгаалахад утга учиртай нэрийг утгагүй эсвэл санамсаргүй тэмдэгтээр сольхыг хэлнэ.

Жишээ: "battsetseg" -> "Оюунаа"

5. Группжүүлэлт (Aggregation)

Хувь хүний өгөгдлийг нийтлэг бүлгүүдэд нэгтгэх Жишээ: 10-29 насны бүлэг, 50-59 насны бүлэг гэх мэт.

6. Давтагдашгүй түлхүүрүүд (Unique Keys)

Хувь хүний өгөгдлийг жинхэнэ нэр эсвэл таних тэмдэггүй давтагдашгүй түлхүүрээр орлуулах арга . Жишээ: "User12345

7. K-Anonymity

Бүртгэл бүрийг таних шинж чанаруудын хувьд хамгийн багадаа k-1 бусад бүртгэлээс ялгах боломжгүй гэдгийг баталгаажуулна.

8.L-Diversity

Эмзэг атрибут нь дор хаяж l сайн илэрхийлэгдсэн утгатай байх замаар k- Anonymity-г сайжруулдаг.

9.*Дифференциал нууцлал (Differential Privacy)*

Дифференциал нууцлал нь өгөгдөлд шуум нэмж, хувь хүний мэдээллийг бүдгэрүүлдэг. Дифференциал нууцлал нь өгөгдлийн ашигтай байдлыг хадгалахыг эрмэлздэг. Энэ нь ананимизацийн бусад аргуудаас ялгаатай нь өгөгдлийг бүрэн устгахгүйгээр нууцлах боломжийг олгодог.

Б) Псевдонимизаци (pseudonymization) хийх аргууд

Псевдонимизаци нь өгөгдлийн эх сурвалжийг тодорхойлох боломжийг бууруулах боловч зарим нөхцөлд дахин холбох боломжийг хадгалдаг арга юм. Энэ аргыг хэрэгжүүлэхдээ дараах аргуудыг ашигладаг:

1.Шинэчилсэн ID үүсгэх (Tokenization)

Эмзэг өгөгдлийг хувилсан ID эсвэл токенээр орлуулах арга юм.Буцаагаад токенизацийн системийг ашиглан оригинал өгөгдлийг сэргээж болдог учраас псевдонимизацийн аргад хамаарна. PCI DSS стандартын дагуу токен систем үүсгэж олно. Мөн токенжуулсан мэдээллийг шинэ нэр өгөх (Re-identification) аргаар давхар хамгаалж болдог .

3. Шифрлэлтийн аргууд

Өгөгдлийн сан дахь өгөгдлийн нууцлал, аюулгүй байдлыг хангахын тулд шифрлэлтийн алгоритмуудыг ашигладаг. Хамгийн түгээмэл хэрэглэгддэг шифрлэлтийн алгоритмуудыг товч тайлбарлая.

- Advanced Encryption Standard (AES)

AES нь үр ашиг, аюулгүй байдлын улмаас өргөн хэрэглэгддэг тэгш хэмт шифрлэлтийн алгоритм. Энэ нь 128, 192, 256 битийн түлхүүрийн уртыг дэмждэг. Энэ нь нэрээ нууцлах аргыг хэрэглэхээс өмнө хувийн таниулбар, санхүүгийн мэдээлэл, эрүүл мэндийн бүртгэл зэрэг эмзэг өгөгдлийг шифрлэхэд ашиглагддаг.

-Rivest–Shamir–Adleman (RSA)

RSA нь шифрлэх, тайлахад хос түлхүүр (нийтийн болон хувийн) ашигладаг тэгш хэмт бус шифрлэлтийн алгоритм. Энэ нь аюулгүй байдлыг найдвартай хангадаг боловч тооцоолол их шаарддаг.

Энэ нь 1978 онд MIT-ийн Рон Ривест, Ади Шамир, Леонард Адлеман нарын бүтээсэн бөгөөд өнөөдөр HTTPS, SSL/TLS, электрон гарын үсэг, шифрлэлт зэрэгт өргөн хэрэглэгддэг . Энэ нь аюулгүй, математик үндэслэлтэй арга юм. RSA нь орчин үеийн криптографийн суурь бөгөөд интернэтийн аюулгүй байдал, мэдээллийн нууцлалд голлох үүрэг гүйцэтгэдэг.

- Homomorphic Encryption

Энэ нь шифрлэгдсэн өгөгдөл дээр шифрийг тайлах шаардлагагүйгээр тооцоолол хийх боломжийг олгодог. Өгөгдлийн агуулах дахь өгөгдөлд дүн шинжилгээ хийх, боловсруулахад нууцлалыг хадгалах, эмзэг мэдээллийг нууцлахын зэрэгцээ шифрлэгдсэн байдлаар ажиллах боломжтой.

Homomorphic Encryption нь криптографын салбарт хувьсгал хийж буй технологи бөгөөд өгөгдлийн нууцлал, аюулгүй байдлыг шинэ түвшинд хүргэж байна.

Эдгээр аргачлалууд нь хувь хүний өгөгдлийг хамгаалахад тусалдаг бөгөөд мэдээллийн нууцлал, аюулгүй байдлыг хангахад чухал үүрэг гүйцэтгэдэг.

В) Хүвь хүнийг тодорхойлох боломжгүй болгох аргыг хэрэглээ

Өгөгдлийг хэрэглээ, ямар судалгаанд ашиглахаас хамааран хүн, хуулийн этгээдэд хамаарах мэдээллийг тодорхойлох боломжгүй болгох аргыг сонгон ашигладаг.

2-р хүснэгт-д хүнд хамаарах өгөгдөл, түүнийг тодорхойлох боломжгүй болгох аргуудыг жишээ болгон оруулаа.

2-Р ХҮСНЭГТ. ХҮНИЙ ХУВИЙН МЭДЭЭЛЭЛД ХАМААРАХ ӨГӨГДЛИЙГ ТОДОРХОЙЛОХ БОЛОМЖГҮЙ БОЛГОХ

№	Хүний хувийн мэдээллийн төрөл	Хэрэглэх арга
1.	Хүний үндэс, угсаа	Ерөнхийлөх
2.	Шашин шүтлэг	Ерөнхийлөх
3.	Итгэл үнэмшил	Ерөнхийлөх
4.	Эрүүл мэнд	Маск хийх Хуурмаг нэрээр солих K-anonymity Дифференциал нууцлал
5.	Захидал харилцаа	Ерөнхийлөх Маск хийх
6.	Генетик	Маск хийх Хуурмаг нэрээр солих K-anonymity Дифференциал нууцлал
7.	Биометрик мэдээлэл	Мэдрэмтгий хэсгийг арилгах, бүдгэрүүлэх, пикселизаци хийх
8.	Тоон гарын үсгийн хувийн түлхүүр	Устгах
9.	Ял эдэлж байгаа болон ял эдэлсэн эсэх	Устгах

10.	Бэлгийн болон хүйсийн чиг баримжаа, илэрхийлэл	Ерөнхийлөх
11.	Бэлгийн харьцааны талаарх мэдээллийг	Ерөнхийлөх
12.	Хүний эцэг /эх/-ийн нэр	Маск хийх Хуурмаг нэрээр солих
13.	Өөрийн нэр	Маск хийх Хуурмаг нэрээр солих
14.	Төрсөн он, сар, өдөр	Маск хийх
15.	Нас	Ерөнхийлөх K-Anonymity
16.	Төрсөн газар	Ерөнхийлөх
17.	Оршин суугаа газрын хаяг, байршил	Ерөнхийлөх
18.	Иргэний бүртгэлийн дугаар	Кодлох
19.	Регистрийн дугаар	Кодлох
20.	Татвар төлөгчийн дугаар	Хуурмаг нэрээр солих
21.	Банкны дансны дугаар	Хуурмаг нэрээр солих
22.	Нийгмийн даатгалын дугаар	Хуурмаг нэрээр солих
23.	Хөрөнгө	Suppression, L-diversity
24.	Боловсрол	Suppression, L-diversity
25.	Гишүүнчлэл	Suppression, L-diversity
26.	Мэдээллийн системийн нэвтрэх нэр	Кодлох
27.	Цахим шуудан	Маск хийх Хуурмаг нэрээр солих
28.	Нийгмийн сүлжээ	Маск хийх Хуурмаг нэрээр солих
29.	Харилцаа холбооны утастай болон утасгүй технологийн хаяг	Маск хийх Хуурмаг нэрээр солих
30.	Бусад төрлийн төхөөрөмж	Маск хийх Хуурмаг нэрээр солих
31.	Хүнийг шууд болон шууд бусаар тодорхойлох, эсхүл тодорхойлох боломжтой бусад мэдээлэл	Маск хийх Хуурмаг нэр
32.	Хүний бие махбод	K-Anonymity
33.	Сэтгэцийн эрүүл мэнд	K-Anonymity
34.	Эрүүл мэндийн тусламж үйлчилгээ авсан тухай мэдээлэл	Маск хийх
35.	Зураг	Мэдрэмтгий хэсгийг арилгах, бүдгэрүүлэх, пикселизаци хийх

IV. ХУВИЙН МЭДЭЭЛЭЛ ХАМГААЛСАН АРГУУДЫГ ТУРШСАН ТЕСТ

Тестийн орчин

Бид дараах тестийн орчныг үүсгэж туршилm хийж үзэв.

- Windows 10 үйлдлийн системтэй PC
- Visual Studio code 1.98.0
- Jupyter notebook extention 2.0
- Python 3.12.9
- Anaconda 24.11.0 программ суулгаж
- Pandas ,numpy, cx_oracle 8.3.0 pyodbc 5.2.0
- Hashlib (өгөгдлийг бүдгэрүүлэхэд)
- Uuid (pseudonymized unique code үүсгэхэд)

-cryptograhy (нууц түлхүүр үүсгэх,шифрлэх ,мэдээлэл тайлах) сангууд суулгав

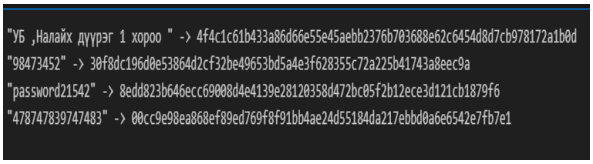
А) Анонимизаци хэш (Hash-256)

Энэ туршилт дээр гэрийн хаяг, утасны дугаар, нууц үг,банкны карт ийн мэдээлэл дээр python программын Hasklib сан ашиглан хэш (Hash) хийж үзэв.

Эхлээд anaconda ашиглан env нэртэй vitual орчин үүсгэж Visual Studio code editor дотор шинэ файл үүсгэн өргөтгөлийн hash.ipunb гэж нэрлэж хадгалав.Ингэснээр python дээр кодоо бичиж ажиллуулахад бэлэн болно.

Өгөгдлийн хэшлэхийн тулд

- Hasklib санг (import hasklib) оруулж ирж хэш функцуудйг ашиглах боломжтой болгов.
- hash_data (data_list) функц нь олон өгөгдөл (list) хүлээн авч, тус бүрийг SHA-256 алгоритмаар хэшлэв, Мөн hashlib сан бай өгөгдөлтэй ажилдаг учраас өгөгдлийн байт руу хөрвүүлсэн
- for давталтаар бүх өгөгдлийг хэшлэж, hashed_results сант (dictionary) хэлбэрээр хадгалав
- hexdigest() функц нь 16-тын тооллын (hex) хэш утгыг үүсгэв.
- Эцэст нь бүх хэшилсэн үр дүнг хэвлэж харсан.
- Үр дүн нь 5-р зурагт харуулав.



5-р зураг. Hash -SHA-256 аргын үр дүн

Б*) Ерөнхийлөх (Generalization)*

1*-р туршилтаар харахад гэрийн хаяг х дээр хэш* (Hash) *ашиглах тохиромжтой биш байна. Тиймээс* Ерөнхийлөх (Generalization) *аргыг ашиглая* . 6*-р зургаас ялгааг хараарай*

6-р зураг. Generalization аргын үр дүн

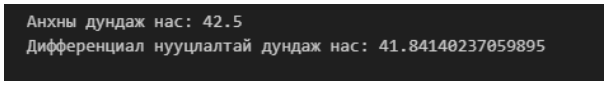
В) Masking болон permutation аргыг туршив

Дээрх 2 туршилтаас харахад Утасны дугаар дээр hash, generalization арга нь тохиромгүй харагдаж байгаа учраас утасны дугаар дээр mask аргыг ашиглаж үзсэн.Мөн хэрэглэгчийн нэр дээр permutation аргыг хэрэглэж үзэв.Үр дүнг 7р зургаас харна уу

7-р зураг. Mask болон permutation аргын үр дүн

Г) Дифференциал нууцлал(Differential Privacy)

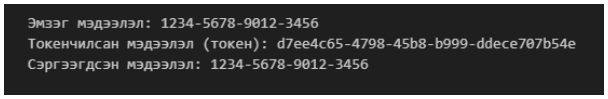
Энэ аргыг хэрэглэгчийн нас дээр туршиж үзэв.
Python программ дээр numpy сан ашиглав .
Лапласын (laplace) механизмыг ашиглан шуугиан (nose) нэмэв . Үүнд
Sensitivity =1 , epsilon=1.0 авав.
Үр дүнгийн 8-р зурагт харуулав



8-р зураг. Дифференциал нууцлал аргын үр дүн

Д) Псевдонимизаци аргуудаас Шинэчилсэн ID үүсгэх (Tokenization) аргыг туршиж үзэв

Ингэхдээ python дээр uuid сан оруулж ирж uuid() функцээр токен код үүсгэж , үүссэн токеноо ашиглан эмзэг мэдээллээ токенжуулж системд хадгалав. Эцэст нь токеноо ашиглан оргинал мэдээллээ сэргээв. 9-р зургаас үр дүнг харна уу



9-р зураг. Tokenization аргын үр дүн

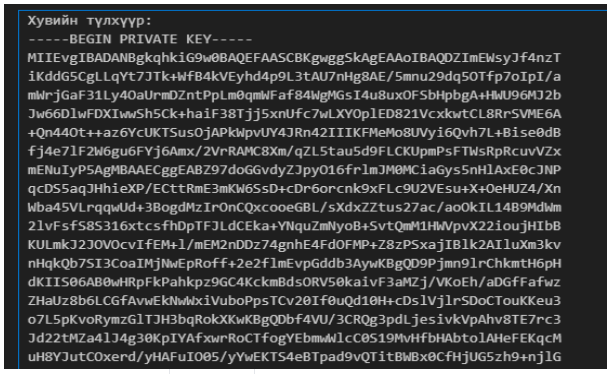
Е) Advanced Encryption Standard (AES) шифрлэлтийн аргыг туршиж үзэв.

Python программ дээр cryptography, os сан суулгаж AES зориулан 32 байт (256 бит) урттай түлхүүрийг urandom() функц ашиглан үүсгэв. AES нь блок шифрлэлт ашигладаг тул мэдээллийг 128 бит блок болгон хуваахын тулд PKCS7 padding нэмэв.Эцэст нь IV болон ciphertext-ийг нэгтгэв.Тайлах процесс нь эдгээр үйлдлийг буцааж хийнэ. Туршилтын үр дүнг 10 зургаас харна уу

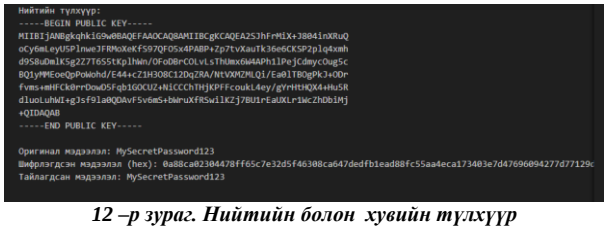
10-р зураг. AES шифрлэхт аргын үр дүн

Ё) Rivest–Shamir–Adleman (RSA) шифрлэлтийн аргыг туршиж үзэв.

RSA арга нь AES нэгэн адил cryptography санг ашиглав. Түүнчлэн RSA түлхүүрүүдийг rsa.generate_private_key() функцийг ашиглан үүсгээд
Хувийн болон нийтийн түлхүүрүүдийг PEM форматаар хадгалав. OAEP (Optimal Asymmetric Encryption Padding) схемийг ашиглан шифрлэлт хийв 11,12 р зургаас үр дүнг харна уу



11 –р зураг. 2048 бит RSA хувийн түлхүүр



12 –р зураг. Нийтийн болон хувийн түлхүүр

ДҮГНЭЛТ

Их өгөгдөлд хэрэглэгчийн өгөгдлийн хамгаалахдаа зорилго зориулалтаасаа хамаарч өгөгдөл нууцлалын аргуудаас сонгож ажиллах хэрэгтэй. Өөрөөр хэлбэл хэрэглэгчийг дахин тодорхойлох шаардлагагүй үед нэг талын хувиргалт хийдэг ананимазаци аргуудаас ашиглахыг санал болгож байна. Үүнд статистик бэлдэх,маркетинг эдийн засгийн тооцоолол хийх үед хувь хэрэглэгчийн мэдээлэл болон эмзэг мэдээллийг тэр бүр мэдэх шаардлагагүй.

Харин хэрэглэгчийг дахин тодорхойлох шаардлагатай үед хоёр талын хувиргалт хийдэг псевдонимизаци аргуудаас ашиглахыг зөвлөж байна. Магадгүй тагнуул, цагдаа шүүхийн байгууллагын ажилд сэжигтнийг илрүүлэхэд шаардлагатай байж болно.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] МУ Хүний эрхийн үндэсний комисс “Хүний хувийн мэдээллийг хамгаалах нь гарын авлага”. 2023

[2] МУ Төрийн ордон. “Хүний хувийн мэдээлэл хамгаалах тухай ” хууль . https://legalinfo.mn/. 2021.12.17

[3] МУ Төрийн ордон. “Нийтийн мэдээллийн ил тод байдлын тухай” хууль.https://legalinfo.mn/ . 2022.12.09

[4] МУ ЗГ . “Их өгөгдлийн(big data) сан үүсгэх тухай” тогтоол .https://legalinfo.mn/ . 2023.11.08

[5] MN Ухаалаг засаг төсөл. “МУ нээлттэй өгөгдлийн бэлэн байдал” судалгаа . 2018.08bruce schneier "data goliath". 2018

[6] David Salomon "Data privacy and security" New York 2003

[7] ENISA european union agency for cybersecurity "pseudonymisation techniques and best practices" pp.21-35 2019

[8] Privacy analytics a quintilesIMS company . "de-identificatopn 301" white paper 2017.

[9] Wei Ren, Lizhe Wang the institution of engineering and technology "Security and Privacy for big data,cloud computing and application" . chapter -8.3 .pp-187 .2019

ON APPLICATION DEVELOPMENT FOR A MONGOLIAN CONTEXT-FREE GRAMMAR

JONATHAN Sande[1], TUYATSETSEG Badarch[2], BALJINNYAM Tsevegmed[2]
School of Information, Communication Technology, Mongolia University of Science and Technology, Ulaanbaatar, Mongolia
Correspondence: tuyatsetseg.b@must.edu.mn

***Abstract*: This paper discusses the development process of one type of a future Mongolian grammar checker which has a context free feature. For our application development, we have chosen Flutter as the development framework, which supports publishing applications to Android, iOS, Mac, Windows, Linux and the web with a single code base. The paper presents the advantages of open-source development, and the application source code itself has been released to the public domain. The open source availability, multiplatform nature of Flutter, and ease of switching Mongolian for another language give the application value as a model for researchers and developers doing similar work for other languages.**

***Key words:* application, Flutter, Dart, Mongolian, context-free grammar, CFG, pushdown automata, PDA**

1. Introduction

Flutter has advantages for multiplatform support, quick feedback during development and the ability to compile to native code [1]. Flutter applications are written in Dart, which is an objected-oriented language and uses C-style syntax.

An important decision when developing an application is where that application will run. We chose Flutter as the application development framework. We believe that open-source development fosters innovation and collaboration. To that end, we released the source code to the public domain. The paper will give more reasons for that and about the license under which that was done. The application itself includes the functionality of both a CFG generator and also a PDA validator, which functions similarly to a grammar checker. There is also additional validation logic built in for more exhaustive sentence testing. The paper will describe the architectural structure of the app and how the logic and UI are implemented in Dart. Finally, it will show the results of what the app is and is not capable of doing.

2. Theoretical background

2.1 Application framework

Traditionally, software engineers have been limited to writing software to target a single platform, even a single type of hardware. Over the years, engineers have been able to generalize various processes to allow their software to run in more environments. For example, the C compiler allowed programmers to write the code once and then compile and run it on any hardware that had a C compiler. This abstracted away the necessity to write assembly code that would only run on a specific CPU architecture.

While programming languages have allowed a certain level of abstraction, in the world of graphical user interfaces (GUIs), it has still been necessary to develop software using different frameworks for different platforms. For example, if a company wanted to support Windows, Mac, and Linux, they would likely need to use different languages and different development frameworks for each of those platforms. With the arrival of Android and iOS smart phones, companies now had two more platforms that they needed to target if they wanted to reach all of their customers. One solution to this problem is a web application. Since Windows, Mac, Linux, Android, and iOS operating systems all come with web browsers, a company has the option to build a single web app. This app can then run in any browser on any platform. This has been a successful strategy for many companies; however, there are some drawbacks to this approach.

One drawback is that web apps are generally slow, especially if the page content is rendered on the server. Native apps, by comparison, are much more responsive to user input, usually showing near instantaneous feedback. Another drawback is that an internet connection is usually required. Native apps, on the other hand, are often functional offline. Finally, users need to remember a URL or perform a search in order to get to the application. Native apps, by comparison, have a homescreen launcher icon or menu item that is easily accessible.

Today there are a number of options that seek to solve the problem of multiplatform UI development. Two of the most popular ones are React Native and Flutter. React Native is a layer on top of the platform's native UI components and uses JavaScript as the programming language. The company behind React Native is Meta (formerly Facebook). While React Native is older than Flutter, Flutter has some unique advantages and has surpassed React Native in terms of popularity according to data from Stack Overflow Trends [2]:

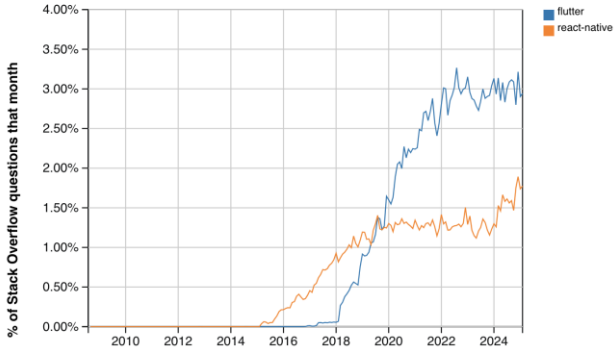


Figure 1. Stack Overflow Trends comparing Flutter and React Native through March 2025

Flutter is developed by Google and takes a different approach than React Native. Rather than wrapping native UI components, Flutter starts with a blank canvas and draws all of the UI elements (called widgets) itself. This gives the developer control over every pixel on the screen. If a developer doesn't like how a button looks, they are free to create a custom button matching their exact design specifications.

One of the most significant advantages of Flutter is that it supports Windows, Mac, Linux, Android, iOS, and web. It is often possible to have a single code base run on all of these platforms with only minimal configuration adjustments. The way Flutter achieves this is through a layered architecture. The following graphic comes from the Flutter documentation site [3]:

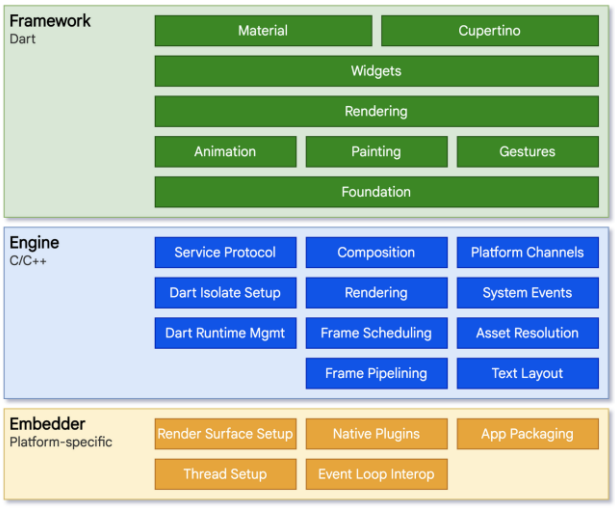


Figure 2. Flutter architecture

As you can see from Figure 2, there are three layers to the Flutter architecture. The top layer is the framework layer. This is the layer of UI widgets that developers interact with when they develop applications. The language that these UI components are written in and the language that developers use is Dart. There will be more about Dart below.

The next layer is the Flutter engine. This layer in written in C and C++ to handle various low-level tasks. For example, platform channels are the means by which messages are passed from the UI layer to the underlying platform. This can include things like communicating with underlying sensors and other hardware.

The third layer is where the multiplatform aspect is handled. This is the embedder layer and is different on every platform. It handles all of the platform specific logic so that the platform is able to talk to and render the platform-independent layers above. Supporting an additional platform with Flutter just means implementing a new embedder layer. In fact, Flutter is also supported on various embedded systems that have done just that. For example, Toyota built an infotainment system using an embedded version of Flutter [4].

Flutter apps are written in the Dart language. Dart had some very specific features that made it ideal for Flutter. One is that it supports both just-in-time (JIT) and ahead-of-time (AOT) compilation. For JIT compilation, this means that during development it is possible to get near-instant feedback. There is no need to wait minutes while the app compiles to see the new color the developer has chosen for a button. In Flutter development, this feature is known as "hot reload". However, when an app is ready for production, it is also possible to use AOT compilation to compile the app into a native executable for the target platform. Unlike JavaScript, which has the performance hit of needing an extra interpretation layer, Dart has the performance benefit of being able to run natively. Figure 3 from the Dart documentation illustrates this [5]:

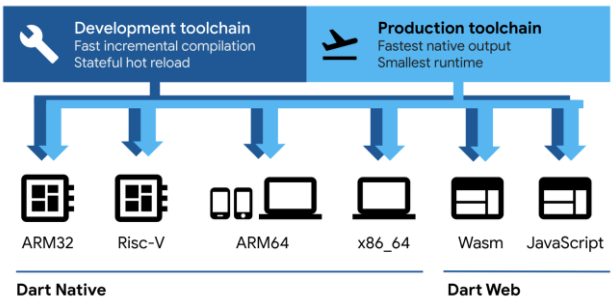


Figure 3. Dart JIT and AOT supported architectures

Dart is a relatively new language with its unveiling in 2011. Like Flutter, it is also developed by Google. It follows a C-style syntax that is generally quick to learn for developers coming from a background of Java or JavaScript. It is an object-oriented language but also incorporates some aspects of functional programming. It is a strongly typed language with sound null safety, which enables discovering many bugs at compile time rather than run time.

2.2 Open source

Another value in developing the application was making and using open-source software (OSS). Flutter and Dart are themselves open source. Unlike native development when working on a platform like iOS, where most of the source code is proprietary and hidden, the source code for Flutter and Dart is all on GitHub under an open-source BSD-3-Clause license. This means that development happens in the open, and developers outside of Google are encouraged to contribute to the code base.

While open-source is much better than closed-source software for the purposes of sharing and innovation, not all open-sources licenses are the same. Some licenses are known as “copyleft” [6], a play on the term copy*right*. Copyleft-licensed software requires derivative software to also remain open source and use the same license. Well known copyleft licenses are GNU General Public License (GPL) and GNU Lesser General Public License (LGPL) [7].

While it may seem great to make software and all of its derivatives open source, there are still problems with the copyleft or “share-alike” approach [8, 9, 10]. The main problem is that the very license that promises to give freedom restricts the freedom of the developer who is modifying the open-source software. That developer can’t use a different license. What if they want to borrow software from another source with a different restrictive license? The licenses are incompatible, and there is no way to combine them in a single derivative work.

There are more permissive licenses like MIT and Apache. However, even these require attribution. The software to the public domain gives the developer the maximum amount of freedom, which in turn stimulates innovation and further development. This should be the default in all of the sciences [11], but computer science can be a model.

Two primary ways to release a code base to the public domain are The Unlicense [12] and Creative Commons Zero (CC0) [13]. We’ve released the source code for the Mongolian CFG application under CC0 [14]. This puts the code in the public domain for maximum reusability by other researchers and developers.

One problem in the past for developers building Mongolian language applications is that a lot of language related data was guarded by prohibitive copyright restrictions. That meant that companies and researchers needed to create their own datasets. Thankfully, this appears to be changing as more and more Mongolian related datasets are being made available [15].

3. Implementation

3.1. Separation of concerns

In a Flutter project, there is a separate folder for each of the platforms that Flutter supports. As you can see from Figure 4, this project has folders for Android, iOS, Linux, macOS, web, and Windows.

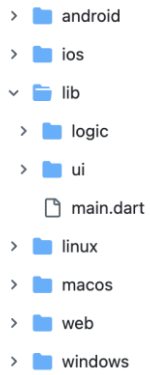


Figure 4. Project folder structure

The platform folders contain platform-specific logic needed to run correctly on the respective platform. For example, this is where you would set launcher icons or request security permissions. The application can generally run without modifying anything in these folders, but when publishing to any particular platform, at least a few small changes are required. For example, since we were publishing a public web version, we updated the configuration files in the **web** folder.

In addition to the platform folders, there is also a **lib** folder. This is where the application logic resides. Flutter gives you a lot of freedom in choosing how to architect your app. One of our architectural decisions was to separate the UI components from the business logic. In the app, that meant storing the code for the UI screens in the **ui** folder, and storing the code for the class models, CFG generator, and PDA parser in the **logic** folder. Such a separation of concerns makes it easier to find code and also easier to maintain the app in the future. For an app with many screens, it’s often better to group by feature.

3.2. Object-oriented

Since Dart is an object-oriented language, the CFG symbols were expressed with a `CfgSymbol` class. A symbol can be either terminal or non-terminal, so a Boolean was used for that distinction (Figure 5).

```
class CfgSymbol {
  const CfgSymbol(this.name, {this.isTerminal = false});
  final String name;
  final bool isTerminal;
```

Figure 5. Beginning of the CfgSymbol class

Similarly, the production rules were expressed using a `GrammarRule` class. A `GrammarRule`’s job is to link an input symbol with one or more output symbols. Since

there can be more than one, the expansion symbols were implemented as a list. For example, an input symbol for an ablative sentence may have a grammar rule with an expansion output of a nominative noun, an ablative noun and a verb. See Figure 6.

```
// Ablative Sentence
GrammarRule(CfgSymbol('AblativeSentence'), [CfgSymbol('NomNoun'), CfgSymbol('AblNoun'), CfgSymbol('Verb')]),
GrammarRule(CfgSymbol('AblNoun'), [CfgSymbol('Place'), CfgSymbol('-аас', isTerminal: true)]),
GrammarRule(CfgSymbol('AblNoun'), [CfgSymbol('RegularNoun'), CfgSymbol('-аас', isTerminal: true)]),
GrammarRule(CfgSymbol('Place'), [CfgSymbol('америк', isTerminal: true)]),
```

Figure 6. Terminal and non-terminal production rules for the ablative case grammar structure.

3.3. CFG generator

For the CFG generator, and for non-terminal symbols with more than one production rule, a random value was selected. Each iteration of the loop corresponded to one level in the tree, similar to a breadth-first traversal. When only terminal symbols remained, the algorithm was finished. The code is located in *cfg_generator.dart*.

3.4. Verification logic

It's possible to run the app and input various terminal symbols to see if they conform to the defined grammar. However, in order to be more systematic, we needed to verify all of the possible sentences. This was implemented with a nested loop. It iterates over every permutation of terminal sequence for length 1 up to the max length. Since the maximum possible sentence length that the rules supported was five terminals, this was the max length for the verification algorithm. For each sentence permutation, the parser checks the validity of the sentence.

3.5 Frontend and Backend

The app logic and data is self-contained within the Flutter project. For that reason, no REST API or other interface to a backend server was needed for the functionality of the application.

However, for publishing the app, we compiled a web version of the Flutter app and hosted the statically generated files on GitHub pages [16].

4. Application

The project was successful within its scope. Since Flutter was used, the app was built for four different platforms all while using the same code base. The tested platforms included Android, iOS, Mac, and web. Windows and Linux were untested, but there is no reason to believe that the application would not run identically on those platforms as well.

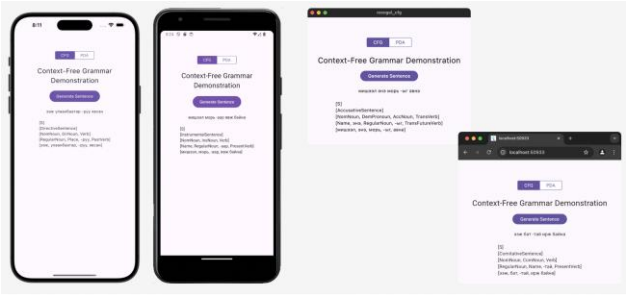


Figure 7. Mongolian CFG application running on (from left to right) iOS, Android, Mac, and Chrome (web)

In the sections that follow, we'll describe the data and then the limitations of the study.

This application was a proof-of-concept for creating a Mongolian CFG and PDA. To that end, it only used a handful of grammar rules and vocabulary words. It is unclear the effect that scaling the rules and words into the thousands would bring. One possible performance strategy would be to group terminal symbols into sets. Since checking member existence in a set has O(1) time complexity, this would save making multiple recursive branch calls for every terminal symbol.

The application is also not a complete grammar checker. A fuller solution would need a backend server that allows users to flag errors.

5. Conclusion

Development of the application has shown the necessary aspects required to build a Mongolian CFG and its related PDA sentence validation parser. The application has value to serve as an example for researchers and developers working on other languages. The source code [14] has been released to the public domain and we welcome others to use and improve on our foundation.

The application, while not itself a full-fledged grammar checker, shows potential as a starting point for building a grammar checking application. More testing and development will be needed with larger datasets. We hope others will be able to build on our modest foundation to achieve that goal.

6. References

[1] Flutter, "Flutter - Build for any screen," [Online]. Available: https://flutter.dev/. [Accessed: Apr. 16, 2025].

[2] Flutter vs. React Native, Stack Overflow Trends, 2025. [Online]. Available: https://trends.stackoverflow.co/?tags=flutter,react-native

[3] "Flutter architectural overview," Flutter, 2025. [Online]. Available: https://docs.flutter.dev/resources/architectural-overview

[4] Flutter, "Improving infotainment systems at Toyota with Flutter," Flutter Showcase, [Online]. Available: https://flutter.dev/showcase/toyota. [Accessed: Apr. 16, 2025].

[5] “Dart overview,” Dart, 2025. [Online]. Available: https://dart.dev/overview

[6] I. V. Heffan, "Copyleft: Licensing collaborative works in the digital age," Stanford Law Review, vol. 49, pp. 1487–1521, 1996.

[7] Free Software Foundation, "Licenses - GNU General Public License," GNU Project, [Online]. Available: https://www.gnu.org/licenses/#GPL. [Accessed: Apr. 16, 2025].

[8] D. Wiley, "Noncommercial isn’t the problem, ShareAlike is," Improving Learning, Jul. 16, 2007. [Online]. Available: https://opencontent.org/blog/archives/347. [Accessed: Apr. 16, 2025].

[9] V. S. Poythress, "The other shoe: Or, copyright and the reasonable use of technology," Frame-Poythress, Mar. 7, 2012. [Online]. Available: https://frame-poythress.org/the-other-shoe-or-copyright-and-the-reasonable-use-of-technology/. [Accessed: Apr. 16, 2025].

[10] V. S. Poythress, "Copyrights and copying: Why the laws should be changed," Frame-Poythress, Mar. 7, 2012. [Online]. Available: https://frame-poythress.org/copyrights-and-copying-why-the-laws-should-be-changed/. [Accessed: Apr. 16, 2025].

[11] J. Wilbanks, "Public domain, copyright licenses and the freedom to integrate science," J. Sci. Commun., vol. 7, no. 2, p. C04, Jun. 2008, doi: 10.22323/2.07020304.

[12] Unlicense, "The Unlicense," Unlicense.org, [Online]. Available: https://unlicense.org/. [Accessed: Apr. 16, 2025].

[13] Creative Commons, "CC0 1.0 Universal (CC0 1.0) Public Domain Dedication," Creative Commons, [Online]. Available: https://creativecommons.org/publicdomain/cc0/. [Accessed: Apr. 16, 2025].

[14] J. Sande, "Mongolian CFG/PDA," GitHub, 2025. [Online]. Available: https://github.com/suragch/mongol_cfg

[15] E. Tuguldur, Mongolian NLP Datasets, GitHub, 2024. [Online]. Available: https://github.com/tugstugi/mongolian-nlp

[16] J. Sande, "CFG Flutter application" GitHub Pages, [Online]. Available: https://suragch.github.io/apps/cfg/. [Accessed: Apr. 16, 2025].

МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ХӨГЖИЛ БА НОМЫН САНГИЙН ҮҮРГИЙН ӨӨРЧЛӨЛТ, ХАНДЛАГА

Цэрэн-Ойдовын БАЯНБИЛЭГ[1], Амарсайханы ТҮВШИНБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: bayanbileg.ts@must.edu.mn[1], tuvshinbayar@must.edu.mn[2]

***Хураангуй*: Мэдээллийн технологийн хөгжил дэвшил нь өнөөдөр номын сангийн орчин, бүтэц, үүрэг, үйлчилгээний загвар, хэрэглэгчийн хандлагыг үндсээр нь өөрчилж байна. Мэдлэг олж авах, түгээн дэлгэрүүлэх, хадгалах орчныг үндсээр нь өөрчилж, номын сангийн уламжлалт үүргийг дахин үнэлэх шаардлагатай болсон. Номын сангууд нь ном, сэтгүүл болон бусад эх сурвалжид хандах боломжийг олгодог мэдээллийн биет агуулах болж ирсэн түүхтэй. Гэсэн хэдий ч дижиталчлал, интернэт бий болсон нь мэдээллийн хаа сайгүй хүртээмжтэй байх эрин үеийг эхлүүлж, номын санг мэдлэгийн анхдагч эх сурвалж гэсэн уламжлалт ойлголтыг өөрчилж байна. Үүний хариуд номын сангууд гүн гүнзгий өөрчлөлтийг хийж, үйлчлүүлэгчдийнхээ хувьсан өөрчлөгдөж буй хэрэгцээ шаардлагад дасан зохицож, дижитал эрин зуунд хамааралтай хэвээр байхын тулд шинэ технологийг нэвтрүүлж байна. Хамгийн чухал өөрчлөлтүүдийн нэг бол цуглуулга төвлөрсөн загвараас татгалзаж, үйлчилгээнд чиглэсэн хандлага руу шилжих явдал юм. Энэхүү өгүүлэлд МХТС-ийн оюутнуудаас ном унших төлөв байдал, номын сангийн орчны тухай судалгаа авч, судалгааны үр дүнг боловсруулах, номын санг талаар дурдана.**

Түлхүүр үг:* Дижитал технологи, *үүлэн тооцоолол, чатбот

I. УДИРТГАЛ

Номын сангууд зөвхөн биет материал олж авах, хадгалахад чиглэхээ больсон бөгөөд хэлбэр, байршлаас үл хамааран мэдээлэл авах боломжийг улам бүр чухалчилж байна. Үүнд дижитал цуглуулгуудыг бэлтгэх, онлайн нөөцөөр хангах, технологид суурилсан олон төрлийн үйлчилгээг санал болгох зэрэг орно. Номын санчид одоо дижитал орчинд номын сан, мэдээллийн үйлчилгээг хөгжүүлэх, идэвхжүүлэх, зохион байгуулах чадвартай, өөрчлөлтийн агентууд болжээ. Номын сангууд дижитал нийгэмд бүрэн оролцоход шаардлагатай технологи, ур чадварт хүртээмжтэй байх боломжийг бүрдүүлж, дижитал оролцоог дэмжихэд чухал үүрэг гүйцэтгэж байна. Энэ нь дижитал технологид нэвтэрч, ур дүнтэй ашиглаж чаддаг хүмүүс болон ашигладаггүй хүмүүсийн хоорондох ялгааг илэрхийлдэг дижитал хуваагдлыг арилгахад онцгой чухал юм.

II. СУДАЛГААНЫ АЖЛЫН ЗОРИЛГО, ЗОРИЛТ

A. Судалгааны ажлын зорилго

Мэдээллийн технологийн хөгжил нь номын сангийн уламжлалт үйл ажиллагааг хэрхэн өөрчилж болох, мэдээллийн сан бүрдүүлэх, хадгалан хамгаалах, хүртээмжийг нэмэгдүүлэх, монголын номын сангийн хөгжлийн чиг хандлагыг тодорхойлж хиймэл оюун ухаан, IoT , Blockchain, үүлэн тооцоолол, чатбот зэрэг шинэ технологийг номын сангийн үйлчилгээнд нэвтрүүлэх боломжийг судлах юм.

Судалгааны хүрээнд МХТС-ийн оюутнуудын ном унших төлөв байдал, номын сангийн орчны талаар сэтгэл ханамжийн судалгаа авч, дүн шинжилгээг хийх, цаашид номын сангийн үйл ажиллагааг хэрхэн өөрчлөх шаардлагатай болохыг судалсан.

B. Судалгааны ажлын зорилт

- МХТС-ийн оюутнуудаас ном унших төлөв байдлын судалгаа авах
- МХТС-ийн номын сангийн орчны сэтгэл ханамжийн судалгаа авах
- Авсан судалгаанд дүн шинжилгээ хийх
- Цаашид номын сангийн үйл ажиллагааг мэдээллийн технологийн хөгжилд нийцүүлэн хэрхэн өөрчлөх боломжийг судлах

III. ОНОЛЫН ХЭСЭГ

Ном унших шаардлагын тухай судалгаа нь олон талаас хийгддэг бөгөөд түүний үр дүнд ном унших нь хүний оюун санааны хөгжлийг дэмжих, мэдлэгийн хүрээг тэлэх, сэтгэх чадварыг сайжруулах, амьдралын чанарыг нэмэгдүүлэхэд ач холбогдолтой гэж үздэг. Ном уншсанаар хүний тархи, сэтгэх чадварыг хөгжүүлэх, анализ хийх чадварыг сайжруулах, дэлхийн үзэл баримтлал, соёл, түүхийн тухай мэдлэгийг нэмэгдүүлэх, сэтгэл зүйн хувьд ч ур дүнтэй байдаг. Судалгаагаар ном унших нь тархины нейропластик шинж чанарыг сайжруулж, оюун санааны эрүүл мэндийг дэмжих, янз бүрийн сэдвээр өргөн мэдлэгтэй болгох, шинжлэх ухаан, урлаг, түүх, философи зэрэг олон салбарт ойлголттой болгох, зөв шийдвэр гаргах, асуудал шийдэх, логик ойлголттой байх, уншиж буй номын төрөл, агуулга нь стресс, түгшүүрийг бууруулах, сэтгэл санааг сайжруулахад туслах, уран зохиол, яруу найраг унших нь эмзэг сэтгэл зүйд дэмжлэг үзүүлэх гэх мэт олон талын чухал үүрэгтэй [1].

Номын сангийн хөгжил нь орчин үеийн технологийн нөлөөгөөр шинэчлэгдэж, цахим номын сангууд болон онлайн үйлчилгээний нөөцүүдийг өргөжүүлж байна. Цахим ном, өгүүлэл, видео контентууд нь мэдээллийг хурдан, хялбар хүлээж авах боломжийг хэрэглэгчдэд олгодог. Технологийн шинэчлэл нь номын сангийн үйлчилгээг автоматжуулах, хэрэглэгчийн хэрэгцээнд нийцүүлэн нэмэлт боломжуудыг нэвтрүүлэхэд чухал үүрэгтэй. Мөн номын сан нь зөвхөн ном хадгалах биш, суралцах, судалгаа хийх, мэдээлэл олж авах зэрэг олон үйл ажиллагааг хэрэгжүүлдэг. Номын сангийн хөгжлийг дэмжихийн тулд дижитал хөрөнгө оруулалт, онлайн сүлжээ, цахим каталог зэргийг ашигладаг. Ирээдүйд номын сангууд 3D хэвлэлт, виртуал бодит байдал (VR), хиймэл оюун (AI) зэрэг технологиор үйлчилгээгээ өргөжүүлж, хэрэглэгчдэд илүү дэвшилтэт үйлчилгээ үзүүлэх болно [2].

Номын сангийн орчин нь хэрэглэгчдэд ном, мэдээлэл, суралцах нөөцүүдийг ашиглах боломжийг олгодог тав тухтай, сэргэг орон зайг бүрдүүлнэ. Орчин үеийн номын сангууд нь технологийн шийдлүүдийг ашиглан цахим болон физик нөөцүүдийг нэгтгэсэн орчин бий болгодог. Хэрэглэгчид тухтай сууж унших, судалгаа хийх, цахим нөөцүүдтэй холбогдох боломжтой тохилог орчныг санал болгодог. Мөн номын сангийн орчин нь олон нийтийн соёл, боловсрол, хамтын ажиллагаа дэмжигддэг, тайван, бүтээлч сэтгэх орчныг бүрдүүлдэг.

Монгол улсад сүүлийн жилүүдэд номын сангийн үйл ажиллагаанд дараах өөрчлөлтүүд ажиглагдаж байна. Үүнд:

- Их дээд сургуулийн номын сангууд цахим каталог, цахим сан, Thesis сан нэвтрүүлж эхэлсэн (ж.нь. МУИС-ийн eLibrary.mn).
- Үндэсний номын сан дижитал шилжилт хийж, арвин их соёлын өвийг цахимжуулж байна.
- Нийтийн номын сангууд аажмаар RFID, автомат ном зээлдүүлгийн систем нэвтрүүлж эхэлсэн.
- Гэвч мэдээллийн технологийн хүртээмж, тоног төхөөрөмж, хүний нөөцийн чадавх харилцан адилгүй байдалтай байна.

IV. СУДАЛГААНЫ АЖЛЫН ҮР ДҮН

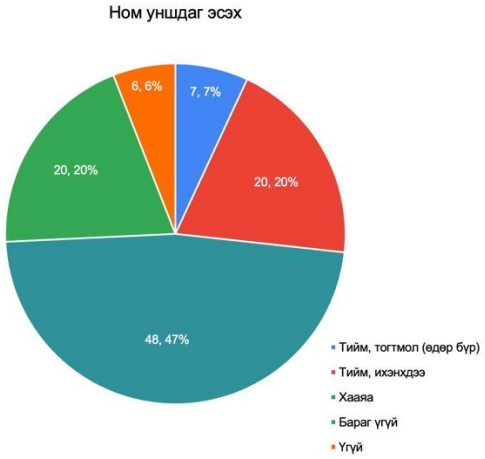
А. Ном унших төлөв байдлын судалгаа

Ном унших төлөв байдлын судалгаанд МХТС-ийн 101 оюутан оролцсон. Судалгааны асуулга нь 9 асуулттай бөгөөд судалгааны үр дүнгээс дараах 6 мэдээллийг олж авахыг зорив.

1. Нас (1-р асуулт)
2. Хүйс (2-р асуулт)
3. Ном уншдаг эсэх (3 – 6-р асуулт)
4. Номын тэмдэглэл хөтөлдөг эсэх (7-р асуулт)
5. Уншсан номын талаар хэлэлцүүлэг өрнүүлэх үйл ажиллагаанд оролцох эсэх (8-р асуулт)
6. Хэрэв ном унших, уншсан номын талаар хэлэлцүүлэг өрнүүлэх үйл ажиллагаанд оролцвол ямар зорилгоор оролцох эсэх (9-р асуулт)

Асуулт 3: Та ном уншдаг уу?

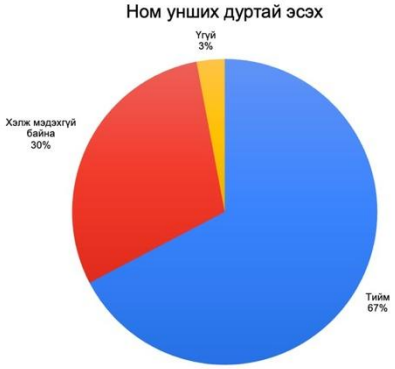
1-р зураг харуулснаар судалгаанд оролцогчдын 7% нь “Тийм, тогтмол (өдөр бүр)”, 20% нь “Тийм, ихэнхдээ”, 48% нь “Хаяа”, 20% нь “Бараг үгүй”, 6% нь “Үгүй” гэж хариулсан. Энд, “Хаяа”, “Бараг үгүй” гэж хариулсан оюутнуудыг хэдийгээр ном уншдаг ч тогтмол уншдаггүй гэж дүгнэж болно. Иймд, судалгаанд хамрагдсан оюутан залуусын 73% нь тогтмол уншдаггүй гэж дүгнэж болно.



1-р зураг. Асуулт 3: Та ном уншдаг уу?

Асуулт 4: Та ном унших дуртай юу?

2-р зураг харуулснаар судалгаанд оролцогчдын 67% нь “Тийм”, 30% нь “Хэлж мэдэхгүй байна”, 3% нь “Үгүй гэж хариулсан. Эндээс 33% нь одоогоор уншдаггүй, уншихад дурладаггүй гэж дүгнэж болох талтай.

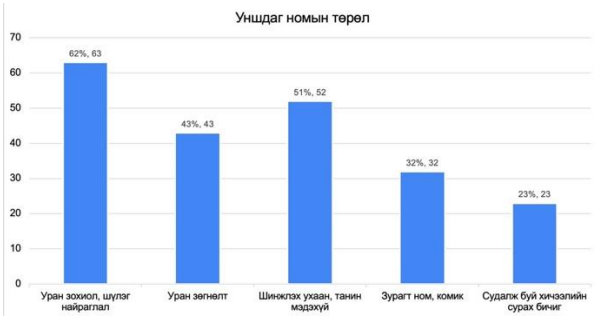


2-р зураг. Та ном унших дуртай юу?

Асуулт 5: Таны уншдаг номын төрөл

3-р зураг харуулснаар судалгаанд оролцогчдын 62% нь уран зохиол, шүлэг найраглал, 43% нь уран зөгнөлт ном, 51% нь шинжлэх ухаан, танин

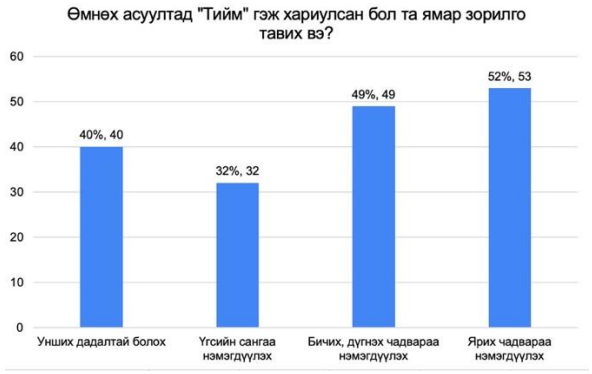
мэдэхүйн ном, 32% нь зурагт ном, 23% нь судалж буй хичээлийн ном, сурах бичгийг уншдаг гэж хариулсан. Эндээс, судалгаанд хамрагдсан оюутан залуусын ихэнх нь тодорхой хэмжээнд ном уншдаг гэж үзэж болно. Хэдийгээр 62% уран зохиол, шүлэг найраглалын ном уншдаг ч судалж буй хичээлийн холбогдох ном, сурах бичгийг 23% нь л уншиж байгаа нь хангалтгүй.



3-р зураг. Таны уншдаг номын төрөл

Асуулт 9: Хэрэв ном унших, уншсан номын талаар хэлэлцүүлэг өрнүүлэх үйл ажиллагаанд оролцвол таны зорилго юу вэ?

4-р зурагт харуулснаар судалгаанд оролцогчдын 40% нь “Унших дадалтай болох”, 32% нь “Үгсийн сангаа нэмэгдүүлэх”, 49% нь “Бичих, дүгнэх чадвараа нэмэгдүүлэх”, 52% нь “Ярих чадвараа нэмэгдүүлэх”гэж хариулсан. Энэ асуултын үр дүнгээс харахад, судалгаанд хамрагдсан оюутнууд ерөнхийдөө ихэнх нь дараах чадваруудыг бүгдийг нь сайжруулахыг хүссэн байна.



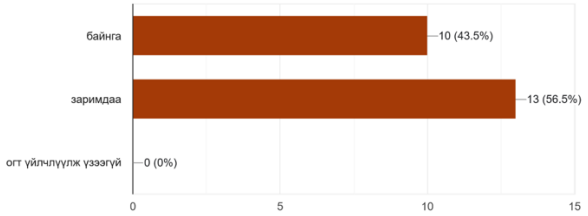
4-р зураг. Таны уншдаг номын төрөл

Е. Ном сангийн орчны судалгаа

Ном сангийн орчны сэтгэл ханамжийн судалгаанд МХТС-ийн 54 оюутан оролцсон. Судалгааны асуулга нь 11 асуулттай.

Асуулт 3: Та номын сангаар ямар давтамжаар үйлчлүүлдэг вэ?

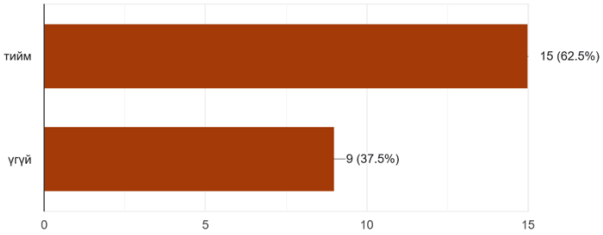
Танхимаар үйлчлүүлдэг оюутны тоо харьцангуй цөөн байгаа нь цахим хэрэглээ болон ном сурах бичгийн хүрэлцээтэй салшгүй холбоотой байж болох талтай.



5-р зураг. Та номын сангаар ямар давтамжтай үйлчлүүлдэг вэ?

Асуулт 5: Catalog.must.edu.mn электрон каталогийн хаягаар ном, сурах бичгийн хайлт хийж байсан уу?

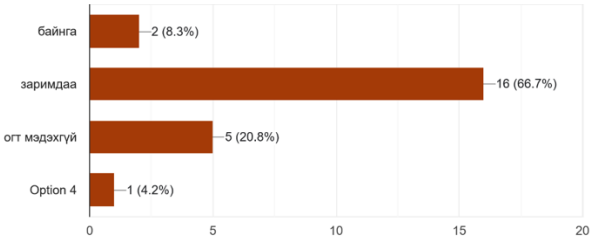
Нийт уншигчдын 62.5% нь электрон каталог ашигладаг гэсэн хариултыг сонгосон нь цаашид номын сангийн үүрэг, чиг хандлага өөрчлөгдөх шаардлагатай ба түлхүү цахим номын фондыг баяжуулах дээр анхаар ажиллах нь зүйтэй гэсэн дүгнэлтэд хүрч байна.



6-р зураг. Catalog.must.edu.mn электрон каталогийн хаягаар ном, сурах бичгийн хайлт хийж байсан уу?

Асуулт 6: Цахим номын сангаар ямар давтамжтай үйлчлүүлдэг вэ?

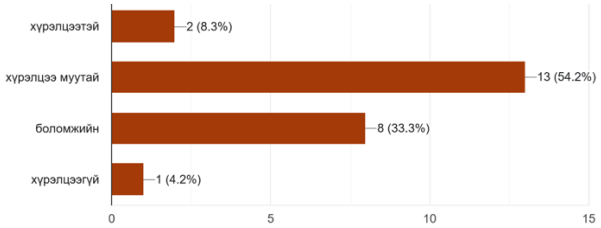
Цахимаар ном унших тал дээр байнга ордог- 8.3%, заримдаа-66,7% огт ордоггүй-20,8% энэ нь монгол хэл дээрх сурах бичиг харьцангуй цөөн байдаг учир хандалт бага байна гэж үзэж болно.



7-р зураг. Цахим номын сангаар ямар давтамжтай үйлчлүүлдэг вэ?

Асуулт 7: Номын сангийн ширээ сандал хэр хүрэлцээтэй вэ?

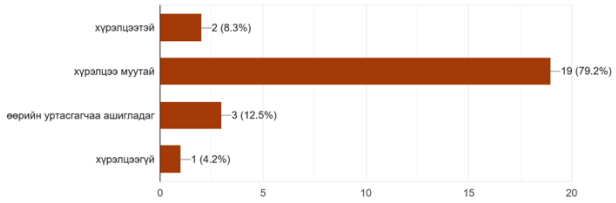
Судалгаанд хамрагдсан уншигчдын 54.2% нь хүрэлцээ муутай гэж хариулжээ. Үүнээс хүүхдүүдийн номын сангаар үйлчлүүлэх эрэлт хэрэгцээ байгааг харж болох юм.



8-р зураг. Цахим номын сангаар ямар давтамжтай үйлчүүлдэг вэ?

Асуулт 8: Залгуур, уртасгагч хэр хүрэлцээтэй байдаг вэ?

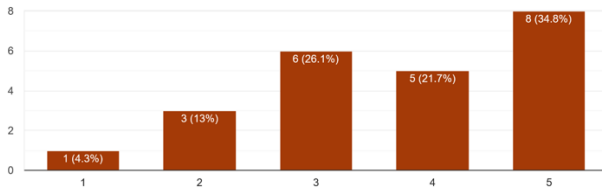
Судалгаанд хамрагдсан уншигчдын 79.2% нь саналаа өгсөн байгаа нь уншигчдын хэрэгцээг хангаж чадахгүй суралцах таатай орчин бүрдэхгүй байгааг харуулж байна.



9-р зураг. Цахим номын сангаар ямар давтамжтай үйлчүүлдэг вэ?

Асуулт 10: Номын санчдын харилцаа хандлагад үнэлгээ өгнө үү?

Номын санчдын харилцаа, хандлага нь номын сангийн үйлчилгээнд хамгийн чухал хэсэг бөгөөд энэ нь хэрэглэгчийн сэтгэл ханамж, өөрийн хүссэн үйлчилгээг авахад шууд нөлөөлдөг.



10-р зураг. Цахим номын сангаар ямар давтамжтай үйлчүүлдэг вэ?

F. Номын сангийн үйл ажиллагааг мэдээллийн технологийн хөгжилд нийцүүлэн хэрхэн өөрчлөх шаардлагыг судлах

Автоматжуулсан номын сангийн системүүд

Номын сангийн автоматаар номын мэдээллийг бүртгэх, хайх, зээлэх, буцаах, нөөцийг удирдах системүүдийг ашиглах. Хэрэглэгчдэд үйлчилгээний хурд, хүртээмжийг сайжруулж, номын сангийн ажилтнуудын цагийг хэмнэх боломжийг олгоно [3].

Интерактив сургалт, онлайн сургалтууд: Виртуал сургалт, онлайн лекцүүд болон сургалтын платформуудыг ашиглан номын сангийн хэрэглэгчдэд мэргэжлийн сургалт, семинар, вебинар зохион байгуулах. Суралцагчид болон хэрэглэгчид өөрийн орон зайнаас хамааран сургалтуудад оролцох боломжтой болох ба номын сан нь суралцах үйл явцад дэмжлэг үзүүлдэг [4].

Мобайл аппликейшн ашиглах: Номын сангийн үйлчилгээг мобайл аппликейшн ашиглан хүргэх, зээлсэн номоо цахимаар удирдах, мэдээллийн асуулга хийх. Хэрэглэгчдэд номын сангийн нөөцүүдэд амархан хандах боломж олгож, үйл ажиллагааг илүү хялбаршуулна [5].

RFID систем: Номын автомат бүртгэл, хамгаалалт, хадгалалтыг хялбаршуулж байна.

Cloud Computing: Мэдээллийг үүлэн орчинд хадгалах, хуваалцах, удирдах боломжийг бий болгосон.

Big Data ба Analytics: Хэрэглэгчийн зан төлөв, ашиглалтыг дүгнэхэд ашиглагдаж байна.

AI & Chatbot: Хэрэглэгчдэд 24/7 мэдээлэл өгөх, чиглүүлэх үйлчилгээнд ашиглагдаж байна.

Digital Archives & Repositories: Судалгааны бүтээл, ном, гар бичмэл зэргийг дижитал хэлбэрт оруулан хадгалж, хүртээмжтэй болгож байна.

Номын сангийн ирээдүйн хандлага: Номын сангийн ирээдүйд технологи, инновац, хэрэглэгчийн хэрэгцээг харгалзан үйл ажиллагаа үргэлжлэн хөгжих болно. Өнөөдөр хамгийн өргөн ашиглагдаж байгаа дижитал технологи нь ирээдүйд номын сангийн үйлчилгээний үндсэн тулгуур болж хувирна. Виртуал болон хийгээд бодит орон зайг холбосон шинэ технологиуд, мөн хиймэл оюун, 3D хэвлэлт, мэдээллийн сангийн автоматжуулалт зэрэг дэвшилтэт шийдлүүд нь номын сангийн үйл ажиллагааг улам хялбаршуулж, хэрэглэгчдэд илүү дэвшилтэт үйлчилгээ үзүүлэх болно. Иймээс номын сангууд илүү олон үйлчилгээг санал болгох, боловсрол, соёл, судалгааны төв болж, нийгмийн хөгжилд чухал хувь нэмэр оруулах болно.

ДҮГНЭЛТ

Оюутнуудын ном унших төлөв байдал, орчны сэтгэл ханамжийн судалгаанаас үзвэл хүний сурч мэдэх хэрэгцээ байгаа цагт сайн номын сан зайлшгүй байх шаардлагатай гэж үзэх болох юм. Иймд хүний хэрэгцээнд нийцүүлж, мэдээллийг товч бөгөөд хүртээмжтэй байлгахын тулд мэдээллийн технологийн хөгжлийг номын сангийн үйл ажиллагаатай хослуулах нь оновчтой зөв шийдэл гэж үзэж байна.

Цахим номын сангаар тогтмол үйлчлүүлэх дадалтай болгохын тулд мэдээллийн технологийг ашиглан онлайн сургалт явуулах, номын сангийн цахим номын сангийн мэдээллийн санг нэмэгдүүлэх, уншигч бүрд мэдээллийг хүртээмжтэйгээр хүргэх гээд олон зүйлийг технологийн хөгжлийг ашиглан хэрэгжүүлэх боломжтой юм. Уншигчдын олон талт хэрэгцээг хялбар аргаар шийдвэрлэх нь цаашид гарах үр дүнгийн гол үндэс суурь болж өгнө.

Мэдээллийн технологийн хөгжил нь номын сангийн үйл ажиллагаанд томоохон өөрчлөлтүүдийг авчирсан бөгөөд энэ нь хэрэглэгчдийн хэрэгцээг илүү хялбар, хурдан, хүртээмжтэй хангах боломжийг олгож байна. Номын сангуудын дижитал шилжилт, цахим номын сангууд, автоматжуулсан системүүд зэрэг нь үйлчилгээний хурд, нөөцийн зохион байгуулалтыг сайжруулсан. Мэдээллийн технологийг нэвтрүүлснээр номын сан нь улам олон хэрэглэгчдэд дэлхий даяар хандах боломжийг олгох бөгөөд боловсролын чанар, судалгааны үр дүнг нэмэгдүүлэх чухал үүрэг гүйцэтгэж байна.

Ирээдүйд номын сангууд илүү дэвшилтэт технологиудыг ашиглан хэрэглэгчдэд онцгой, шинэ үйлчилгээ санал болгох боломжтой бөгөөд энэ нь номын сангийн үүргийг боловсрол, соёл, мэдээлэл өгөх төв болж өргөжүүлэхэд тусална. Номын сангийн орчин үеийн технологиудыг нэвтрүүлснээр илүү сайн мэдээллийн менежмент, автоматжуулсан үйлчилгээ, цахим нөөцүүдийг санал болгох чадвартай болно.

Мэдээллийн технологийн хөгжил нь номын сангийн ирээдүйг улам бүр өөрчлөх бөгөөд энэ нь тэдний чадавхыг сайжруулж, хэрэглэгчдийн мэдээлэлд хандах эрхийг илүү өргөжүүлж, суралцах, судлах, мэдлэг олж авах үйл явцыг хялбаршуулна. Тиймээс, номын сангийн хөгжлийн стратеги нь технологийн шинэчлэлд суурилсан байх ёстой бөгөөд энэ нь түүний үүргийг гүнзгийрүүлж, нийгмийн хөгжилд чухал хувь нэмэр оруулах болно.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] https://mn.wikipedia.org/wiki/%D0%9D%D0%BE%D0%BC%D1%8B%D0%BD_%D1%81%D0%B0%D0%BD

[2] https://blog.pressreader.com/libraries-institutions/21st-century-library-evolution-timeline

[3] Lynch, C. A. (2003). The Role of Digital Libraries in the Digital Age. D-Lib Magazine.

[4] He, W., & Wei, X. (2018). Digital Libraries and Learning: Implications for Education. Springer.

[5] Bishoff, B. D. (2019). The Use of Mobile Applications in Libraries. Journal of Library Administration.

БАРАА МАТЕРИАЛЫН НӨӨЦ ТӨЛӨВЛӨЛТИЙН УХААЛАГ СИСТЕМ (MRP) -ИЙН ХӨГЖҮҮЛЭЛТ

Өмирзахын АЗАМАТ[1], Эрдэнэбатын БАТЦЭЦЭГ[2], Батдоржийн ЦЭРЭНЛХАМ[2], Бямбаагийн АЛТАНТУЯА[2], Бадарчийн ТУЯАЦЭЦЭГ[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын ухааны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: tuyatsetseg.b@must.edu.mn

***Хураангуй*: Smart MRP (Material Requirements Planning) систем нь барааны нөөцийн төлөвлөлтийг автоматжуулж, хангамжийн гинжин хэлхээг оновчтой удирдахад чиглэсэн дэвшилтэт систем юм. Энэхүү систем нь нийлүүлэлт, эрэлт, агуулахын түвшин, захиалгын урсгалыг динамик байдлаар удирдах боломжийг олгодог. Энэхүү системийг үр дүнтэй хэрэгжүүлснээр байгууллагууд хомсдол болон хэт их нөөцийн эрсдэлээс зайлсхийж, борлуулалт болон үйлдвэрлэлийн тасралтгүй ажиллагааг хангах боломжтой. Уг судалгааны ажлаар системийг бүрэн хөгжүүлж энгийн болон Машин сургалт, AI ашиглан оновчлол хийж аргуудыг судалж нэвтрүүлэхэд оршино.**

Түлхүүр үг: Smart MRP, Барааны нөөц, Борлуулалтын таамаглал, ABC, Дундаж борлуулалт, ML, LSTM

I. УДИРТГАЛ

Орчин үеийн үйлдвэрлэлийн болон худалдааны байгууллагуудын өрсөлдөх чадвар нь бараа материалын нөөцийн менежментээс шууд хамааралтай. Бараа материалын нөөц төлөвлөлтийн систем (Material Requirements Planning – MRP) нь байгууллагын агуулахын үлдэгдэл, барааны эргэлт, захиалгын төлөвлөлтийг оновчтой болгох, нийлүүлэлтийн сүлжээг оновчлох, зардлыг бууруулах стратегийн шийдэл юм. Энэхүү системийг үр дүнтэй хэрэгжүүлснээр байгууллагууд хомсдол болон хэт их нөөцийн эрсдэлээс зайлсхийж, үйлдвэрлэлийн тасралтгүй ажиллагааг хангах боломжтой.

MRP системийн үндсэн зорилго

- Түүхий эд, барааны нөөцийн үр ашигтай удирдлага – Захиалгын төлөвлөлт болон нөөцлөлтийг оновчтой хийх.
- Үйлдвэрлэлийн тасралтгүй ажиллагаа – Түүхий эдийн хангалтыг тасралтгүй байлгах замаар үйлдвэрлэлийг саатуулахгүй байх.
- Нийлүүлэлтийн сүлжээний удирдлага – Олон салбар, агуулахын нөөцийн уялдааг хангах.
- Зардлын оновчлол – Илүүдэл нөөцийг багасгаж, санхүүгийн эргэлтийг сайжруулах.

Тулгамдаж буй асуудал – Худалдааны компанийн хувьд бараагаа зөв удирдаж чадахгүй, зөв цагт зөв шийдвэр гаргахад боловсруулсан зөв мэдээллээр хангагдахгүй, realtime хяналт байхгүй, аль бараагаа илүү татаж, ямар барааны татан авалтаа зогсоох ёстой юм гэдгээ мэдэхгүй тодорхой бус явсан мөн татан авалтын хугацаагаа тооцоогүй, бүтээгдэхүүний хугацаа дуусах, борлуулалтаа таамаглахгүйгээр хэт их хэмжээний таталт хийх, уг шалтгаануудаар агуулахдаа бараануудаа устгалд оруулах гэх мэт асуудал нь тухайн байгууллага алдагдал хүлээх, дампуурах эрсдэлтэй. Эдгээр тулгамдсан асуудлуудыг ухаалаг MRP системийг хөгжүүлснээр шийдвэрлэх боломжтой. AI суурьтай MRP систем нь материалын нөөц төлөвлөлтийг ухаалгаар хийх боломжийг олгодог. AI загвар нь шийдвэрлэхээр зорьж байгаа асуудлаасаа хамаарч уламжлалт машин сургалт, гүн сургалт, оновчлолын алгоритм гэх мэт хиймэл оюуны техникүүдийг ашиглан хөгжигдөж байна. LSTM нь дараалсан өгөгдлийн таамаглалыг үр дүнтэй боловсруулахад зориулагдсан гүн сургалтын аргад суурилагдсан хөгжигддөг RNN сүлжээний нэг төрөл.

II. СИСТЕМИЙН ХӨГЖҮҮЛЭЛТ

Энэхүү системийг хөгжүүлэх ажлын хүрээнд процесууд тодохойлж тохиргооны цонхнууд хөгжүүлэх, турших, автоматжуулах цонхнууд хөгжүүлэх, математик загварчлал, өгөгдлийн шинжилгээ, машин сургалтын алгоритм ашиглах аргуудыг хослуулан хэрэгжүүлнэ.

Системийн боломжууд:

- Үлдэгдэл дууссан барааг анхааруулна.
- Үлдэгдэл анхааруулах түвшинд хүрсэн барааг анхааруулна
- Барааны захиалах тоог байршилаар тооцоолж харах боломжтой
- Гадаад болон дотоод татан авалт хийх боломжит хугацаа, тоог тооцох боломжтой
- Борлуулалтын мэдээллэл дээр үндэслэн барааны нөөцийг хянана
- Барааны үлдэгдэлийг бүх байршлаар зэрэг харах боломжтой
- Барааны үлдэгдэлийг бренд, бүлгээр харах боломжтой
- Барааны ABC тооцох
- Дундаж борлуулалт тооцох
- Худалдан авалт, захиалга санал болгох
- Машин сургалтын арга, AI судалж нэвтрүүлсэн байх

А. Үндсэн хөгжүүлэлт, судалгаа

- Smart MRP системийн хөгжүүлэлт болон хэрэглээний чиг хандлага
- Уламжлалт аргууд болох ABC, Дундаж борлуулалт аргачлалууд
- LSTM болон AI алгоритмуудыг нөөцийн удирдлагад ашигласан туршлага
- Борлуулалтын таамаглалын уламжлалт болон орчин үеийн аргачлалууд

B. Өгөгдөл цуглуулалт, бэлтгэл

- Өмнөх жилийн борлуулалтын мэдээлэл, нөөцийн түвшин, эрэлтийн өгөгдлийг судлах
- Агуулахын менежментийн системээс (WMS) болон ERP системээс өгөгдөл хандалт хийж
- Өгөгдлийг цэвэрлэх, ангилах, тренд болон улирлын хамаарал тодорхойлох

C. Таамаглалын математик загварчлал ба алгоритм боловсруулах

- Борлуулалтын таамаглалыг LSTM загвар ашиглан боловсруулах
- ABC шинжилгээг хэрэгжүүлж, бараа материалын ангилал хийх
- Дундаж борлуулалтын тооцоолол дээр үндэслэн захиалгын загвар боловсруулах

D. Туршилт ба загварын шалгалт

- LSTM загварыг сургалтын өгөгдөл дээр сургаж, бодит өгөгдөлтэй тааруулж турших [10][11]
- Борлуулалтын урьдчилсан таамаглалын нарийвчлалыг хэмжих
- Тохиргоо болон гиперпараметрийн оновчлол хийх (learning rate, batch size, epochs)[21]

E. Үр дүнгийн шинжилгээ ба харьцуулалт

- Машин сургалтын бусад аргуудтай харьцуулж, оновчтой шийдэл гаргах[17]
- Судалгааны үр дүнг дүрслэн үзүүлэх, график болон дүн шинжилгээ хийх
- Борлуулалтын таамаглал ба бодит өгөгдөлтэй харьцуулалт LSTM загвараар гаргасан таамаглал нь бодит өгөгдөлтэй хэрхэн нийцэж байгааг судлах нь чухал юм.

III. ТООЦООЛЛЫН АРГУУД

1. Уламжлалт аргууд

Энэ арга нь богино хугацааны төлөвлөлт хийхэд тохиромжтой бөгөөд цаг хугацааны энгийн таамаглал гаргах боломжтой.

A. ABC анализ

ABC анализ нь бараа материалын удирдлагад өргөн хэрэглэгддэг бөгөөд бараануудыг борлуулалтын дүнгээр нь A, B, C гэсэн 3 ангилалд хуваана:

- A ангилал – нийт борлуулалтын 70-80%-ийг бүрдүүлдэг хамгийн чухал бараанууд.
- B ангилал – нийт борлуулалтын 15-25%-ийг бүрдүүлдэг дунд зэргийн чухал бараанууд.
- C ангилал – нийт борлуулалтын 5%-ийг бүрдүүлдэг бага чухал бараанууд.

B. Дундаж борлуулалтын арга

Дундаж борлуулалтын арга нь тодорхой хугацааны дундаж борлуулалтыг тооцоолох энгийн боловч үр дүнтэй арга юм. Энэ нь улирлын болон жилийн борлуулалтын хэлбэлзлийг тодорхойлоход ашиглагддаг.

Дундаж борлуулалтыг дараах томьёогоор тооцоолно:

$$\text{Дундаж борлуулалт} = \frac{\sum_{i=1}^{n} S_i}{n}$$

S_i- тухайн хугацааны борлуулалт,
n - хугацааны интервалын тоо.

Энэ арга нь богино хугацааны төлөвлөлт хийхэд тохиромжтой бөгөөд цаг хугацааны энгийн таамаглал гаргах боломжтой.

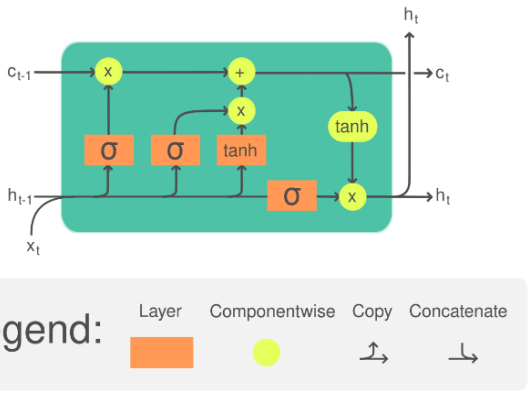
2. LSTM Загварын онолын томьёолол

LSTM (Long Short-Term Memory) [1] сүлжээ нь RNN (Recurrent Neural Network)-ийн сайжруулсан хувилбар бөгөөд санах ой (cell state)[2] ашиглан урт хугацааны хамаарлыг хадгалдаг[4]. Энэхүү аргыг борлуулалтын таамаглал гаргах, цаг хугацааны өгөгдөлд шинжилгээ хийх, санхүүгийн урьдчилсан төсөөлөл гаргах зэрэг олон салбарт ашигладаг.[18]

Урт богино хугацааны ой санамж (LSTM)[1] нь уламжлалт RNN-д ихэвчлэн тулгардаг алга болох градиентийн асуудлыг[2] багасгахад чиглэгдсэн давтагдах мэдрэлийн сүлжээ (RNN) юм [5]. Цоорхойн уртад харьцангуй мэдрэмтгий байдаггүй нь бусад RNN, далд Марков загварууд болон бусад дараалсан сургалтын аргуудаас давуу талтай юм. Энэ нь RNN-д зориулсан богино хугацааны санах ойг хангах зорилготой бөгөөд энэ нь хэдэн мянган удаа үргэлжлэх боломжтой (ингэснээр "урт богино хугацааны санах ой").[1] Энэ нэрийг 20-р зууны эхэн үеэс хойш танин мэдэхүйн сэтгэл судлаачдын судалж ирсэн урт хугацааны ой санамж, богино хугацааны ой санамж ба тэдгээрийн хамааралтай зүйрлэн бүтээжээ.

LSTM загвар нь улирлын шинж чанартай өгөгдөл дээр уламжлалт статистик аргуудаас илүү сайн ажилладаг.[20][26] Таамаглалын нарийвчлалыг

нэмэгдүүлэхийн тулд LSTM-ийн hyperparameter-үүдийг оновчлох шаардлагатай (learning rate, batch size, epochs гэх мэт).[21]



1-р зураг. Урт богино хугацааны санах ой (LSTM) нь өгөгдлийг дараалан боловсруулж, цаг хугацааны туршид далд төлөвөө хадгалж чаддаг [19]

- Мартах хаалга (Forget Gate)[3]
  Энэ нь өмнөх мэдээллээс аль хэсгийг хадгалах, аль хэсгийг устгахаа шийддэг [1][4]

$$f_t = \sigma(W_f \cdot [h_{t-1}, x_t] + b_f)$$

f_t– тухайн үеийн мартах хаалганы утга,
W_t, b_f– жингийн матриц, өрөөсгөл (bias),
h_{t-1} – өмнөх үеийн далд төлөв (hidden state),
x_t– тухайн үеийн оролтын өгөгдөл,
σ– логистик сигмоид функц.

- Оролтын хаалга (Input Gate)[5]
  Шинэ мэдээллээс аль хэсгийг шинэчлэхээ шийддэг [17][18]

$$i_t = \sigma(W_i \cdot [h_{t-1}, x_t] + b_i)$$

$$\tilde{C}_t = \tanh(W_C \cdot [h_{t-1}, x_t] + b_C)$$

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t$$

i_t– тухайн үеийн оролтын хаалга,
$\tilde{C}_t$ – шинэ санах ойн төлөв,
C_t– шинэчлэгдсэн санах ойн төлөв.

- Гаралтын хаалга (Output Gate)[4][5][25]
  Одоогийн төлөвөөс ямар мэдээллийг гаралтад илгээхийг шийддэг

$$o_t = \sigma(W_o \cdot [h_{t-1}, x_t] + b_o)$$

$$h_t = o_t * \tanh(C_t)$$

o_t– гаралтын хаалга,
h_t– тухайн үеийн далд төлөв.

Эдгээр томьёонуудын тусламжтайгаар LSTM сүлжээ нь урт хугацааны хамааралтай өгөгдлийг сурч, таамаглал гаргах боломжтой. Гэхдээ зөвхөн LSTM загварыг ашиглах нь үр дүнтэй бус байж болох тул уламжлалт аргууд болох ABC анализ болон дундаж борлуулалтын аргыг мөн хослуулан хэрэглэвэл илүү үр дүнтэй болно.[10][17]

3. LSTM-ийн давуу болон сул талууд

Давуу талууд:

- Урт хугацааны хамаарал сурах чадвартай. LSTM нь өгөгдлийн алс холын хамаарлыг сайн ойлгож, удаан хугацааны турш мэдээллийг хадгалах боломжтой.[21][13]
- Ванишинг градиент асуудлыг шийдвэрлэх: Сургалтын явц тогтвортой, урт дараалын өгөгдөл дээр үр дүнтэй ажилладаг.[24]
- Холбогдох мэдээллийг хадгалах чадвартай мөн мартах хаалгатай тул хэрэгцээгүй мэдээллийг устгаж, зөвхөн чухал мэдээллийг авч үлддэг.[8]
- Уян хатан чанар сайтай. Төрөл бүрийн урттай дарааллыг боловсруулж, цаг хугацааны динамик өөрчлөлтөд дасан зохицох чадвартай.[9][12]

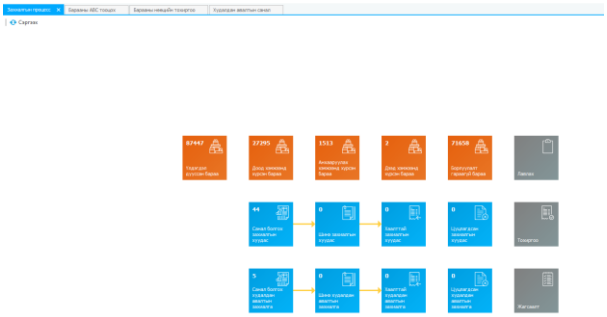
Сул талууд:

- Өндөр тооцооллын зардалтай. Нарийн бүтэцтэй тул RNN-ээс илүү GPU, их санах ой, тооцооллын хүч шаарддаг.[14]
- Оверфитинг хийх магадлал өндөр. Олон параметртэй тул их өгөгдөл[15] дээр хэт тохирч, шинэ өгөгдөл дээр буруу таамаг гаргах эрсдэлтэй.[22]
- Тайлбарлахад төвөгтэй. Дотоод үйл ажиллагаа нь “хар хайрцаг” мэт ойлгомжгүй, бизнесийн шийдвэрт шууд ашиглахад бэрхшээлтэй.[16]
- Сургалтын эмзэг байдал. Сургалтын тохиргооноос хамаарч тогтворгүй болох магадлалтай тул нарийн параметрийн тохируулга шаардлагатай.[19]

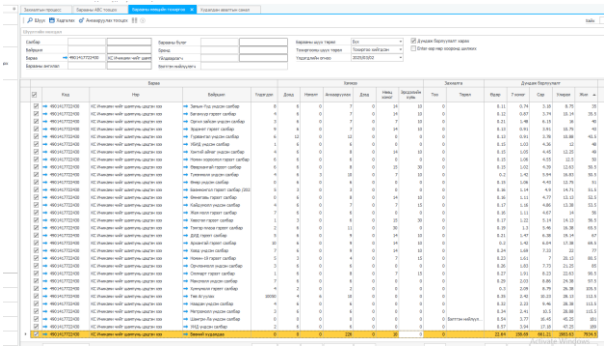
LSTM нь хүчирхэг ч, зөв тохируулахгүй бол ихээхэн нөөц шаарддаг тул практикт сайтар оновчлох шаардлагатай загвар юм.[11]

IV. ҮР ДҮН БА ХЭЛЭЛЦҮҮЛЭГ

Smart MRP системийг version 1 ийн хөгжүүлэлтийг хийж дуусгаж, ABC анализ болон борлуулалтын дунджаар таамаглах боломжийг бүрэн оруулсан ба борлуулалтын таамаглалыг LSTM загвар ашиглан боловсруулах судалгааны ажлууд хийж тодорхой туршилтууд хийж байгаа.



2-р зураг. Smart MRP системийн захиалгын процесийн дэлгэцийн зураг

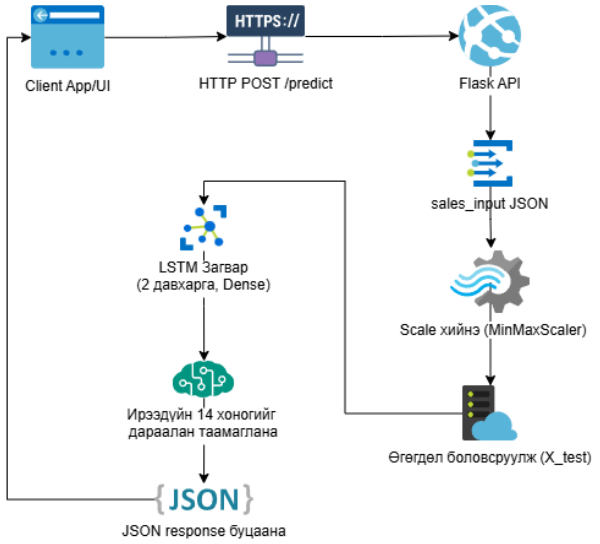


3-р зураг Smart MRP системийн бараан тохиргоо цонхны дэлгэцийн зураг

```
# LSTM загвар
model = Sequential([
    LSTM(50, return_sequences=True, input_shape=(look_back, 1)),
    LSTM(50),
    Dense(1)
])
model.compile(optimizer='adam', loss='mean_squared_error')

# Загварыг сургах
model.fit(X_train, y_train, epochs=50, batch_size=1, verbose=0)
```

4-р зураг. LSTM загвар үүсгэж сургаж байгаа хэсэг [27]

Судалгааны ажлын хүрээнд Python Flask ашиглан REST API хөгжүүлж, LSTM (Long Short-Term Memory) загварыг сургаж, ирээдүйн төлөв байдлыг таамаглах туршилтыг гүйцэтгэлээ. Энэхүү таамаглалыг Web Blazor UI дээр REST API ашиглан харуулж, үр дүнг шинжилсэн болно. Судалгааны үр дүнгээс харахад, LSTM загварын тохиргоог зөв оновчлох замаар таамаглалын нарийвчлалыг нэмэгдүүлэх боломжтой бөгөөд бодит өгөгдөлтэй өндөр хамааралтай үр дүн гаргах боломжтой[14] болох нь ажиглагдсан. LSTM загварын тохиргоог зөв оновчлох замаар таамаглалын нарийвчлалыг нэмэгдүүлэх боломжтой бөгөөд бодит өгөгдөлтэй өндөр хамааралтай үр дүн гаргах боломжтой.[6] [7][23]



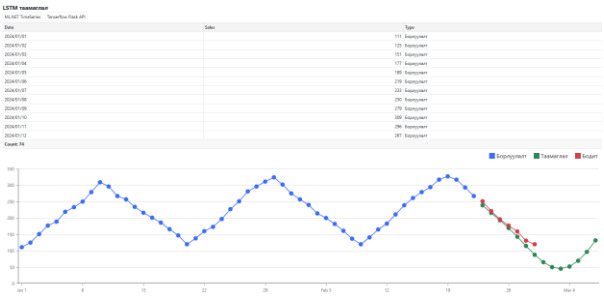
5-р зураг. Туршилт хийсэн системийн архитектур

Энэхүү судалгааны ажилд борлуулалтын өгөгдөл дээр суурилсан урьдчилсан таамаглалыг гаргах зорилгоор Python Flask ашиглан REST API үүсгэж, LSTM (Long Short-Term Memory) гүн сургалтын загварыг сургасан.

Архитектур нь дараах үндсэн бүрэлдэхүүн хэсгүүдтэй:

- **Flask сервер**: REST API горимоор ажиллаж, sales_input өгөгдөл хүлээн авна.
- **LSTM загвар**: Keras ашиглан 2 давхаргатай LSTM болон 1 гаралтын Dense давхаргатай загвар үүсгэн, урьдчилсан борлуулалтын таамаглал гаргана.
- **MinMaxScaler**: Борлуулалтын өгөгдлийг 0-1 хооронд масштабжуулж, нейроны сургалтын үр дүнг сайжруулдаг.
- **Таамаглал хийх логик**: Сүүлийн 30 хоногийн өгөгдөлд тулгуурлан 14 хоногийн борлуулалтыг нэг бүрчлэн дараалан таамаглах итератив арга ашигласан.

Загварын сургалтыг API-ийн дотор хийж байгаа бөгөөд цаашид model.save() болон load_model() ашиглан **загварыг хадгалах**, сургалтыг дахин хийхгүйгээр хурдан таамаг гаргах боломжтой.



6-р зураг. . LSTM загвараар хийсэн туршилтын үр дүн хэсгээс.

Туршилт: Өссөн → буурсан → дахин өссөн хэлбэлзэл.

Оролт: [111, 125, 151, 177, 189, 219, 233, 250, 279, 309,
296, 267, 257, 234, 216, 201, 186, 166, 147, 120,
138, 160, 173, 197, 227, 251, 281, 296, 311, 324,
302, 275, 257, 240, 214, 200, 182, 161, 137, 120,
141, 165, 183, 211, 239, 261, 279, 294, 317, 327,
317, 293, 267]

- Эхэндээ **тогтвортой өсөлттэй**
- Дараа нь **огцом буурсан**
- Дараа нь **дахин өсөж хэлбэлзсэн** өгөгдөл

Үр дүн: [238.93, 220.84, 202.12, 181.16, 157.11, 130.81, 104.8]

RMSE (Root Mean Squared Error): 16.14
MAPE (Mean Absolute Percentage Error): 9.4%

LSTM загвар нь хэлбэлзэлтэй, уналт-өсөлт давтагддаг өгөгдөл дээр харьцангуй сайн нарийвчлалтай таамаглал гаргасан байна. MAPE нь 9.4% байгаа нь “маш сайн” гэж үздэг <10% ангилалд багтана.

RMSE нь 16.14 байгаа нь бодит утгуудын хажууд (доод утга 111, дээд утга 327) харьцангуй бага гэж үзэж болно. Загвар том зөрүүтэй утгуудыг төвөггүй даван гарч, дундаж чиг хандлагыг сайн барьж байна.

ДҮГНЭЛТ

Уламжлалт аргууд болох ABC, Дундаж борлуулалт аргачлалууд нь тодорхой хэмжээнд системийн хэрэглээг хялбаршуулж байгаа ч гэсэн илүү олон гар ажиллагаанууд орж байна.

Энэхүү судалгаагаар уламжлалт аргууд болон LSTM загварыг хослуулан Smart MRP системийг хөгжүүлж, борлуулалтын таамаглалыг илүү нарийвчлалтай хийх боломжтойг нотолж чадлаа. Туршилтын үр дүн нь энэхүү AI суурьтай системийн хэрэгцээ, үр ашиг өндөр байгааг харуулсан. Цаашид өгөгдлийн төрөл болон гүн сургалтын архитектурын нарийвчлалыг нэмэгдүүлснээр улам нарийн, хурдан, найдвартай загвар бий болгох боломжтой.

LSTM загвар нь удаан хугацааны дараалсан өгөгдөл дэх хамаарлыг сурч, цаг хугацааны цувааны таамаглалд өндөр гүйцэтгэл үзүүлдэг орчин үеийн гүн сургалтын арга юм[6]. Давуу талуудынхаа хүчээр LSTM нь борлуулалтын төлөвийг таамаглах, нөөцийн түшинг оновчтой удирдахад өргөн хэрэглэгдэж байна. Гэхдээ нарийн төвөгтэй байдал, тооцооллын өндөр шаардлага зэрэг сул талууд нь практикт хэрэгжүүлэхэд тодорхой хүндрэл үүсгэж болохыг анхаарах хэрэгтэй. Мөн цаашид баярыг өдөр, амралтын өдөр, ирэх жил борлуулалт маркетингийн ажлаа идэвхжүүлж борлуулалтыг тэдэн хувь нэмэгдүүлэх гэх мэт зорилтын хүрээг тусгаж таамаглалыг илүү нарийн түвшинд хийхийг зорин судалгааны ажлуудаа хийж байна.

Цаашид Smart MRP системийг LSTM болон AI ашиглан улам нарийвчлалтай хөгжүүлэх нь үйлдвэрлэл, худалдааны байгууллагуудын нөөц төлөвлөлтийг оновчтой болгож, өрсөлдөх чадварыг нэмэгдүүлэх чухал арга зам болох юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Sepp Hochreiter; Jürgen Schmidhuber (1997). "Long short-term memory". Neural Computation. 9 (8): 1735–1780. doi:10.1162/neco.1997.9.8.1735. PMID 9377276. S2CID 1915014.

[2] Hochreiter, Sepp (1991). Untersuchungen zu dynamischen neuronalen Netzen (PDF) (diploma thesis). Technical University Munich, Institute of Computer Science.

[3] Hochreiter, Sepp; Schmidhuber, Jürgen (1996-12-03). "LSTM can solve hard long time lag problems". Proceedings of the 9th International Conference on Neural Information Processing Systems. NIPS'96. Cambridge, MA, USA: MIT Press: 473–479.

[4] Felix A. Gers; Jürgen Schmidhuber; Fred Cummins (2000). "Learning to Forget: Continual Prediction with LSTM". Neural Computation. 12 (10): 2451–2471. CiteSeerX 10.1.1.55.5709. doi:10.1162/089976600300015015. PMID 11032042. S2CID 11598600.

[5] Graves, Alex; Fernández, Santiago; Gomez, Faustino; Schmidhuber, Jürgen (2006). "Connectionist temporal classification: Labelling unsegmented sequence data with recurrent neural networks". In Proceedings of the International Conference on Machine Learning, ICML 2006: 369–376. CiteSeerX 10.1.1.75.6306.

[6] Karim, Fazle; Majumdar, Somshubra; Darabi, Houshang; Chen, Shun (2018). "LSTM Fully Convolutional Networks for Time Series Classification". IEEE Access. 6: 1662–1669. arXiv:1709.05206. Bibcode:2018IEEEA...6.1662K. doi:10.1109/ACCESS.2017.2779939. ISSN 2169-3536.

[7] Wierstra, Daan; Schmidhuber, J.; Gomez, F. J. (2005). "Evolino: Hybrid Neuroevolution/Optimal Linear Search for Sequence Learning". Proceedings of the 19th International Joint Conference on Artificial Intelligence (IJCAI), Edinburgh: 853–858.

[8] Sak, Hasim; Senior, Andrew; Beaufays, Francoise (2014). "Long Short-Term Memory recurrent neural network architectures for large scale acoustic modeling" (PDF). Archived from the original (PDF) on 2018-04-24.

[9] Li, Xiangang; Wu, Xihong (2014-10-15). "Constructing Long Short-Term Memory based Deep Recurrent Neural Networks for Large Vocabulary Speech Recognition". arXiv:1410.4281 [cs.CL].

[10] Wu, Yonghui; Schuster, Mike; Chen, Zhifeng; Le, Quoc V.; Norouzi, Mohammad; Macherey, Wolfgang; Krikun, Maxim; Cao, Yuan; Gao, Qin (2016-09-26). "Google's Neural Machine Translation System: Bridging the Gap between Human and Machine Translation". arXiv:1609.08144 [cs.CL].

[11] Ong, Thuy (4 August 2017). "Facebook's translations are now powered completely by AI". www.allthingsdistributed.com. Retrieved 2019-02-15.

[12] Sahidullah, Md; Patino, Jose; Cornell, Samuele; Yin, Ruiking; Sivasankaran, Sunit; Bredin, Herve; Korshunov, Pavel; Brutti, Alessio; Serizel, Romain; Vincent, Emmanuel; Evans, Nicholas; Marcel, Sebastien; Squartini, Stefano; Barras, Claude (2019-11-06). "The Speed Submission to DIHARD II: Contributions & Lessons Learned". arXiv:1911.02388 [eess.AS].

[13] Mayer, H.; Gomez, F.; Wierstra, D.; Nagy, I.; Knoll, A.; Schmidhuber, J. (October 2006). "A System for Robotic Heart Surgery that Learns to Tie Knots Using Recurrent Neural Networks". 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems. pp. 543–548. CiteSeerX 10.1.1.218.3399. doi:10.1109/IROS.2006.282190. ISBN 978-1-4244-0258-8. S2CID 12284900.

[14] "Learning Dexterity". OpenAI. July 30, 2018. Retrieved 2023-06-28.

[15] Rodriguez, Jesus (July 2, 2018). "The Science Behind OpenAI Five that just Produced One of the Greatest Breakthrough in the History of AI". Towards Data Science. Archived from the original on 2019-12-26. Retrieved 2019-01-15.

[16] Stanford, Stacy (January 25, 2019). "DeepMind's AI, AlphaStar Showcases Significant Progress Towards AGI". Medium ML Memoirs. Retrieved 2019-01-15.

[17] Schmidhuber, Jürgen (2021). "The 2010s: Our Decade of Deep Learning / Outlook on the 2020s". AI Blog. IDSIA, Switzerland. Retrieved 2022-04-30.

[18] Calin, Ovidiu (14 February 2020). Deep Learning Architectures. Cham, Switzerland: Springer Nature. p. 555. ISBN 978-3-030-36720-6.

[19] Lakretz, Yair; Kruszewski, German; Desbordes, Theo; Hupkes, Dieuwke; Dehaene, Stanislas; Baroni, Marco (2019), "The emergence of number and syntax units in", The emergence of number and syntax units (PDF), Association for Computational Linguistics, pp. 11–20, doi:10.18653/v1/N19-1002, hdl:11245.1/16cb6800-e10d-4166-8e0b-fed61ca6ebb4, S2CID 81978369

[20] Klaus Greff; Rupesh Kumar Srivastava; Jan Koutník; Bas R. Steunebrink; Jürgen Schmidhuber (2015). "LSTM: A Search Space Odyssey". IEEE Transactions on Neural Networks and Learning Systems. 28 (10): 2222–2232. arXiv:1503.04069. Bibcode:2015arXiv150304069G. doi:10.1109/TNNLS.2016.2582924. PMID 27411231. S2CID 3356463.

[21] Gers, F. A.; Schmidhuber, J. (2001). "LSTM Recurrent Networks Learn Simple Context Free and Context Sensitive Languages" (PDF). IEEE Transactions on Neural Networks. 12 (6): 1333–1340. doi:10.1109/72.963769. PMID 18249962. S2CID 10192330.

[22] Gers, F.; Schraudolph, N.; Schmidhuber, J. (2002). "Learning precise timing with LSTM recurrent networks" (PDF). Journal of Machine Learning Research. 3: 115–143.

[23] Xingjian Shi; Zhourong Chen; Hao Wang; Dit-Yan Yeung; Wai-kin Wong; Wang-chun Woo (2015). "Convolutional LSTM Network: A Machine Learning Approach for Precipitation Nowcasting". Proceedings of the 28th International Conference on Neural Information Processing Systems: 802–810. arXiv:1506.04214. Bibcode:2015arXiv150604214S.

[24] Hochreiter, S.; Bengio, Y.; Frasconi, P.; Schmidhuber, J. (2001). "Gradient Flow in Recurrent Nets: the Difficulty of Learning Long-Term Dependencies (PDF Download Available)". In Kremer and, S. C.; Kolen, J. F. (eds.). A Field Guide to Dynamical Recurrent Neural Networks. IEEE Press.

[25] Fernández, Santiago; Graves, Alex; Schmidhuber, Jürgen (2007). "Sequence labelling in structured domains with hierarchical recurrent neural networks". Proc. 20th Int. Joint Conf. On Artificial Intelligence, Ijcai 2007: 774–779. CiteSeerX 10.1.1.79.1887.

[26] Graves, A.; Schmidhuber, J. (2005). "Framewise phoneme classification with bidirectional LSTM and other neural network architectures". Neural Networks. 18 (5–6): 602–610. CiteSeerX 10.1.1.331.5800. doi:10.1016/j.neunet.2005.06.042. PMID 16112549. S2CID 1856462

[27] https://www.tensorflow.org Google LLC

МИКРОСКОПЫН ДҮРСНЭЭС ENTEROBIUS VERMICULARIS-ИЙН ӨНДГИЙГ ГҮН СУРГАЛТ АШИГЛАН ИЛРҮҮЛЭХ НЬ

Тэгшээгийн ТҮВШИНСАЙХАН[1], Батжаргалын ДОЛГОРСҮРЭН[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: tegsheetuvshinsaikhan[1]

***Хураангуй*: Энэхүү судалгаагаар гүн сургалтын YOLOv8 алгоритмыг ашиглан микроскопын дүрснээс Enterobius vermicularis (цагаан хорхой)-ийн өндгийг автоматаар илрүүлж, тоолох загварыг боловсруулсан. Цагаан хорхой нь хүний гэдсэнд шимэгчлэн амьдарч, бохир гар, хувцас, ор дэрний хэрэгсэл зэрэг ахуйн хэрэглээний зүйлсээр дамжин амархан халдварладаг. Энэ нь бага насны хүүхдүүдийн дунд өргөн тархалттай, олон нийтийн эрүүл мэндэд сөргөөр нөлөөлдөг. Одоогийн оношилгооны арга нь микроскопоор шинжилгээ хийх замаар хүний нүдээр өндгийг илрүүлдэг бөгөөд энэ нь лабораторийн ажилтны туршлага, анхаарал төвлөрлөөс ихээхэн хамаарч, оношилгооны үр дүнд алдаа гарах эрсдэлтэй. YOLOv8 загварыг ашигласнаар энэхүү процессыг автоматжуулж, өндгийг илрүүлэн тоолох ажлыг хурдан, найдвартай гүйцэтгэх боломж бүрдэж байна. Ингэснээр оношилгооны нарийвчлал нэмэгдэж, хүний оролцоог багасган, халдварт өвчний эрт илрүүлэлт, хяналтад ахиц дэвшил гаргах нөхцөл бүрдэх юм. Судалгааны үр дүн нь зөвхөн эмнэлзүйн хэрэглээнд төдийгүй, анагаах ухааны дүрс боловсруулалтын цаашдын судалгаанд чухал ач холбогдолтой юм.**

Түлхүүр үг: Enterobius vermicularis, цагаан хорхойн өндөг, микроскопын дүрс боловсруулалт, гүн сургалт, YOLOv8, хиймэл оюун ухаан, эмнэлзүйн оношилгоо, дүрс танилт, автомат оношилгоо

I. УДИРТГАЛ

Enterobius vermicularis буюу цагаан хорхой нь хүний нарийн гэдсэнд шимэгчлэн амьдардаг бөгөөд дэлхий дахинд, ялангуяа бага насны хүүхдүүдийн дунд түгээмэл тархсан шимэгчийн халдвар юм. Энэхүү халдвар нь бохир гар, хувцас, ор дэрний хэрэглэл, тоглоом болон халдварлагдсан гадаргууд хүрэх замаар амархан дамждаг. Тиймээс цэцэрлэг, сургууль зэрэг олон нийтийн орчинд халдвар хурдацтай тархах эрсдэл өндөр байдаг. Халдвар авсан хүүхдүүдэд анусны орчмоор загатнах, тайван бус байдал, нойргүйдэл, хоолны дуршил буурах, хэвлийн зовиур зэрэг шинж тэмдэг илэрдэг. Гэвч оношилгоо хүндрэлтэй байдаг тул халдвар дахин сэргэх эрсдэл ихтэй.

Одоогийн байдлаар цагаан хорхойн өндгийг илрүүлэхэд дараах уламжлалт аргуудыг лабораторид өргөн ашигладаг. Үүнд:

1. Үзүүртээ хөвөнтэй мод ашиглан хошногоны хуниаснаас сорьц авах,
2. Грэхэмийн наалдуулагч туузын арга – тусгай тууз ашиглан сорьц авч, микроскопоор шинжлэх.

Гэвч эдгээр аргууд нь оношилгооны нарийвчлал хязгаарлагдмал, үр дүн нь лабораторийн ажилтны туршлагаас хамаарч ихээхэн хэлбэлздэг. Мөн сорьц шинжлэхэд олон цаг шаарддаг тул эмч, ажилтнуудад ядаргаа үүсгэж, анхаарал сарниж, оношилгоонд алдаа гарах магадлалтай.

Сүүлийн жилүүдэд хиймэл оюун ухаан, ялангуяа гүн сургалтын (deep learning) аргууд анагаах ухааны дүрс боловсруулалтын салбарт амжилттай нэвтэрч байна. Объект илрүүлэлтийн салбарт өндөр үр дүнтэйд тооцогддог YOLO (You Only Look Once) алгоритм нь зургийг бүхэлд нь нэг дор боловсруулж, тухайн объектын байршил болон ангиллыг нэгэн зэрэг таамагладаг нэгдсэн архитектуртай. Энэ нь илрүүлэлтийн хурдыг нэмэгдүүлж, нарийвчлалыг сайжруулах, хүний оролцоог бууруулах давуу талтай.

Энэхүү судалгааны зорилго нь YOLOv8 алгоритмыг ашиглан *Enterobius vermicularis*-ийн өндгийг микроскопын дүрсэн дээрээс автоматаар илрүүлэх, тоолох загвар боловсруулах явдал юм. Ингэснээр оношилгооны үр дүнг хурдан, үнэн зөв гаргах, хүний алдааг багасгах, өвчний эрт илрүүлэлт, хяналтыг сайжруулах нөхцөл бүрдэнэ. Уг аргачлал нь зөвхөн цагаан хорхойн халдварыг оношлохоос гадна бусад төрлийн шимэгчийн оношилгоонд өргөн ашиглагдах боломжтой тул анагаах ухааны судалгаа, эмнэлзүйн хэрэглээнд өндөр ач холбогдолтой юм.

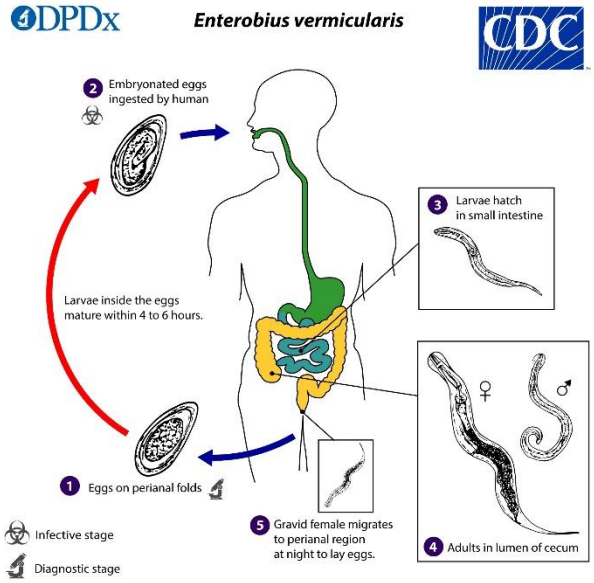
II. ОНОЛЫН ХЭСЭГ

Энтеробиоз нь дэлхийд хамгийн өргөн тархалттай шимэгчийн халдвар бөгөөд нийт халдварлагсдын 70-90%-ийг 5-12 насны хүүхэд эзэлдэг. [1] Д.Ганболд (1990) нарын судалгаагаар Улаанбаатар хотын хүн амын дунд E.vermicularis-ийн халдвар бусад гельминтозуудаас хамгийн их (40.2%) байсан бөгөөд тэдгээрийн 82.5%-ийг 4-7 насныхан эзэлж байжээ. [2] Судлаач Н.Гиймаа (2008) нарын судалгаагаар энтеробиозын тархалт 46.55±0.13% байжээ. [3] Дээрх судалгаануудаас харахад E.vermicularis-ийн халдварт бага насны хүүхдүүд илүү өртөж байгаа нь эрүүл ахуйн дадал бүрэн олж аваагүй, бие биедээ болон өөртөө эргэн халдварлуулах мөн өвчин

үүсгэгч хорхойн амьдралын мөчлөг улирлын ямар ч нөхцөлд идэвхтэй явагддаг, түүний тархалтын хүрээ харьцангуй их байгаатай холбоотой байна. Энтеробиоз нь нийгэм, соёл, арьс өнгө зэрэгтэй холбоогүй боловч нийгмийн эрүүл мэнд, хүн амын хэт төвлөрөл, ядуурал, ахуйн болон хувийн ариун цэвэр зэрэг хүчин зүйлүүд нөлөөлдөг. Түүнчлэн хүүхдүүдэд сандрах, тайван бус байх, цочромтгой болох, анхаарал сарниулах зэрэг хүүхдийн өсөлтөд нөлөөлдөг болохыг судлаачид нотолсон байна. [4]

2.1. ЦАГААН ХОРХОЙН АМЬДРАЛЫН МӨЧЛӨГ

Enterobius vermicularis буюу цагаан хорхой нь хүний гэдсэнд амьдардаг шимэгч хорхой юм. Энэ шимэгч нь голчлон нарийн гэдэс болон хошногоны орчимд амьдарч, эмэгчин цагаан хорхой нь хошногоны орчим өндөг гаргадаг. Эдгээр өндөг нь маш жижиг бөгөөд хүмүүсийн биед нэвтэрч халдвар үүсгэх чадвартай байдаг. Цагаан хорхойн халдварын эх үүсвэр нь зөвхөн хүн бөгөөд энэ шимэгчийн өндөг нь бохир гар, хувцас, ор дэрний даавуу, тоглоом зэрэг зүйлсээр дамжин хүнээс хүний биед нэвтэрдэг. Энэ нь халдвар авахад маш амархан бөгөөд тухайн хүний эрүүл ахуйн нөхцөл байдлаас шууд хамаардаг.



Зураг 2. Цагаан хорхойн амьдралын мөчлөг

1. **Өндөг гаргалт:** Нас бие гүйцсэн эмэгчин цагаан хорхой нь шөнө дундын үед хошногоны орчим руу шилжиж, тэнд өндгөө гаргадаг. Эдгээр өндөг нь хошногоны амсар дээр наалддаг.
2. **Халдвар дамжуулалт**: Халдвар дамжуулах нь хоёр үндсэн аргаар явагддаг:

- Өөрөө халдвар авах: Хүн хошногоны орчимд загтаж, хумсны завсраар өндөг нь гарт орж, дараа нь амаар дамжин биедээ шилждэг.
- Орчны өндгөөр халдвар авах: Өндөг нь бохир гадаргуу, хувцас, ор дэрний даавуу зэргээр дамжин бусад хүмүүст шилжиж болдог.

3. **Өндөгний боловсрол**: Хүний биед орсон өндөг нь нарийн гэдэс рүү шилжиж, 4-6 цагийн дотор личинк болж хувирдаг. Эдгээр личинк нь нарийн гэдсэнд боловсорч, насанд хүрсэн цагаан хорхой болдог.
4. **Насанд хүрэлт:** Насанд хүрсэн цагаан хорхой нь ихэвчлэн ходоодны хэсэгт (cecum) амьдардаг. Эрэгчин ба эмэгчин цагаан хорхойнууд тэндээ хосолж, эмэгчин нь өндөг гаргах бэлтгэлээ хийдэг.
5. **Өндөгний хөгжил:** Эмэгчин цагаан хорхой нь шөнө дундын үед хошногоны орчим руу шилжиж, өндгөө гаргадаг. Эдгээр өндөг нь 4-6 цагийн дотор боловсорч, халдвар үүсгэх чадвартай болдог.
6. **Амьдралын мөчлөгийн давталт:** Өндөг нь дахин хүний биед орж, амьдралын мөчлөгөө давтана. Энэ процесс нь хүмүүсийн хооронд халдвар хурдан тархахад хүргэдэг.

ДҮГНЭЛТ

YOLOv8 суурилсан автомат илрүүлэлтийн систем нь хүний цагаан хорхойн өндгийг микроскопын зургаас 91.8% нарийвчлалтай, 0.12 секундэд илрүүлж, оношилгооны хурд, үр ашиг, найдвартай байдлыг эрс сайжруулсан. Хэмжилтийн нарийвчлал 93.2%, F1-үзүүлэлт 92.5% байсан ба хуурамч эерэг (3.5%) болон хуурамч сөрөг (4.2%) үзүүлэлтүүд бага гарсан нь зөв оношт тавихад чухал нөлөөтэй. Энэхүү арга нь уламжлалт шинжилгээтэй харьцуулахад хурдан, тогтвортой, хүний алдаа багатай оношилгоог хийх боломжийг олгож, клиникийн хэрэглээнд тохиромжтой болохыг баталлаа.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. *arXiv preprint arXiv:1506.02640*.

[2] Redmon, J., & Farhadi, A. (2017). YOLO9000: Better, Faster, Stronger. *arXiv preprint arXiv:1612.08242*.

[3] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, Real-Time Object Detection. *arXiv preprint arXiv:1506.02640*.

[4] Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. *arXiv preprint arXiv:1804.02767*

[5] Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). YOLOv4: Optimal Speed and Accuracy of Object Detection. *arXiv preprint arXiv:2004.10934*.\

[6] Wang, C. Y., Bochkovskiy, A., & Liao, H. Y. M. (2021). Scaled-YOLOv4: Scaling Cross Stage Partial Network. *arXiv preprint arXiv:2011.08036*.

[7] Zhang, X., et al. (2020). Deep Learning for Microscopic Image Analysis: A Review. *IEEE Access*, 8, 182355-1

УХААЛАГ ТӨХӨӨРӨМЖИЙН АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛ, БУУРУУЛАХ АРГА ЗАМ

Батчулууны ЖАВХЛАНТӨГС[1], Дондогмэгдийн БЯМБАДОРЖ[2], Бат-Эрдэнийн МӨНХБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургуулийн, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: javkhlantugsb@must.edu.mn

Хураангуй-Зүйлсийн интернэт (IoT) төхөөрөмжүүдийн хэрэглээ өргөжихийн хэрээр тэдгээрийн аюулгүй байдалтай холбоотой эрсдэлүүд нэмэгдэж байна. Эдгээр төхөөрөмжүүд нь мэдээллийн хулгай, сүлжээний халдлага, программ хангамжийн эмзэг байдал зэрэг олон төрлийн аюул заналхийлэлд өртөх магадлалтай. Мэдээллийн хулгай нь хэрэглэгчийн хувийн болон санхүүгийн мэдээлэл алдагдах, улмаар хууль бус үйл ажиллагаанд ашиглагдах эрсдэлийг үүсгэдэг. Сүлжээний халдлагаар халдагчид IoT төхөөрөмжүүдийг ашиглан үйлчилгээний саатал үүсгэх, ботнетийн халдлага явуулах, сүлжээнд нэвтрэх боломжтой. Программ хангамжийн эмзэг байдал нь хортой код суулгах, төхөөрөмжийн хэвийн ажиллагааг алдагдуулах, зөвшөөрөлгүй хяналт тогтоох шалтгаан болдог. Иймээс бид судалгааны ажлын хүрээнд IoT төхөөрөмжийн эмзэг байдал аюул заналхийллийн судалгаа хийсэн.

Түлхүүр үг— IoT, IP, Smart technology, Cyber security, Cyber attack.

I. УДИРТГАЛ

Интернэтийн зүйлсийн сүлжээ (IoT) нь аж ахуйн нэгжийн сүлжээнд чухал ач холбогдолтой нөлөө үзүүлж, бодит цагийн өгөгдлийн шинжилгээ, шийдвэр гаргах үйл явцыг сайжруулан, инновацыг хурдасгах боломжийг бүрдүүлж байна. Сүүлийн жилүүдэд IoT төхөөрөмжүүдийн тоо цаашид эрчимтэй нэмэгдэж, ойрын жилүүдэд олон арван тэрбум төхөөрөмж ашиглагдах төлөвтэй байна. Энэхүү өсөлт нь IoT технологийг салбар бүрд өргөнөөр нэвтрүүлэх, шинэ хэрэглээний тохиолдлууд болон практик хэрэглээг хөгжүүлэх үйл явцтай шууд холбоотой болохыг судлаачид онцолж байна. IoT системүүдийн гол асуудлууд нь кибер гэмт хэрэг, хувийн мэдээллийн зөрчил юм.[1] IoT төхөөрөмжийн тоо нэмэгдэхийн хэрээр байгууллагын сүлжээний халдлагын эрсдэл нэмэгдэж буй нь анхаарал татахуйц асуудал болж байна. Эдгээр төхөөрөмжүүдийн хамгаалалт хангалтгүй байвал кибер халдлагад өртөх магадлал өндөр байх бөгөөд үүнээс улбаалан өгөгдлийн алдагдал, сүлжээний хэвийн үйл ажиллагааны доголдол зэрэг ноцтой үр дагавар үүсэх эрсдэлтэй. Иймд IoT төхөөрөмжийн аюулгүй байдлыг сайжруулах нь байгууллагын мэдээллийн системийн найдвартай ажиллагааг хангахад чухал ач холбогдолтой юм. Иймээс бид судалгааны ажлын хүрээнд зүйлсийн интернэт төхөөрөмжийн халдлагын чиг хандлагын талаар дэлгэрэнгүй танилцуулах болно.

II. ҮНДСЭН ХЭСЭГ

Аж үйлдвэрийн дөрөвдүгээр үеийн эрин үед ухаалаг төхөөрөмжүүдийн хэрэглээ дэлхий даяар хурдацтай хөгжиж байгаа билээ. IoT төхөөрөмжүүдийн хэрэглээ хурдацтай өсөн нэмэгдэж, хүмүүсийн өдөр тутмын амьдралын олон талбарт хувьсгал авчирч байна. Олон улсын Өгөгдлийн Корпорац (IDC)-ийн таамаглалын дагуу ойрын ирээдүйд IoT төхөөрөмжийн тоо хоёр их наяд хүрэх төлөвтэй байна. Гэвч энэхүү өргөн холболт нь мөн хакеруудын довтолгооны шинэ боломжуудыг бий болгож байна. IoT технологийг бизнес, хэрэглэгчид ихээр ашиглахын хэрээр түүний аюулгүй байдал чухал асуудал болж байгаа юм.[2] Монгол Улсын зах зээл ч үүнээс хоцролгүй ухаалаг тоног төхөөрөмжийг өргөнөөр ашиглах болж, сүүлийн жилүүдэд айл өрх болон албан газруудын хэрэглээ мэдэгдэхүйц өссөн байна. Судалгаанаас үзэхэд, 2023 оноос 2028 он хүртэл Монгол Улсад ухаалаг төхөөрөмжийн хэрэглээ жил бүр 1.69%-аар өсөх төлөвтэй байгаа бөгөөд энэ нь гэрийн ухаалаг системүүд, хамгаалалтын тоног төхөөрөмжүүд болон бусад IoT (Internet of Things) төхөөрөмжийн нэвтрэлттэй шууд холбоотой [3] юм. Үүнд:

Ухаалаг төхөөрөмжийн хэрэглээний өсөлтөд нөлөөлж буй гол хүчин зүйлүүд нь дараах байдалтай байна.

Гэрийн ухаалаг төхөөрөмжүүд: Ухаалаг хяналтын камер, ухаалаг чанга яригч, утаа мэдрэгч болон автоматжуулсан гэрэлтүүлэгтэй төхөөрөмжүүдийн хэрэглээ нэмэгдэж байна [4].

Байгууллагын ухаалаг системүүд: Албан байгууллагууд кибер аюулгүй байдлыг сайжруулах, дата анализ хийх, ухаалаг хяналтын системүүдийг ашиглах чиглэлээр хөрөнгө оруулалт хийж байна [5].

Мэдээллийн технологийн дэвшил: 5G технологи, үүлэн тооцоолол, AI болон машин сургалт зэрэг хөгжлүүд IoT-ийн өргөн хэрэглээг дэмжиж байна [6]. IoT төхөөрөмжийн өсөлт нь шинэ төрлийн аюулгүй байдлын эрсдэлийг бий болгож байна. Үүнд:

- Сүлжээний халдлага: Ухаалаг төхөөрөмжүүдийн ихэнх нь хангалттай хамгаалагдаагүй тул халдлагад өртөх магадлал өндөр байдаг [7].
- Мэдээлэл хулгайлах эрсдэл: IoT төхөөрөмжүүдээс дамжуулж буй өгөгдөл

шифрлэгдээгүй байвал гуравдагч этгээд хакердах боломжтой [8].

Судалгааг хяналттай, тусгаарлагдсан орчин бүрдүүлсний дараа үйлдлийн системийн эхний төлөвийн мэдээллийг цуглуулж, сүлжээний урсгал дээр анализ хийхийн тулд дараах программуудыг ашиглав. Үүнд:

- Ettercap -G [9];
- Wireshark [10];
- Nmap [11];
- Netdiscover [12] зэрэг хэрэгслүүд орно.

Эдгээр хэрэгслүүдийг ашиглан тусгайлан бэлдсэн үйлдлийн систем дээр сүлжээгээр дамжих өгөгдлийг шинжлэх ажлыг дараах үе шаттайгаар гүйцэтгэсэн. Үүнд:

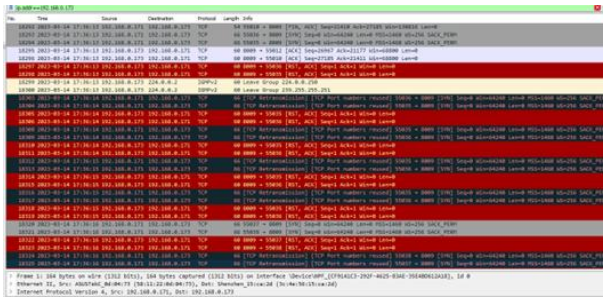
- Тандалт хийх – Сүлжээний орчныг судлах, боломжит зорилтот төхөөрөмжүүдийг илрүүлэх.
- Нэвтрэх эрх олж авах – Илрүүлсэн эмзэг байдлыг ашиглан хандалтын түшинг тодорхойлох.
- Хандалтыг хадгалах – Олж авсан хандалтыг тогтвортой хадгалах, нэмэлт хяналт хийх.
- Тохиргоог дахин тохируулах – Судалгааны үндсэн дээр сүлжээний аюулгүй байдлын сайжруулалтын арга хэмжээг боловсруулах.

Ийнхүү өгөгдлийг шинжлэх энэхүү үе шатууд нь системийн эмзэг байдлыг тодорхойлж, сүлжээний хамгаалалтын түвшинг үнэлэхэд чиглэсэн болно.

III. СУДАЛГААНЫ ҮР ДҮН

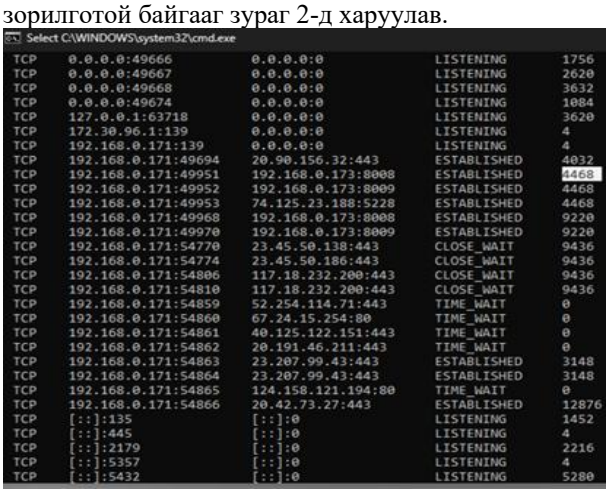
Бид судалгааны ажлын хүрээнд дотоод сүлжээний хэвийн болон халдлагатай пакет дээр дүн шинжилгээг харьцуулах байдлаар судалгаа хийсэн. Туршилтын ажлыг гүйцэтгэхдээ Intel Core i7 процессортой 16 гига санах ойтой компьютер дээр Virtualbox программ дээр Kali Backtrack үйлдлийн систем суулгаж туршилт хийсэн.

Байгууллагын дотоод сүлжээний төхөөрөмжүүдийн портын мэдээлэл сүлжээнд холбогдсон компьютерын бүртгэлийг Nmap хэрэгслийн тусламжтай тодорхойлсон. Wireshark 4.4.5 хэрэгслээр сүлжээгээр дамжиж байгаа пакетууд дээр дүн шинжилгээ хийсэн. IoT төхөөрөмж, хостын түвшний пакетуудын мэдээлэл дээр тулгуурлан сэжигтэй пакетуудын дата дамжуулалт болон хүлээн авсан протокол дээр анализ хийсний үр дүнд IP 192.168.0.173 хаягийг тодорхойлсон. Уг IP 192.168.0.173 хаягийг Wireshark хэрэгслээр нарийвчлан шалгаж үзэхэд дотоод сүлжээнд идэвхтэй байгаа төгсгөлийн төхөөрөмж болох хост уруу тандалт хийж байгааг зураг 1-д үзүүлэв.



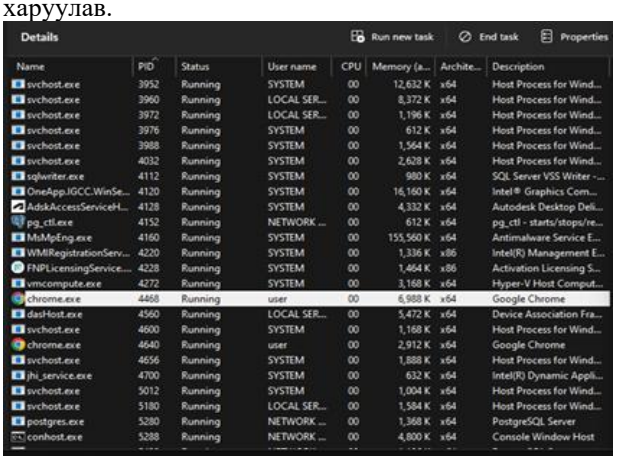
1-р зураг. IP 192.168.0.171 хаягтай хост уруу IP 192.168.0.173 хаягаас тандалт хийж байгаа байдал

Зураг 1-д харуулсан IP 192.168.0.171 хаягтай хост уруу тандалт хийж ACK пакетыг дахин ачаалсан байгааг тодорхойлсон. Уг халдлагын зорилго нь хостын эмзэг сул тал, программын цоорхой байгаа эсэхийг зайнаас тандалт хийж нэвтрэх эрх олж авах зорилготой байгааг зураг 2-д харуулав.



2-р зураг. IP 192.168.0.173 хаягаас 8008 порт

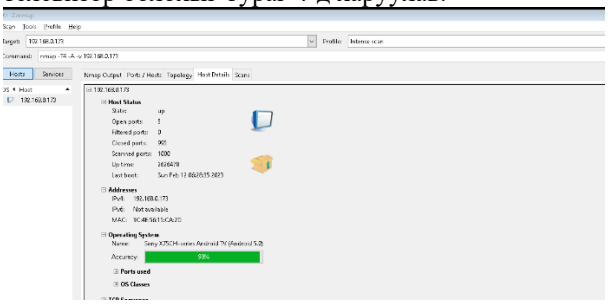
Зураг 2-д харуулсан IP 192.168.0.173 хаяг, порт 8008-ын тусламжтай chrome.exe файл уруу хандаж байгааг илрүүлсэн. Хостын IP хаягийн судалгааг зураг 3-д харуулав.



3-р зураг. Chrome.exe файл уруу хандалт хийж байгаа байдал

Уг портыг нарийвчлан судалж үзэхэд порт 8008 TCP нь сүлжээнд идэвхтэй байгаа хостуудад холболт болон өгөгдлийг нарийвчлан судалж үзэхэд IP 192.168.0.173 хаягтай хостыг илрүүлсэн. Уг хостыг

Zenmap хэрэгслээр тандалт хийж үзэхэд смарт телевизор болохыг Зураг 4-д харуулав.



4-р зураг. IP 192.168.0.173 хаяг дээрх IoT Sony X75CH-series Android TV телевизор

Зураг 4-д IoT төхөөрөмж дээр нээлттэй байгаа портуудыг нарийн судалж үзэхэд дараах портууд нээлттэй байсан. Үүнд:

- 8008
- 8009
- 8080
- 8443
- 9000 портууд нээлттэй байсан.

Эдгээр нээлттэй байгаа портуудын тусламжтай Cyclops Blink ботнет бэктор программаар DDoS халдлага хийх боломжтойг тодорхойлсон.

ДҮГНЭЛТ

Олон улсын судалгаагаар 2025 он гэхэд 25 тэрбум IoT төхөөрөмж сүлжээнд холбогдох хэрэгцээ үүсэж байгаа тул энэ талын шинэ төрлийн халдлагын орон зай үүсгэж байна. Сүүлийн жилүүдэд IoT төхөөрөмж дээр суурилсан цахим халдлага дайралт ихсэх болсон. Уг цахим халдлага дайралтын үндсэн зорилго нь улс орны мэдээлэл технологийн салбарыг хяналтдаа байлгаж шаардлагатай тохиолдолд үйл ажиллагааг доголдуулах зорилгоор Backdoor, Bot хөнөөлт программуудыг зориудаар тарааж байна. Иймээс Монгол Улс нь дээрх сөрөг арга хэмжээний эсрэг хариу арга хэмжээ яаралтай авах шаардлагатай байна.

НОМ ЗҮЙ

[1] Assessing the Cybersecurity Risks Associated with the Internet of Things (IoT) Devices

Taiwo Abdulahi Akintayo, Emmanuel Asolo, Chinenye Cordelia Nnamani, Omojola Ayogoke Felix, Chukwuemeka Chukwuma Osaro, Aregbesola Taobat Atinuke

21 Sep 2024 Vol. 1, Iss: 3, pp 170-184

[2] Developing a Comprehensive Security Framework for Detecting and Mitigating IoT Device Attack Rajeev Arora, Mohd Muqeem, Manish Saxena 30 Sep 2024 Research Square

[3] Smith, J., & Brown, A., "Cybersecurity Risks in Smart Devices and IoT," *Cybersecurity Trends Journal*, vol. 12, no. 3, pp. 45-60, 2022.

[4] "2023 Cybersecurity Report," Kaspersky Security Research, 2023. [Онлайн]. Available: https://www.kaspersky.com

[5] Anderson, T., "Smart Security Technologies: Best Practices," *Proceedings of the Smart Security Conference*, 2022.

[6] "NIST IoT Cybersecurity Guidelines," National Institute of Standards and Technology, 2023. [Онлайн]. Available: https://www.nist.gov.

[7] "Cisco Annual Cybersecurity Report 2023," Cisco Systems, 2023. [Онлайн]. Available: https://www.cisco.com.

[8] "Cybersecurity & Infrastructure Security Agency Report," CISA, 2023. [Онлайн]. Available: https://www.cisa.gov.

[9] Ettercap Project, "Ettercap Official Documentation," [Online]. Available: https://www.ettercap-project.org.

[10] Wireshark Foundation, "Wireshark: Network Protocol Analyzer," [Online]. Available: https://www.wireshark.org.

[11] Gordon Lyon, "Nmap Network Mapper - Official Documentation," [Online]. Available: https://nmap.org.

[12] Kali Linux, "Netdiscover - Network Address Discovery Tool," [Online]. Available: https://tools.kali.org/information-gathering/netdiscover

CCTV/IP КАМЕРЫН КИБЕР ЭМЗЭГ БАЙДЛЫН СУДАЛГАА

Оюунцэцэгийн ЭНХТУУЛ[1], Батбаярын ДЭНСМАА[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: enkhtuul.o@must.edu.mn[1], b.densmaa@must.edu.mn[2]

***Хураангуй*: Сүүлийн жилүүдэд IP камер болон CCTV системүүд нь зөвхөн хяналтын зориулалтаас гадна кибер халдлагын гарц болох өндөр эрсдэлтэй болж байна. Технологийн хөгжилтэй уялдан аналог камерууд тоон технологи руу шилжиж, интернэтэд холбогдож, дэлхийн хаанаас ч хянах боломжтой болсон нь эдгээр төхөөрөмжүүдийг кибер халдлагад өртөмтгий болгох гол хүчин зүйлсийн нэг болж байна. Ялангуяа сүлжээний хамгаалалт муутай, эмзэг байдлыг засварлаагүй, сул нууц үгтэй IP камерууд нь байгууллагын дотоод сүлжээнд аюул учруулж, гаднын халдагчид алсаас нэвтрэх боломж бүрдүүлж байна.Энэхүү судалгаанд UB-19 хаалттай санд ашиглагдаж буй IP камер болон NVR (Network Video Recorder) төхөөрөмжүүдийн аюулгүй байдлын эрсдэлийг тодорхойлох зорилгоор Wireshark, Zenmap, RegShot, Process Monitor зэрэг сүлжээний аюулгүй байдлын хэрэгслүүдийг ашиглаж, өгөгдлийн урсгалыг хянаж, CVE-2013-3381 зэрэг эмзэг байдлыг илрүүлсэн. Судалгааны явцад анхдагч нууц үг өөрчлөгдөөгүй, сул хамгаалалттай IP камерууд нь кибер халдлагад өртөх өндөр эрсдэлтэй болох нь тогтоогдсон бөгөөд Wireshark анализын үр дүнд эдгээр төхөөрөмжүүд нь гаднын серверүүд рүү зөвшөөрөлгүйгээр өгөгдөл дамжуулж буйг илрүүлсэн.Мөн CVE эмзэг байдлуудыг ашиглан гадны халдагчид алсын зайнаас камер болон холбогдсон сүлжээний бусад төхөөрөмжүүдийг удирдах боломжтой болох нь батлагдсан. Түүнчлэн Botnet халдлагад өртөх боломжтой сул хамгаалалттай камерууд байгааг тогтоосон бөгөөд Mirai, Mozi зэрэг хортой кодын халдлагад өртөх эрсдэлтэй болохыг илрүүлсэн. Эдгээр асуудлууд нь зөвхөн хувь хүн, байгууллагад бус, улсын хэмжээнд мэдээллийн аюулгүй байдалд нөлөөлөх ноцтой эрсдэл үүсгэж болзошгүй тул IP камерын хамгаалалтыг сайжруулах шаардлагатай гэсэн дүгнэлтэд хүрсэн.**

Түлхүүр үг: кибер аюулгүй байдал, камерын эмзэг байдал, халдлага, DoS, хакер

I. УДИРТГАЛ

CCTV (Closed-Circuit Television) камерууд нь анх эрүүгийн гэмт хэргээс урьдчилан сэргийлэх, нийтийн аюулгүй байдлыг хангах зорилгоор гудамж талбай, нийтийн эзэмшлийн газруудад байршуулж эхэлсэн[1].Технологийн хөгжлийн явцад аналог камерууд тоон технологи руу шилжиж, интернэтэд холбогдон дэлхийн хаанаас ч хянах боломжтой болсон. Энэ нь камерын хяналт, мэдээлэл дамжуулалт, аюулгүй байдлыг сайжруулсан ч кибер халдлагад өртөх эрсдэлийг нэмэгдүүлж байна[2].

Сүүлийн жилүүдэд олон улсын судалгаагаар IP камерууд нь сүлжээнд бүрэн нэвтрэх боломжийг олгож, тэдгээрийг ашиглан халдлага үйлдэж буй тохиолдлууд ихсэж байгааг харуулж байна[3]. Төр болон хувийн хэвшлийн байгууллагын мэдээллийн сан, компьютерын сүлжээнд нэвтрэхийн тулд IP камеруудыг халдлагын гарц болгон ашиглах боломжтой бөгөөд зайнаас тухайн байгууллагын сүлжээний үйл ажиллагааг тандан судлах, интернэтийн гарц үүсгэх зэрэг аюул заналхийллийг бий болгож байна [4].

Энэхүү судалгааны зорилго нь IP камер болон сүлжээний аюулгүй байдалтай холбоотой эрсдэлүүдийг тодорхойлох, халдлагын боломжит аргуудыг судлах, хамгаалалтын арга хэмжээг боловсруулах явдал юм[5]. Судалгааны хүрээнд Монгол Улсад ашиглагдаж буй IP камер, NVR (Network Video Recorder) төхөөрөмжүүд дээр туршилт хийж, Wireshark, Zenmap, RegShot, Process Monitor зэрэг сүлжээний аюулгүй байдлын хэрэгслүүдийг ашиглан өгөгдлийн урсгалыг хянах, халдлагын шинж тэмдгүүдийг илрүүлэхийг зорьсон[6]. Судалгааны дүнд IP камерын сул хамгаалалт, CVE (Common Vulnerabilities and Exposures) эмзэг байдал, өгөгдөл дамжуулалтын аюулгүй байдлын алдаа зэрэг нь байгууллагын сүлжээнд аюул учруулж болохыг харуулсан[7]. Камеруудын сул хамгаалалт нь зөвхөн хувь хүн, аж ахуйн нэгжүүдийн төдийгүй, улсын мэдээллийн аюулгүй байдалд ч ноцтой эрсдэл учруулж болзошгүй тул хамгаалалтын арга хэмжээг оновчтой боловсруулах, хэрэгжүүлэх нь нэн тэргүүний асуудал болоод байна[7]. Энэхүү судалгаа нь IP камерын аюулгүй байдлын эрсдэлүүдийг тодорхойлох, CVE эмзэг байдлуудыг шинжлэх, кибер халдлагаас урьдчилан сэргийлэх арга замыг боловсруулахад чухал ач холбогдолтой[8].

II. ОНОЛЫН СУДАЛГАА

Сүлжээний дэд бүтэц нь мэдээллийн урсгалыг зохицуулж, аюулгүй байдлыг хангахад чиглэсэн үндсэн бүрэлдэхүүн хэсгүүдийн цогц юм[9]. Энэ нь чиглүүлэгч (router), унтраалга (switch), галт хана (firewall), сервер болон бусад сүлжээний төхөөрөмжүүдээс бүрддэг[10]. IP камер нь сүлжээгээр холбогдож, дүрс мэдээллийг дамжуулдаг ухаалаг төхөөрөмж бөгөөд ихэвчлэн алсын хяналт хийх, аюулгүй байдлыг хангахад ашиглагддаг[11]. Гэсэн хэдий ч, кибер халдлагын өндөр эрсдэлтэй байдаг. IP камерын аюулгүй байдлыг зөрчих гол эмзэг байдал нь дараах хүчин зүйлүүд нь[12]:

- Алдаатай программ хангамж (Firmware vulnerabilities): Камерын үйлдвэрлэгчийн

программ хангамжийг шинэчлээгүйгээс үүдэн халдагчид сул талыг нь ашиглах боломжтой[13].

- Сул нууц үг (Weak passwords): Анхдагч эсвэл хялбар таамаглагдах нууц үгнээс шалтгаалан гаднын этгээд нэвтрэх боломжтой[14].
- Шифрлэлгүй өгөгдөл дамжуулалт (Unencrypted data transmission): IP камерын дамжуулж буй өгөгдөл нь шифрлэлгүй байвал Man-in-the-Middle (MitM) халдлагад өртөх магадлал өндөр[15] байдаг.
- CVE эмзэг байдал (Common Vulnerabilities and Exposures - CVE): Камерын системд бүртгэгдсэн CVE эмзэг байдал нь халдагчдад алсын зайнаас нэвтрэх боломж олгодог[16].
- IP камерын эсрэг ашиглагдаж болох халдлагын аргууд нь:
- Brute-force халдлага гэдэг нь халдагч тодорхой нэг төхөөрөмжийн нэвтрэх мэдээллийг олон төрлийн нууц үг ашиглан таах оролдлого хийдэг довтолгооны нэг төрөл юм[17]. IP камерын анхдагч эсвэл сул нууц үгтэй (admin: admin гэх мэт) төхөөрөмжүүд халдлагад өртөх өндөр эрсдэлтэй[18].
- Камерын анхдагч нууц үгийг өөрчлөөгүй хэрэглэгчид халдлагад хамгийн их өртдөг[19].
- Brute-force халдлагад "dictionary attack" буюу урьдчилан тодорхойлсон түгээмэл нууц үгийн жагсаалт ашиглах, "credential stuffing" буюу өмнө нь алдагдсан хэрэглэгчийн мэдээллийг ашиглах арга түгээмэл [20] CVE эмзэг байдлыг ашиглах
- IP камерууд нь CVE-2013-3381 зэрэг эмзэг байдлын улмаас гаднаас хянах боломжтой болохыг судалгааны явцад тогтоосон[21].
- SNMP (Simple Network Management Protocol) v2c протокол ашиглан камерын мэдээлэл авах, удирдах боломжтой[22].
- CVE-2013-3381 эмзэг байдал нь IoT (Internet of Things) төхөөрөмжүүдийг зайнаас хянах, удирдах боломж олгодог[15].
- Үүнээс гадна, CVE-2021-28372 зэрэг шинэчлэгдээгүй төхөөрөмжүүдэд халдаж болох эмзэг байдал бүртгэгдсэн[16].
- Man-in-the-Middle (MitM) халдлага
- MitM халдлага гэдэг нь сүлжээнд дамжиж буй мэдээллийг таслан авч, өөрчлөх эсвэл хулгайлах боломжийг олгодог довтолгооны арга юм[17]. Wireshark зэрэг хэрэгслүүдийг ашиглан сүлжээний өгөгдлийг хянах үед ARP spoofing ашиглан IP камерын дамжуулж буй өгөгдлийг өөрчилж, хуурамч мэдээлэл илгээх боломжтой нь тогтоогдсон[18].
- MitM халдлагын нэг төрөл болох ARP poisoning нь камер болон чиглүүлэгчийн хоорондын мэдээллийг өөрчлөх боломжтой[19].
- Камерын дамжуулсан бодит дүрсийг хуурамч дүрсээр солих боломжтой, үүнээс шалтгаалан бодит байдлыг гажуудуулж, аюулгүй байдлын асуудал үүсгэж болзошгүй[20].
- Botnet халдлага (Mirai, Mozi гэх мэт)
- Botnet халдлага гэдэг нь халдагч сүлжээнд холбогдсон олон тооны төхөөрөмжийг удирдаж, олон төрлийн халдлага үйлдэх боломжтой болох эрсдэлийг хэлнэ[21].
- 2016 онд болсон Mirai ботнет халдлага нь олон мянган IP камерыг хакердаж, интернэтийн томоохон үйлчилгээ үзүүлэгчдийг унагасан[22].
- Mirai нь сул нууц үгтэй IoT төхөөрөмжүүдийг халдварлуулж, DDoS (Distributed Denial of Service) халдлага үйлдэж байсан[23].
- Mozi ботнет халдлага нь P2P (Peer-to-Peer) сүлжээг ашиглан илүү ухаалаг, хяналтгүй халдлага хийх боломжтой болсон[24].

IP камерууд нь IoT төхөөрөмжүүдийн нэг хэсэг тул ботнет халдлагад хамгийн өртөмтгий төхөөрөмжүүдийн нэг[25]юм.

III. СУДАЛГААНЫ АРГАЧЛАЛ

Судалгааг нарийвчлан, оновчтой гүйцэтгэхийн тулд тусгайлан бэлтгэсэн орчинд туршилт хийсэн. Судалгааны үндсэн аргачлал дараах үе шатуудаас бүрдэнэ. Үүнд:

A. Судалгааны орчны бүрдүүлэлт: Туршилтыг тусгаарлагдсан орчинд хийхийн тулд өндөр хяналт бүхий, хамгаалагдсан виртуал орчин бэлтгэж, Windows 10 үйлдлийн систем суулгаж, сүлжээний урсгалыг хянах программ хангамжуудыг ашигласан. Процессор: Intel Core i7, Санах ой: 16GB RAM, WMware ашиглан Windows 10 үйлдлийн систем үүсгэсэн.

B. Судалгаанд ашигласан хэрэгслүүд: Сүлжээний дэд бүтцийн аюулгүй байдлыг хангахын тулд олон төрлийн программ хангамж ашигладаг бөгөөд үүнд RegShot, Wireshark, Zenmap, Process Monitor зэрэг хэрэгслүүд багтдаг.

1) RegShot нь Windows үйлдлийн системийн бүртгэлийн өөрчлөлтийг хянахад ашиглагддаг

хэрэгсэл юм. Энэ нь сүлжээний аюулгүй байдлын аудит хийх, хортой программын улмаас системийн бүртгэлд гарсан өөрчлөлтийг илрүүлэхэд чухал үүрэгтэй. RegShot-ийг ашиглан системийн бүртгэлийн эхний агшныг хадгалж, дараагийн агшныг хадгалсны дараа тэдгээрийг харьцуулж өөрчлөлтийг илрүүлэх боломжтой. Энэ нь кибер халдлагын үед халдлагаас үүдэлтэй өөрчлөлтийг илрүүлэхэд ашиглагддаг[23].

2) Wireshark нь сүлжээний урсгалыг хянах, дүн шинжилгээ хийх хамгийн алдартай хэрэгслүүдийн нэг юм. Энэ нь сүлжээний багцуудыг барьж авах, тэдгээрийг задлан шинжилж, сүлжээний асуудлыг оношлох, халдлагыг илрүүлэхэд ашиглагддаг. Wireshark нь Deep Packet Inspection (DPI) буюу сүлжээний багцын нарийвчилсан шинжилгээ хийх чадвартай. Ингэснээр, халдагчийн илгээсэн сэжигтэй багцуудыг тодорхойлох, зөвшөөрөлгүй дата дамжуулалтыг илрүүлэх, галт ханын тохиргоог шалгах боломжтой болдог[24].

3) Zenmap нь Nmap хэрэгслийн график интерфейстэй хувилбар бөгөөд сүлжээний сканер хийх, төхөөрөмжүүдийг илрүүлэх, портын нээлттэй байдлыг шалгах зорилготой. Zenmap-ийг ашигласнаар тухайн сүлжээнд ямар төхөөрөмжүүд холбогдсон байгаа, тэдгээрийн IP хаяг, нээлттэй портууд, үйлчилгээний төрлийг тодорхойлох боломжтой. Сүлжээний хамгаалалтыг сайжруулахын тулд penetration testing буюу нэвтрэх тест хийхэд Zenmap-ийг өргөн ашигладаг[25].

4) Process Monitor нь Windows үйлдлийн системийн үйл ажиллагааг хянах, тухайн үед ажиллаж буй процессуудын талаар дэлгэрэнгүй мэдээлэл өгөх хэрэгсэл юм. Энэ нь системийн процессуудыг гүнзгий судлах, хортой программ хангамжийн үйл ажиллагааг илрүүлэхэд ашиглагддаг. Process Monitor нь real-time event monitoring буюу бодит цагийн горимоор процессуудыг ажиглаж, registry access, file system activity, network connections зэрэг мэдээллийг бүртгэж, ул мөрийг нь тодорхойлдог. Кибер аюулгүй байдлын мэргэжилтнүүд энэ хэрэгслийг ашиглан хортой кодын үйл ажиллагааг судалж, системийн аюулгүй байдлыг сайжруулдаг[26].

Сүлжээний дэд бүтцийн аюулгүй байдлыг хангахын тулд RegShot, Wireshark, Zenmap, Process Monitor зэрэг хэрэгслүүдийг ашиглаж, систем дэх өөрчлөлтийг хянах, сүлжээний урсгалыг шалгах, нээлттэй портуудыг тодорхойлох, үйлдлийн системийн процессуудыг хянах зэрэг олон төрлийн арга хэмжээг авах шаардлагатай. Эдгээр хэрэгслүүдийг хослуулан ашигласнаар халдлагыг эрт үед нь илрүүлэх, урьдчилан сэргийлэх, сүлжээний найдвартай ажиллагааг хангах боломжтой юм

Судалгааг дараах үндсэн дарааллаар гүйцэтгэнэ. Үүнд:

a) Төлөвлөлт болон тойм судалгаа: Олон улсын болон дотоодын IP камер, NVR төхөөрөмжийн аюулгүй байдлын талаарх өмнөх судалгаануудыг судалсан.
b) Тандалт хийх: Zenmap болон Wireshark ашиглан дотоод сүлжээнд холбогдсон IP камер болон NVR төхөөрөмжүүдийн мэдээллийг тодорхойлсон.
c) Нэвтрэх эрх олж авах: Эмзэг IP хаягуудыг тодорхойлон, халдлагын боломжийг судалсан.
d) Хандалтыг хадгалах: Халдлагын үр нөлөө хэрхэн хадгалагдаж байгааг судалсан.
e) Үндсэн хамгаалалтын тохиргоонд дүн шинжилгээ хийх: Хамгаалалтын сул талуудыг тодорхойлон, тэдгээрийг хэрхэн засах талаар судалсан.

IV. СУДАЛГААНЫ ҮР ДҮН

UB-19 хаалттай санд түгээмэл хэрэглэж байгаа IP камер, NVR төхөөрөмж дээр илэрдэг Wireshark 2.0.1 хэрэгслээр сүлжээгээр дамжиж байгаа пакетууд дээр дүн шинжилгээ хийсэн. Wireshark хэрэгслээр сүлжээний өгөгдлийн урсгалаас халдлагыг илрүүлэхдээ дотоод сүлжээний IP камер, хостын түвшний пакетуудын мэдээлэл дээр тулгуурлан сэжигтэй пакетуудын дата дамжуулалт болон хүлээн авсан протокол дээр дүн шинжилгээ хийж үзэхэд дараах үр дүн гарсан. ARP протоколын тусламжтай гадаад хаяг үүсгэж байгааг зураг 1-д харуулав.

arp

	Time	Source	Destination	Protoc	Lengt	Info
8	2023-03-10 05:56:51.994171	5a:58:11:56:1e:40	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.156
9	2023-03-10 05:56:51.994171	5a:58:11:56:1e:40	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.156
10	2023-03-10 05:56:51.994171	5a:58:11:56:1e:40	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.156
11	2023-03-10 05:56:52.003560	5a:58:d1:a9:a2:e6	Broadcast	ARP	60	Who has 1.0.0.0? Tell 192.168.1.151
12	2023-03-10 05:56:52.090657	5a:58:ad:51:0f:a6	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.1.164
13	2023-03-10 05:56:52.120152	5a:58:ad:51:0f:a6	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.164
14	2023-03-10 05:56:52.120152	5a:58:ad:51:0f:a6	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.164
15	2023-03-10 05:56:52.120152	5a:58:ad:51:0f:a6	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.164
18	2023-03-10 05:56:52.328687	5a:58:57:6a:5e:65	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.165
19	2023-03-10 05:56:52.328687	5a:58:57:6a:5e:65	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.165
20	2023-03-10 05:56:52.328687	5a:58:57:6a:5e:65	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.165
21	2023-03-10 05:56:52.396250	5a:58:bb:87:a5:42	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.158
22	2023-03-10 05:56:52.396250	5a:58:bb:87:a5:42	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.158
23	2023-03-10 05:56:52.396626	5a:58:bb:87:a5:42	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.158
24	2023-03-10 05:56:52.412162	Ubiquiti_59:c0:91	Broadcast	ARP	60	Who has 192.168.1.66? Tell 192.168.1.10
26	2023-03-10 05:56:52.436394	5a:58:a7:04:c8:f7	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.155
27	2023-03-10 05:56:52.436394	5a:58:a7:04:c8:f7	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.155
28	2023-03-10 05:56:52.436394	5a:58:a7:04:c8:f7	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.155
29	2023-03-10 05:56:52.536002	5a:58:c0:97:f4:48	Broadcast	ARP	60	Who has 47.252.8.80? Tell 192.168.1.154
30	2023-03-10 05:56:52.536002	5a:58:c0:97:f4:48	Broadcast	ARP	60	Who has 47.74.153.98? Tell 192.168.1.154
31	2023-03-10 05:56:52.536002	5a:58:c0:97:f4:48	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.154
32	2023-03-10 05:56:52.543504	5a:58:11:56:1e:40	Broadcast	ARP	60	Who has 8.8.8.8? Tell 192.168.1.156
33	2023-03-10 05:56:52.750002	Ubiquiti_59:c2:90	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.18
36	2023-03-10 05:56:52.970525	Ubiquiti_59:c2:90	Broadcast	ARP	60	Who has 192.168.1.33? Tell 192.168.1.18
37	2023-03-10 05:56:53.006836	5a:58:a7:04:c8:f7	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.1.155
39	2023-03-10 05:56:53.023445	5a:58:11:56:1e:40	Broadcast	ARP	60	Who has 139.9.5.224? Tell 192.168.1.156

1-р зураг. ARP протоколын тусламжтай гадаад хаяг үүсгэж байгаа

1-р зураг. ARP протоколын тусламжтай IP камерууд гадаад хаягийн хайлт хийж байгаа Wireshark ашиглан сүлжээний урсгалыг судлахад ARP (Address Resolution Protocol) ашиглан гаднын сервер рүү холбогдох оролдлого илэрсэн. Зураг 1-д ARP хүсэлт дамжуулж буй байдлыг харуулсан бөгөөд Alibaba US Technology Co., Ltd. домэйн руу холбогдож буйг тогтоосон. Дээрх хаягуудын дэлгэрэнгүй мэдээллийг хүснэгт 1-д харуулав.

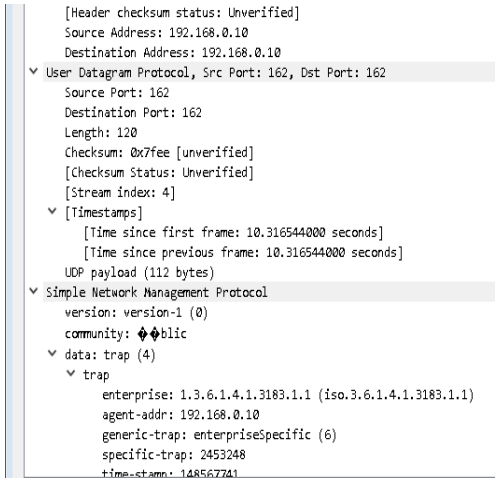
ALIBABA US TECHNOLOGY CO., LTD. ДОМАЙН РУУ ХОЛБОГДОЖ БУЙ ХАЯГУУДЫН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЭЛ

1-Р ХҮСНЭГТ

№	IP камерын хаяг	Төхөөрөмж	Тайлбар
1	192.168.1.164	Камер	Alibaba US Technology Co., Ltd. Домэйн шалгаж байна
2	192.168.1.156	Камер	Alibaba US Technology Co., Ltd. Домэйн шалгаж байна
3	192.168.1.155	Камер	Alibaba US Technology Co., Ltd. Домэйн шалгаж байна
4	192.168.1.154	Камер	Alibaba US Technology Co., Ltd. Домэйн шалгаж байна

1-р хүснэгтэд харуулсан IP хаягуудыг нарийвчилсан байдлаар судалж үзэхэд ARP протоколын тусламжтай үйлдвэрлэгч улс уруу холболт тогтоох хайлт хийж байна. IP 192.168.0.10 хаягаас порт 162 руу өгөгдөл дамжуулж буйг илрүүлсэн. Судалгааны үр дүнд уг порт нь CVE-2013-3381 эмзэг байдлыг ашиглаж, зайнаас халдлага үйлдэх боломжтой болохыг тогтоосон. Энэ алдаа нь хост болон IoT төхөөрөмжүүдийн хамгаалалтыг тойрон гарах боломжийг олгодог

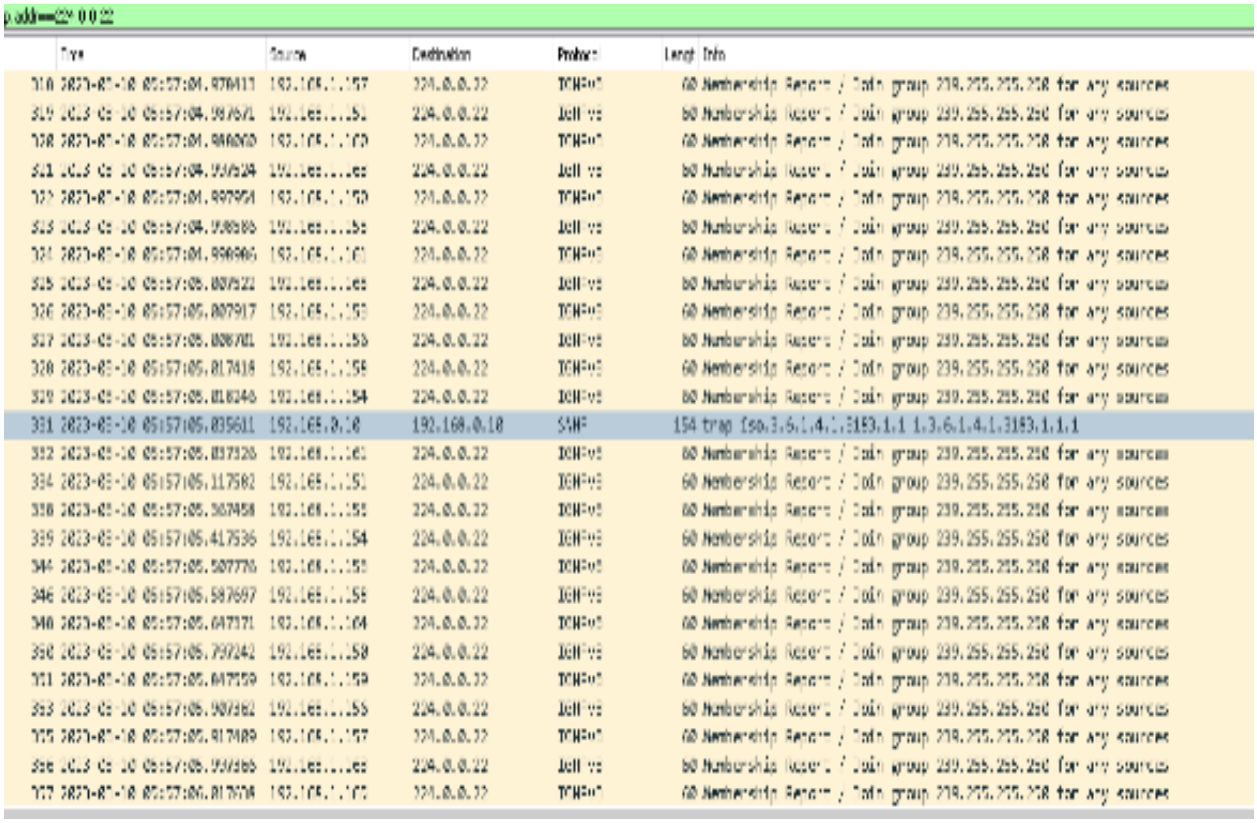
Зураг 2-д харуулсан IP 224.0.0.22 хаягийн тусламжтай IP камер, хостуудыг IP 239.255.255.250 хаяг уруу холбож байна. Хаяг дундаас IP 192.168.0.10 хаягийн өгөгдлийн нарийвчилсан мэдээллийг зураг 2-д харуулав. 224.0.0.22 хаяг нь IGMP (Internet Group Management Protocol) ашиглаж, IP камер, NVR төхөөрөмжүүдийг олон хосттой холбох үйл ажиллагааг явуулж байна. Иймүйлдэл нь халдлага үйлдэхэд ашиглагдаж болох боломжит эмзэг байдал үүсгэж буйг илтгэнэ.



2-р зураг. Дээрх IP хаягууд мультист групт бүртгүүлэх хэсэг

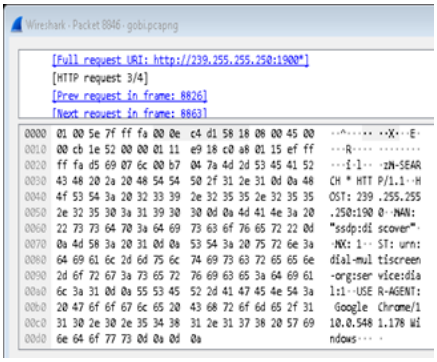
Зураг 2-д харуулсан IP 192.168.0.10 хаягаас порт 162 уруу өгөгдөл илгээж байгааг илрүүлсэн. Уг порт 162 судалж үзэхэд CVE-2013-3381 алдааны код илэрсэн.

Уг алдааны код нь зайнаас холболт тогтоож хост болон IoT төхөөрөмжийн эмзэг сул тал уруу халдлага хийдэг.



3-р зураг. IP 192.168.0.10 хаягнаас порт 162 уруу өгөгдөл илгээсэн байдал

IP 239.255.255.250 хаяг нь порт 1900 аар өгөгдөл дамжуулж байгааг зураг 3-д харуулав. Wireshark анализын явцад IP 192.168.0.10 хаягаас порт 162 руу өгөгдөл илгээж буйг илрүүлсэн. Уг портыг шинжилж үзэхэд CVE-2013-3381 эмзэг байдал илэрсэн. CVE-2013-3381 алдааны код нь зайнаас холболт тогтоох боломжийг олгодог. Энэ эмзэг байдал IoT төхөөрөмжүүд болон хост компьютеруудын хамгаалалтыг тойрон гарах боломжтой. IP 192.168.0.10 нь сүлжээний бусад төхөөрөмжүүдтэй холболт үүсгэж, сүлжээнд халдлага үйлдэх эрсдэлийг бий болгож байна.



4-р зураг. IP 239.255.255.250 хаяг дээр дүн шинжилгээ хийсэн үр дүн

Зураг 4- д харуудсан IP 239.255.255.250 SSDP протокол нь DDoS халдлагыг далд дэмжиж байна. Wireshark анализын үр дүнд IP 239.255.255.250 хаяг нь порт 1900 ашиглан өгөгдөл дамжуулж буйг илрүүлсэн. SSDP (Simple Service Discovery Protocol) нь IoT болон ухаалаг төхөөрөмжүүдийг автоматаар холбох үүрэгтэй протокол юм. Энэ протоколыг ашиглан DDoS халдлага үйлдэх боломжтой. Зорилтот халдлага нь Google Chrome, Microsoft Edge веб хөтөч уруу чиглэж байгааг тодорхойлсон.

ДҮГНЭЛТ

Энэхүү судалгаагаар CCTV камер, IP камерын аюулгүй байдал, тэдгээрийн сүлжээний эмзэг байдал, халдлагын боломжууд, хамгаалалтын арга хэмжээг шинжилж, бодит кейс дээр тулгуурлан дүгнэлт хийсэн. Камерууд нь анх гэмт хэргээс урьдчилан сэргийлэх, хамгаалалт хийх зорилготой байсан боловч орчин үед интернэтэд холбогдож, ухаалаг системтэй болж хөгжсөн нь кибер халдлагад өртөх эрсдэлийг нэмэгдүүлж байна.

Судалгааны үр дүнд UB-19 хаалттай санд ашиглагдаж буй IP камер, NVR төхөөрөмжүүдийн хамгаалалт сул бөгөөд Wireshark, Zenmap, Process Monitor, RegShot зэрэг хэрэгслүүдийг ашиглан сүлжээний эмзэг байдал, сэжигтэй өгөгдөл дамжуулалтыг хянах боломжтой болохыг тогтоосон.

Судалгааны явцад дараах чухал дүгнэлтүүд хүрсэн. Үүнд:

1. Камеруудын аюулгүй байдал сул хэвээр байна. Үүнд:
    - Анхдагч нууц үг өөрчлөгдөөгүй камерууд халдлагад өртөх өндөр эрсдэлтэй байна.
    - CVE-2013-3381 зэрэг эмзэг байдал ашиглагдвал камерын удирдлагыг гаднаас авах боломжтой.
    - ARP spoofing болон MitM (Man-in-the-Middle) халдлага хийж, камерын дүрсийг өөрчлөх боломжтой.
2. Судалгааны туршилтаар сүлжээнд дараах аюул илэрсэн.
    - IP 192.168.0.10 хаягаас порт 162 руу өгөгдөл илгээж буйг илрүүлсэн бөгөөд CVE-2013-3381 эмзэг байдалтай болох нь батлагдсан.
    - IP 239.255.255.250 SSDP протоколыг ашиглан DDoS халдлага үйлдэх боломжтой байна.
    - Wireshark хэрэгслээр сүлжээний урсгалыг хянах үед гаднын сервертэй холбогдох оролдлого гарч байгаа нь тогтоогдсон.
3. IP камерын хамгаалалтыг сайжруулах шаардлагатай. Судалгааны үр дүнд IP камерын аюулгүй байдлыг сайжруулах дараах арга хэмжээг авах шаардлагатай гэдэг нь тодорхой болов. Үүнд:
    - Анхдагч нууц үг солих, бат бөх нууц үг хэрэглэх.
    - Программ хангамжийн шинэчлэл (firmware update)-ийг тогтмол хийх.
    - Галт хана (firewall) ашиглаж, зөвхөн шаардлагатай портуудыг нээлттэй байлгах.
    - Сүлжээний урсгалыг Wireshark, Zenmap ашиглан тогтмол хянах.
    - VPN болон шифрлэлтэй холболт ашиглах замаар өгөгдлийг хамгаалах.
4. Камерын аюулгүй байдлыг бүрэн хангахгүй бол кибер халдлагад өртөх эрсдэл өндөр байна. IP камерууд нь зөвхөн дүрс дамжуулах биш, байгууллагын сүлжээний нэг хэсэг болсноор тухайн байгууллагын сервер, өгөгдлийн санд халдах гарц болж болохыг судалгааны үр дүн харууллаа. Кибер халдагчид сул хамгаалалттай IP камер ашиглан байгууллагын дотоод сүлжээ рүү нэвтрэх боломжтой нь батлагдлаа.

Энэхүү судалгаа нь IP камер, NVR төхөөрөмжүүдийн кибер аюулгүй байдлын асуудлуудыг тодорхойлох, судлах, хамгаалалтын арга хэмжээг боловсруулахад чухал хувь нэмэр оруулж байна. Өнөөгийн дижитал эринд байгууллагууд болон хувь хүмүүс CCTV/IP камерын аюулгүй байдлыг хангах бодлого боловсруулах, CVE мэдээллийг тогтмол шалгах, хамгаалалтын системээ шинэчлэ**х** шаардлагатай.

IP камерын сул хамгаалалт нь зөвхөн хувь хүний биш, байгууллага, улсын аюулгүй байдалд ч ноцтой эрсдэл учруулж болзошгүй тул аюулгүй байдлын арга хэмжээг шууд хэрэгжүүлэх нь зүйтэй

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Bejtlich, R. (2005). The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley Professional.

[2] Fyodor. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.

[3] Russinovich, M. E., Solomon, D. A., & Ionescu, A. (2012). Windows Internals, Part 1. Microsoft Press.

[4] Sikorski, M., & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. No Starch Press.

[5] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94.

[6] Stallings, W. (2020). Computer Networking: Principles, Protocols, and Practice. Pearson Education.

[7] MITRE Corporation. (n.d.). Common Vulnerabilities and Exposures (CVE). Retrieved from https://cve.mitre.org.

[8] Cisco Systems. (2016). Network Security Fundamentals. Cisco Press.

[9] Northcutt, S., & Novak, J. (2002). Network Intrusion Detection. New Riders Publishing.

[10] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

[11] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Shoshitaishvili, Y. (2017). Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, Vancouver, Canada.

[12] Cisco Systems. (2016). Network Security Fundamentals. Cisco Press.

[13] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

[14] Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94.

[15] Stallings, W. (2020). Computer Networking: Principles, Protocols, and Practice. Pearson Education.

[16] MITRE Corporation. (n.d.). Common Vulnerabilities and Exposures (CVE). Retrieved from https://cve.mitre.org.

GPON СҮЛЖЭЭНИЙ УДИРДЛАГЫН СИСТЕМ БА МОНГОЛЫН НӨХЦӨЛД СҮЛЖЭЭ ЗОХИОН БАЙГУУЛАХ СУДАЛГАА

Нэргүйн МЯГМАРСҮРЭН[1], Ямхины ДАШДОРЖ[2], Тогоохүү БУЛГАНМАА[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: j.in23e001@must.edu.mn[1], dashdorj@must.edu.mn bulganmaa.t@must.edu.mn[3]

***Хураангуй*: Энэхүү судалгааны ажил нь GPON технологийн сүлжээний удирдлагын системийн дизайн ба судалгааг хийж, монголд байгуулсан жижиг сүлжээг танилцуулах болно. Интернэтийн энэ эрин үед хэрэглэгчдийн шаардлагаар өндөр хурдтай бас найдвартай интернэт зайлшгүй хэрэгцээ үүсэж байгаа бөгөөд бид GPON сүлжээ байгуулснаар хэрэглэгчдэд найдвартай, өндөр хурдны Интернэт болон OTT үйлчилгээг авах боломжийг олгох болно. GPON (Gigabit Passive Optical Network) нь өндөр хурдны интернэт болон дата дамжуулахад ашиглагддаг шилэн кабель-based пассив оптик сүлжээний технологи юм. Энэ нь дэлхий даяар өндөр хурдны интернэт, телевиз, дуудлага зэрэг үйлчилгээг хамгийн үр ашигтайгаар хүргэхэд ашиглагддаг. Менежмент ба урьдчилан сэргийлэх хяналт, автоматжуулсан алдаа илрүүлэлт, шийдэл гаргах аргуудыг хэрэгжүүлэх,үйлчилгээний тасалдалтыг багасгахын тулд бодит цагийн хяналт болон урьдчилсан шинжилгээ ашиглах зорилготой. GPON нь нэг сүлжээнд өндөр хурдтай (1 Gbps хүртэл) өгөгдөл дамжуулах боломжтой. Энэ нь пассив буюу идэвхгүй шилэн кабельд суурилсан систем учраас эрчим хүчний хувьд харьцангуй зардал бага байдаг.**

Түлхүүр үг: NMS, GPON сүлжээ, загвар, Харьцуулалт

I. УДИРТГАЛ

Энэхүү судалгаа нь GPON сүлжээг удирдах, хянах, алдааг илрүүлэх удирдлагын системийг судлах сайжруулахад оршино.GPON сүлжээг загварчлахад архитектур, стандарт, бүрэлдэхүүн хэсгүүдэд оптик шугамын терминал (OLT) болон оптик сүлжээний нэгжүүд (ONU/ONT) гол бүрэлдэхүүнүүд багтдаг бөгөөд эдгээр нь сүлжээний гүйцэтгэл, найдвартай байдлыг удирдахад чухал үүрэгтэй GPON сүлжээг үр дүнтэй төлөвлөх нь маш чухал.Энэ нь сүлжээний топологи болон бүрэлдэхүүн хэсгүүдийн сонголтыг оновчтой болгох замаар хэрэглээний тодорхой шаардлагыг хангах боломжийг бүрдүүлдэг. ITU-T G.984 зэрэг GPON стандартуудыг дагаж мөрдөх нь сүлжээний харилцан нийцтэй байдал болон гүйцэтгэлийг сайжруулах үндэс болдог.

II. GPON СҮЛЖЭЭ УДИРДЛАГЫН СИСТЕМ

II.1. NMS-ийн үүрэг

GPON сүлжээг үр ашигтай, найдвартай удирдах гол хэрэгсэл нь Сүлжээний Удирдлагын Систем (Network Management System – NMS) юм. NMS нь OLT (Optical Line Terminal) болон ONT (Optical Network Terminal)-ийн төлөв байдлыг хянах, доголдлыг илрүүлэх, алдааны мэдээллийг дамжуулах, мөн гүйцэтгэлийн дүн шинжилгээ хийх зэрэг олон чухал үүргийг гүйцэтгэдэг.

II.2 Алдаа илрүүлэлт ба мэдээлэх

II.2.1 **Байнгын хяналт**

NMS нь GPON сүлжээний үндсэн төхөөрөмжүүд болох OLT болон ONT-ийн ажиллах төлөвийг бодит цагт хянаж, сүлжээний ерөнхий гүйцэтгэлийн мэдээлэл, сигналын чадал, үйлчилгээний тасалдал, хоцрогдол зэрэг үзүүлэлтүүдийг тогтмол хянаж байдаг. NMS нь төхөөрөмжүүдээс ирж буй мэдээллийн дагуу системд гарч буй алдаануудыг илрүүлж, холбогдох анхааруулгыг хэрэглэгч болон системийн администраторт дамжуулдаг. Үүнд дараах нийтлэг алдаанууд хамаарна:

Loss of Signal (LOS) – Дохио бүрэн тасарсан Шалтгаан: шилэн кабелийн тасралт, холбогчийн сулрал, тоног төхөөрөмжийн гэмтэл.

Low / High Optical Power – Оптикийн хүчний алдагдал Шалтгаан: бохир коннектор, муу чанартай кабель, хэт урт зам. Loss of Frame (LOF) – GPON фрейм бүрэн хүлээж авахгүй байх Шалтгаан: синхрончлолын алдаа.

Loss of GEM Mapping (LOM) – GEM сувагчлалын алдагдал Шалтгаан: тохируулгын алдаа, портын доголдол.

Time Drift / Synchronization Error – Цагийн зөрчил Шалтгаан: TDMA технологийн онцлогоос хамааран ONT ба OLT хоорондын синхрон алдагдах.

II.2. Алдааны мэдээллийг дамжуулах механизм NMS нь алдааг илрүүлснээр дараах аргуудыг ашиглан мэдээлэл дамжуулдаг: SNMP Trap эсвэл Syslog-оор төв серверт мэдэгдэл илгээх Веб интерфейс дээр реал-тайм анхааруулга гаргах И-мэйл болон SMS мэдэгдэл илгээх боломж Тэмдэглэл (Log) үүсгэн, түүхэн мэдээллийг хадгалах

III. GPON СҮЛЖЭЭНД АШИГЛАГДАХ ПРОТОКОЛ

• SNMP (Simple Network Management Protocol) SNMP нь сүлжээний төхөөрөмжүүдийг удирдах хамгийн түгээмэл протокол юм. Энэ нь NMS-д OLT, ONT болон бусад төхөөрөмжүүдийн мэдээллийг цуглуулах боломжийг олгодог.

• OMCI (ONT Management and Control Interface) OMCI нь ITU-T G.984 стандартаар тодорхойлогдсон протокол бөгөөд OLT нь OMCI-ийг ашиглан ONT төхөөрөмжүүдийг удирддаг.

• TR-069 (CPE WAN Management Protocol) TR-069 нь CPE (Customer Premises Equipment) төхөөрөм- жүүдийг зайнаас удирдах протокол юм. GPON сүлжээнд энэ нь ONT-удын тохиргоо, хяналт, алдааг илрүүлэх зорилгоор ашиглагддаг.

• NETCONF / YANG NETCONF (Network Configuration Protocol) нь сүлжээний төхөөрөмжүүдийн тохиргоо болон менежментийг программчлагдсан аргаар удирдах зориулалттай протокол юм. Харин YANG (Yet Another Next Generation) нь эдгээр төхөөрөмжүүдийн тохиргоо, төлөв байдлыг тодорхойлох өгөгдлийн загварын хэл юм. Энэ хоёр нь хамтдаа ажилласнаар сүлжээний удирдлага, автоматжуулалтыг илүү үр дүнтэй, уян хатан болгодог.

IV. МОНГОЛЫН НӨХЦӨЛД GPON СҮЛЖЭЭ БАЙГУУЛАХ

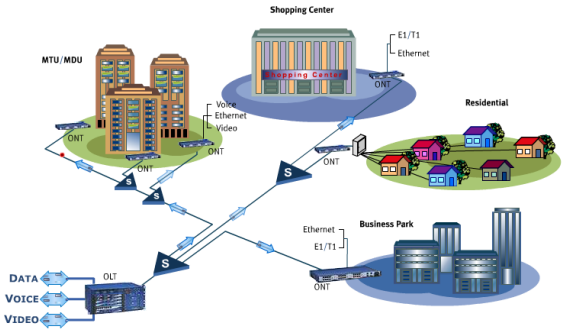
Манай багийн зүгээс GPON технологийн хэрэглээг бодит нөхцөлд хэрэгжүүлэх зорилгоор жижиг хэмжээний туршилтын сүлжээ байгуулсан. Энэхүү жишээ нь GPON сүлжээ хэрхэн зохион байгуулагддаг, ямар төхөөрөмжүүд ашиглагддаг талаар практик ойлголт өгөх зорилготой. Ашиглагдсан гол бүрэлдэхүүнүүд:

1. Optical Line Terminal (OLT): Сүлжээний үндсэн удирдлагын төхөөрөмж болох 8 порттой OLT ашигласан. Нэг порт нь 128 хүртэлх хэрэглэгчийг холбох боломжтой бөгөөд энэхүү төхөөрөмж нь сигнал үүсгэж, шилэн кабелиар дамжуулан хэрэглэгчдийн төхөөрөмж рүү түгээдэг.
2. Шилэн кабель (Fiber Optic Cable): OLT болон хэрэглэгчийн салаалагч хооронд 450 метр урттай шилэн кабель татсан. Энэ нь сигналын чанарыг алдагдуулалгүй дамжуулах үүрэгтэй.

3. Салаалагч (Splitter): Шилэн кабелийн сигналыг олон хэрэглэгч рүү хуваарилах зорилгоор хоёр төрлийн Splitter ашиглав. Үүнд: 1x4 Splitter – Үндсэн салаалагч байдлаар, хэрэглэгчид өгөх дараагийн салаалагч руу холбох үүрэгтэй. 1x16 Splitter – Сүүлийн түвшний салаалагч бөгөөд хэрэглэгчид шууд хуваарилагдана.

4. Drop Cable (Шилэн кабель): Салаалагчаас хэрэглэгчийн төхөөрөмж хүртэл холбогдох нарийн бүтэцтэй, нэг судалтай шилэн кабель ашигласан. Энэ төрлийн кабель нь хэрэглэгч бүрд тусад нь захиалгаар хийгдсэн.

5. Optical Network Unit (ONU): Хэрэглэгчийн байранд байрлах терминал төхөөрөмж бөгөөд гаднаас ирж буй шилэн кабелийн SC холбогчийг хүлээн авч, GPON сигналыг Ethernet эсвэл WiFi сигнал болгон хувиргаж, хэрэглэгчдэд интернэт болон бусад үйлчилгээ үзүүлнэ.



1-р зураг. GPON сүлжээг монголд зохион байгуулсан ерөнхий зураглал

V. МОНГОЛЫН НӨХЦӨЛД GPON СҮЛЖЭЭ БАЙГУУЛСАН ТӨСЛИЙН ҮР ДҮН

А. Бидний зүгээс тухайн байгуулсан сүлжээний хэрэглэгчдэдээ 1 төрлийн багц өгсөн бөгөөд тухайн багц нь Basic(Нэр) Download-20mbps Uplink-16mbps байхаар тохируулсан бөгөөд хэрэглэгчийн хүлээн авах ONT дээр LAN болон Wifi дээр хэмжилт хийсэн ба хэмжилтийн үр дүнг доор үзүүллээ.

LAN холболттой үед:

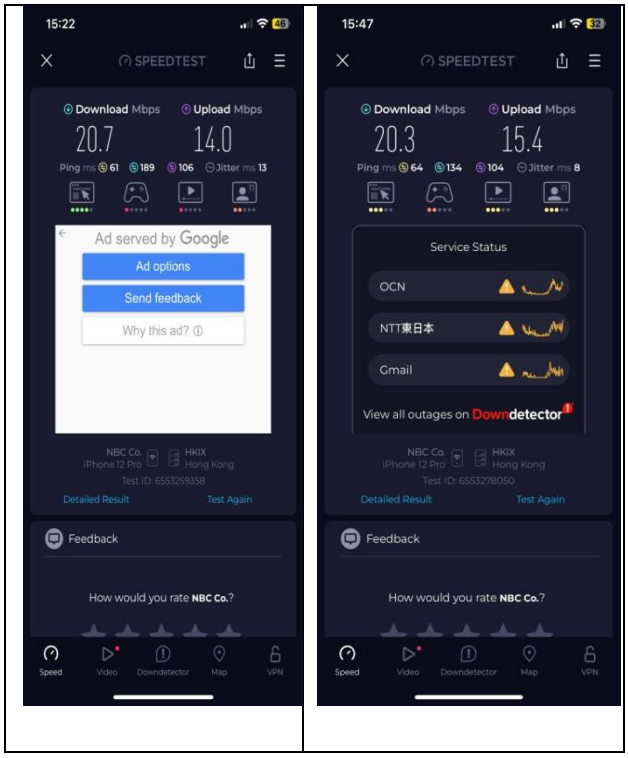
- Хамгийн их DL хурд 20.7 mbps, UL хурд 14.0 mbps

Wifi холболттой үед:

- Хамгийн их DL хурд 20.3 mbps, UL хурд 15.4 mbps

Хэмжилтийг SPEED TEST application ашиглан Хонконгийн HKIX exchange рүү хийв.

1-Р ХҮСНЭГТ. SPEED TEST APPLICATION ДЭЭР ХИЙСЭН ТЕСТИЙН ҮР ДҮН



B. Тестийн үр дүн

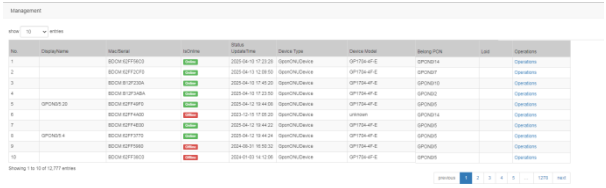
Хэрэглэгчийн төхөөрөмж дэх ONT дээрх хэмжилтүүд бидний өгсөн багцыг авч чадаж байгаа тул амжилттай болсон гэж харж байгаа

GPON БОЛОН БУСАД СҮЛЖЭЭНИЙ ХАРЬЦУУЛАЛТ

2-Р ХҮСНЭГТ

Ялгаатай	GPON	**xDSL, Ethernet, HFC гэх мэт**
Дамжуулах дээд хурд	2.5 Gbps (downlink), 1.25 Gbps (uplink)	DSL: 10–100 Mbps HFC: 100 Mbps – 1 Gbps
Хамрах хүрээ	20 км хүртэл (passive splitter ашиглана)	DSL: 5 км хүрэхгүй Ethernet: 100 м – 1 км
Дамжуулах орчин	Шилэн кабель (fiber optic)	Зэс утас (DSL), коаксиал кабель (HFC)
Эрчим хүчний хэрэглээ	Бараг байхгүй (passive splitter ашигладаг)	Өндөр – идэвхтэй төхөөрөмж олон хэрэгтэй
Тоног төхөөрөмжийн тоо	Цөөн, энгийн (OLT, ONT, splitter)	Олон (DSLAM, модем, router, repeater гэх мэт)
Найдвартай байдал	Өндөр – шилэн кабелийн алдагдал бага, хөндлөн нөлөөнд тэсвэртэй	Харьцангуй бага – цахилгаан, радиогийн нөлөөлөл их
Үйлчилгээний төрөл	Triple Play: Интернэт, IPTV, Телефон	Үндсэндээ интернэт, зарим тохиолдолд ТВ

2-р хүснэгтээр хэрэглэгчдийн сүлжээний өргөнийг харьцуулахыг зорив. Gpon сүлжээний 1 хэрэглэгч хамгийн багадаа 20 mbps хурдыг авах боломжтой байна.



2-р зураг. GPON сүлжээний удирдлагын системийн ерөнхий харагдах байдал (Зураг хэрэглэгчдийн холбогдож байгаа GPON хаяг болон MAC хаяг, идэвхитэй байгаа зэрэг мэдээллүүдийг харуулж байна)

ДҮГНЭЛТ

GPON сүлжээ нь өндөр хурдны интернэтийн хэрэгцээ нэмэгдэж байгаа өнөө үед түгээмэл технологи болж байна. Энэ нь олон төрлийн үйлчилгээнд интернэт, телевиз, утас зэргийг нэг сүлжээнд нийлүүлж, хэрэглэгчдэд өндөр хурдтай, найдвартай үйлчилгээг санал болгодог. Тиймээс томоохон хотууд, байгууллагууд, мөн орон нутгийн хэрэглэгчид энэ технологийг хэрэглэвэл өндөр хурдтай өгөгдөл дамжуулах боломжтой, зардал багатай цахилгаан хэрэглээ багатай, засвар үйлчилгээ бага шаарддаг өргөтгөх боломжтой нь маш том давуу тал болж байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Ali Israr, Muhammad Junaid, Adil Israr, "Performance Analysis of Advance Optical Modulation Formats for GPON System", 2015 он 13 дахь International Conference on Frontiers of Information Technology (FIT), pp.77-80

[2] Stanislav Milanovic, "Case Study for a GPON Deployment in the Enterprise Environment", Journal of Networks, vol.9, no.1, 2014 он.

[3] Erik Weis, Rainer Hölzl, Dirk Breuer, Christoph Lange "GPON FTTH trial", 2010 оны 2 сарын 02.

СҮЛЖЭЭНИЙ ХАЛДЛАГА ИЛРҮҮЛЭХ, СЭРГИЙЛЭХ НЭЭЛТТЭЙ ЭХИЙН СИСТЕМИЙГ АШИГЛАХ СУДАЛГАА

Эрдэнийн ЭНХ-ОД[1], Ямхины ДАШДОРЖ[2], Хүчитийн УЯНГА[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: odko1988@gmail.com[1], dashdorj@must.edu.mn[2]

***Хураангуй*: Өдөр бүр тохиолдож байгаа сүлжээний аюул занал нь кибер аюулгүй байдалд үүсэж буй маш том эрсдэл юм. Ийм учраас энгийн галт ханын системээс илүү өртөг багатай, хялбар, хэрэглэгчид ээлтэй, өөрсдийн нөхцөлд тохируулан ашиглах боломжтой аюулгүй байдлын сонголтуудыг авч үзэх нь өнөөдөр чухал болоод байна. Тиймээс энэхүү өгүүлэлд нээлттэй эхийн буюу бүрэн чадлаар нь шууд ашиглах боломжтой халдлага илрүүлэх систем (IDS) болон халдлагаас сэргийлэх систем (IPS) гэж нэрлэгддэг шийдлийн давуу болон сул талуудын талаар авч үзэн IDS/IPS системийн ажиллах зарчмыг тайлбарлаж, туршилтын ажлыг гүйцэтгэх болно.**

Түлхүүр үг: Open source IDS/IPS, Denial-of-Service attack, Hping3 tool, Suricata

I. УДИРТГАЛ

Дэлхий дахинд кибер орон зайн хэрэглээ жил ирэх тусам ихсэж байна. Олон улсын статистик, судалгааны нэгдсэн сайт (statista)-ын 2025 оны 2 дугаар сарын байдлаар гаргасан тайланд дэлхий даяар 5.56 тэрбум интернэт хэрэглэгч байгаа нь дэлхийн хүн амын 67.9 хувийг эзэлж байна. Үүний 5,24 тэрбум нь буюу дэлхийн хүн амын 63,9 хувь нь сошиал медиа хэрэглэгчид бөгөөд үлдсэн 2.63 тэрбум хүн офлайн хэвээр байна [1].

SecureWorks-ийн 2024 оны 11 дүгээр сарын тайланд дурдсанаар дэлхий даяар кибер гэмт хэргийн хохирол 2025 он гэхэд 10.5 их наяд ам.долларт хүрнэ гэж таамаглаж байна. Энэ үр дүн нь санхүүгийн томоохон алдагдалд хүргэж болзошгүй бөгөөд үүнээс урьдчилан сэргийлэхийн тулд албан байгууллагууд IDS болон IPS зэрэг аюулгүй байдлын дэвшилтэт шийдлүүдийг ашиглан арга хэмжээ авах шаардлагатай байгааг харуулж байна [2].

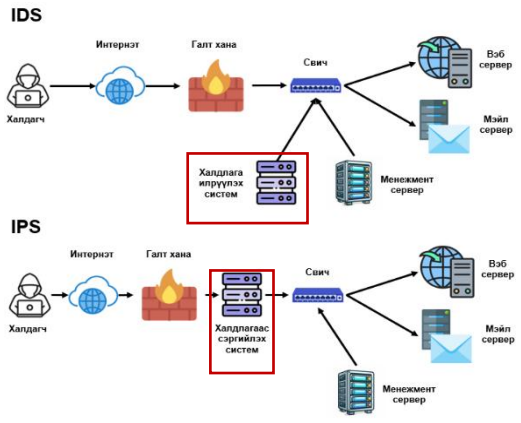
Судалгаанаас үзэхэд IDS шийдлийн халдлага илрүүлэх түвшин нь 80%-ас 98% хүртэл байдаг байна. IPS шийдлийг нэвтрүүлсэн байгууллагын зөрчилд хариу үйлдэл үзүүлэх хугацаа 50%-ас 75% хүртэл буурдаг байна. IPS нь халдлагыг илрүүлж, хамгаалах явцыг автоматжуулснаар илрүүлэхээс эхлээд хариу арга хэмжээ авах хүртэлх хугацааг бууруулдаг юм.

Verizon-оос гаргасан Мэдээллийн зөрчлийн судалгааны тайланд дурдсанаар, зөрчлийн 70 орчим хувь нь гаднаас чиглэсэн халдлагууд байсан бөгөөд IDS болон IPS нь хортой программ, ransomware зэрэг гадна аюулыг илрүүлэхэд чухал үүрэг гүйцэтгэдэг талаар дурдсан [3].

Тиймээс энэхүү өгүүлэлдээ сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх нээлттэй эхийн системүүдийг аюулгүй байдлын шийдэл болгон ашиглах давуу талуудыг судалгаа, шинжилгээнд тулгуурлан гаргаж, ажиллах зарчмыг харуул туршилтын ажлыг гүйцэтгэх болно.

II. НЭЭЛТТЭЙ ЭХИЙН IDS/IPS-ИЙН ТУХАЙ

Чөлөөт болон нээлттэй эхийн программ хангамж гэдэг нь хэн ч эх кодыг үзэх, судлах, үнэлэх дүгнэх болон шинэчлэн өөрчлөх боломжтой байдаг программ хангамж юм. Эх код нээлттэй байдаг учир хэн ч сайн дураараа программ хангамжийн дизайныг сайжруулах үйл ажиллагаанд оролцох боломжийг олгодог бөгөөд хаалттай эхийн программ хангамж нь хувилах эрх нь хязгаарлагдмал, эх код нь хэрэглэгчдэд харагддаггүй, патенттай өмчийн программ хангамжаас ялгаатай юм. Нээлттэй эхийн программ хангамжийг ашиглахын давуу талууд нь программ хангамж бүтээх зардлыг бууруулах, хамгаалалт болон тогтвортой байдлыг өндөрсгөх, хэрэглэгчдэд өөрсдийн техник хангамжаа илүү сайн удирдах боломж олгодог зэрэг юм.



1-р зураг. IDS/IPS-ийн ажиллах зарчим

Мөн нээлттэй эхийн үйлдлийн систем болох Linux нь өнөөдөр олон хүнд ашиг тусаа өгч, серверүүд, суурин компьютер, ухаалаг утаснууд зэрэг олон төхөөрөмжүүдийг ажиллуулсаар байна.

Байнгын хувьсан өөрчлөгдөж буй цахим аюулгүй байдлын орчинд хэрэглэгчдийн нууц мэдээлэл, эмзэг датаг хамгаалах нь байгууллага болон хувь хүний

хувьд хамгийн чухал зорилт болоод байгаа билээ. Энэхүү аюулгүй байдлын тогтолцооны бүрэлдэхүүн хэсэг нь халдлага илрүүлэх систем (IDS) ба халдлагаас урьдчилан сэргийлэх систем (IPS) юм. IPS/IDS системүүд нь хоёулаа сүлжээнд үүсэж болзошгүй аюулыг тодорхойлох, удирдах, хариу арга хэмжээ авах үүрэгтэй байдаг.

Intrusion Detection System (IDS) –

IDS нь сүлжээнд заналхийлсэн аливаа халдлага, сэжигтэй тохиолдлыг илрүүлж анхааруулга, мэдэгдлийг өгдөг болов ч тэдгээрийг блок хийх эсвэл зогсоох арга хэмжээ авдаггүй.

A. Халдлага илрүүлэх систем (IDS)

IDS нь сүлжээний урсгалыг сэжигтэй үйлдэл, аюулгүй байдлын нийтлэг зөрчлийг зөрчиж буй эсэхийг хянаж, болзошгүй халдлага, сэжигтэй үйлдэл сүлжээнд илэрсэн үед мэдээлэх, анхааруулах зарчмаар ажилладаг.

IDS-д гурван үндсэн төрөл байдаг:

Сүлжээнд суурилсан IDS (NIDS): Network based IDS (Сүлжээний орчинд шаардлагатай хэсэгт суурилагдаж сүлжээг бүхэлд нь хянах зориулалттай.)

Хостод суурилсан IDS (HIDS): Host based IDS (Ямар нэгэн хост, сервер дээр тусгайлан суурилагдаж, тухайн суусан хост, серверийн сүлжээнд анализ хийх зарчмаар ажилладаг.)

Вебд суурилсан IDS (WIDS): Web based IDS (Веб программууд болон түүний сүлжээний урсгал руу чиглэсэн халдлагыг илрүүлэхэд онцгойлон анхаарч ажилладаг.)

IDS нь сүлжээнд заналхийлсэн аливаа халдлага, сэжигтэй тохиолдлыг илрүүлж анхааруулга, мэдэгдлийг өгдөг болов ч тэдгээрт хаалт хийх эсвэл зогсоох арга хэмжээ авдаггүй.

B. Халдлагаас сэргийлэх систем (IPS)

IDS системээс ялгаатай нь сэжигтэй үйлдлийг илрүүлээд зогсохгүй тэдгээр халдлагаас сэргийлэх, хамгаалах арга хэмжээг авах боломжтой.

IPS нь мөн адил сүлжээнд суурилсан эсвэл хост дээр суурилсан байж болно. IPS нь сүлжээний пакетуудыг шалгаж, сэжигтэй үйлдэл илэрсэн тохиолдолд тухайн пакетыг блок хийх, холболтыг дахин эхлүүлэх, холбогдож буй эх үүсвэрийг хаах зэрэг яаралтай арга хэмжээг автоматаар авдаг ба энэ нь цаашлаад сүлжээнд ажиллаж буй аливаа сервер, сүлжээний төхөөрөмж зэргийг сүлжээний түвшний түгээмэл халдлагад өртөх, цаашлаад Application системийн түвшний халдлагад өртөхөөс урьдчилан сэргийлдэг энгийн бөгөөд үр дүнтэй аюулгүй байдлын системүүд юм.

C. Халдлага илрүүлэлтийн хувьд давуу болон сул талууд

Өгөгдөлд суурилсан (Signature based) илрүүлэлтийн үед худал эерэг үр дүн бага гардаг ч зөвхөн мэдэгдэж байгаа халдлагын өгөгдөл нь илэрч, шинэ бөгөөд хараахан тогтоогдоогүй аюул занал сүлжээний цоорхойг бий болгодог. Гажуудалд суурилсан (Anomaly based) илрүүлэлтийн үед илүү олон худал эерэг үр дүн гарч ирдэг ч зөв тохируулагдсан тохиолдолд алдаагүй, урьд өмнө мэдэгдээгүй аюулыг хүртэл илрүүлж чаддаг.

D. Snort (Нээлттэй эхийн IDS/IPS)

Snort-ийг 1998 онд Мартин Рош бүтээсэн бөгөөд сүлжээний халдлага илрүүлэх, сэргийлэх нээлттэй эхийн систем юм.

Snort-ийг гурван өөр аргаар хэрэглэж болно; tcpdump, пакет бүртгэгч эсвэл сүлжээний халдлагыг илрүүлэх, урьдчилан сэргийлэх систем гэх мэт пакет sniffer. Пакет sniffer болгон ашиглах үед Snort нь сүлжээний пакетуудыг уншиж, консол дээр харуулах ба пакет бүртгэгчийн хувьд Snort нь пакетуудыг диск рүү бүртгэх болно. Халдлага илрүүлэх горимд энэ нь сүлжээний урсгалыг хянаж, хэрэглэгчийн тодорхойлсон дүрмийн дагуу урсгалыг шинжлэх болно [6].

E. Bro (Нээлттэй эхийн IDS/IPS)

Bro нь 1998 онд Верн Пакссон үүсгэн байгуулагдсан бөгөөд нээлттэй эхийн UNIX дээр суурилсан сүлжээний халдлагыг илрүүлэх систем юм.

Bro идэвхгүй сүлжээний урсгалыг хянаж, хортой урсгалыг хайж байдаг. Энэ нь эхлээд сүлжээний траффикийг задлан шинжлэх замаар халдлагыг илрүүлж, дараа нь үйлдлийг хортой гэж үзсэн загвартай харьцуулахад чиглэсэн анализаторуудыг ажиллуулдаг. Шинжилгээнд тодорхой халдлага (гарын үсэг, үйл явдал) болон ер бусын үйл ажиллагаа (гажиг) илрүүлэх зэрэг орно.

Bro нь ихэвчлэн сүлжээний гол уулзвар дээр байрладаг бөгөөд энэ нь ирж буй болон гарч буй бүх урсгалыг хянах боломжтой. Bro нь сүлжээний урсгалыг цуглуулах, шүүх, дүн шинжилгээ хийх зэрэг функцуудыг хангадаг. Энэ нь түгээмэл протоколуудын нарийвчилсан дүн шинжилгээ хийх чадвартай бөгөөд энэхүү шинжилгээний үр дүн нь ажиглагдсан үйл ажиллагааг дүрсэлсэн хэд хэдэн үйл явдал юм [6].

F. Suricata (Нээлттэй эхийн IDS/IPS)

Suricata бол 'Нээлттэй мэдээллийн аюулгүй байдлын сангаас' боловсруулсан нээлттэй эх сурвалжийн халдлагыг илрүүлэх, сэргийлэх систем юм. Бета хувилбар нь 2009 оны 12-р сард гарсан бол анхны тогтвортой хувилбар нь 2010 оны 7-р сард гарсан. Suricata нь халдлагыг илрүүлэх талбарт шинэ санаа, технологийг нэвтрүүлэх зорилгоор бүтээгдсэн.

Нээлттэй Мэдээллийн Аюулгүй байдлын Сан (OISF) нь Suricata-д халдлага илрүүлэх, сэргийлэх дүрмийн багцыг олгодог бөгөөд аюулгүй байдлын оновчтой түвшнийг хадгалах үйл явцыг Suricata-ийн тусламжтайгаар хялбаршуулдаг [6].

Сүлжээнд галт хана нь зөвхөн заасан портууд дээр ирж буй болон гарах сүлжээний траффикийг зөвшөөрөх замаар сүлжээний аюулгүй байдлыг хангах чухал үүрэг гүйцэтгэдэг. Галт хана нь тодорхой порт эсвэл хууль ёсны порт руу илгээсэн сүлжээний траффик эсвэл аливаа халдлага, халдлагыг илрүүлэх зорилгоор бүтээгдээгүй. [8].

Жишээлбэл, TCP порт 80 дээр дотогшоо нэвтрэх боломжийг олгодог галт ханын дүрэм нь дотоод веб серверт алсаас хандах боломжийг олгоно. Халдагчид веб сервер рүү халдахдаа HTTP портыг ашиглаж болно. Энэ хувилбарт IDS нь веб траффикийн гарын үсэг болон сайн мэддэг халдлагын гарын үсгийн мэдээллийн сангийн хооронд харьцуулалт хийх замаар хууль ёсны траффик (зөвшөөрөгдсөн холболтууд) болон веб сервер рүү халдахыг оролдсон хоорондын ялгааг тодорхойлж чадна. Энд IDS нь сүлжээний администраторт ийм халдлагын талаар мэдэгдэж, зохих арга хэмжээ авахыг анхааруулж, чухал үүрэг гүйцэтгэдэг [9].

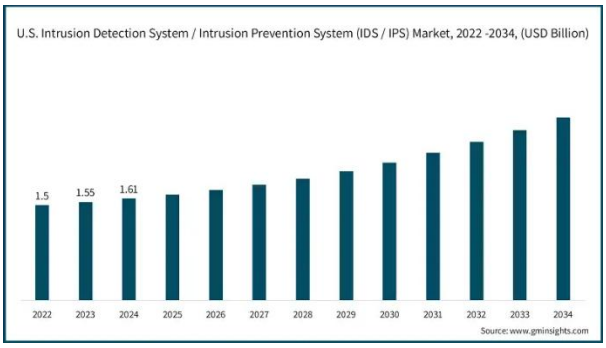
Нөгөөтэйгөөс, IPS нь довтолгооны оролдлогын үед зохих арга хэмжээг автоматаар авах замаар чухал үүрэг гүйцэтгэдэг. Жишээлбэл, веб сервертэй холболтыг таслах / хаах. Тиймээс IDS нь халдлагын оролдлого эсвэл хортой үйлдэл гарсны дараа бүртгэл үүсгэж, сүлжээний администраторт сэрэмжлүүлэх замаар идэвхгүй үйлдэл хийдэг бол IPS нь эдгээр үйл ажиллагааг идэвхтэй хянаж, сүлжээг хамгаалахын тулд эдгээр үйл ажиллагааны эсрэг арга хэмжээ авдаг. Тиймээс IDS болон IPS нь компьютерын сүлжээг хамгаалах сүлжээний түвшний хамгаалалтын үүрэг гүйцэтгэдэг [10].

НЭЭЛТТЭЙ ЭХИЙН IDS/IPS

1-Р ХҮСНЭГТ

д/д	***Халдлага илрүүлэх, сэргийлэх систем***	***Үнэлгээ***
1	Snort	9.1
2	Suricata	9
3	Zeek (Bro)	8.9
4	Maltrail	8.5
5	Security Onion	7.6
6	Kismet	7
7	Psad	6.8
8	Sagan	6.3

[a] Нийт 10 ононоос үнэлсэн болно.



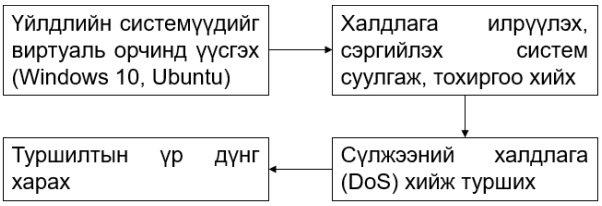
3-р зураг. Худалдааны IDS/IPS-ийн зах зээлийн өсөлтийн үзүүлэлт, тэрбум ам,доллараар гаргасан байдал [4]

III. ТУРШИЛТЫН АЖИЛ

Сүлжээний халдлага илрүүлэх систем (IDS) нь аюулгүй байдлын хамгаалалтын хамгийн өргөн хэрэглэгддэг хэрэгслүүдийн нэг юм. Эдгээр IDS-ийн зарим нь нээлттэй эх үүсвэртэй бөгөөд хамгийн өргөн хэрэглэгддэг нээлттэй эхийн IDS нь Snort болон Suricata юм. Эдгээр хоёр хэрэгсэл нь гарын үсэгт суурилсан болон хорлонтой үйл ажиллагааг тодорхойлох дүрэмд тулгуурладаг. Дүрмүүд нь агуулга, протокол, порт гэх мэт, түүнчлэн үйл ажиллагаа/траффикийн гарал үүсэлтэй холбоотой хортой үйл ажиллагааг тодорхойлдог - энэ тохиолдолд сэжигтэй IP хаягуудыг "хар жагсаалтад" оруулж, эдгээр IP хаягаас гаралтай траффик илэрвэл анхааруулга өгдөг. IDS-ийн тохиргооноос хамааран траффикийг сэрэмжлүүлэх боловч траффикийг зөвшөөрөх, эсвэл сэрэмжлүүлэг өгч зогсоохын тулд IDS нь халдлагаас урьдчилан сэргийлэх систем (IPS)-ийн горимд ажиллаж байх ёстой [7].

Уг туршилтын ажлаар үйлдлийн системүүдийг үүсгэж, халдлага илрүүлэх, сэргийлэх системийг суулган тохиргоо хийж, сүлжээнд туршилтаар халдлага хийн үр дүнг харах болно.

Халдлага илрүүлэх, халдлагаас сэргийлэх нээлттэй эхийн систем болох Suricata-г сонгох болсон шалтгаан нь суулгаж ашиглахад хялбар, тохиргоо хийхэд маш ойлгомжтой, бодит цаг хугацаанд аюулыг илрүүлэх, нөөцийг үр ашигтай ашиглах, аюулын олон талт дүн шинжилгээ хийх зэрэг давуу талуудтай.



4-р зураг. Туршилтын ажлын ерөнхий бүтэц

Туршилтын ажлыг гүйцэтгэхэд дараах төхөөрөмж, үйлдлийн систем, халдлагын хэрэгслийг ашигласан. Үүнд:

a) Зөөврийн компьютер (Dell G15, i5-13450, Memory 16gb, Disk 512gb SSD)

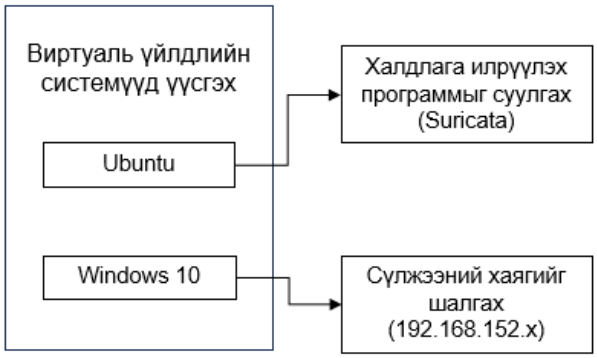
b) Виртуаль үйлдлийн систем (VMWare Workstation Pro-д Ubuntu, Windows 10 үүсгэх)

c) Нээлттэй эхийн систем (Suricata)

d) Халдлагын хэрэгсэл (hping3)

e) Халдлагын төрөл (Denial-of-Service /DoS/)

A. Туршилтын орчныг бэлдэх, халдлага илрүүлэх, сэргийлэх системийг суулгах



5-р зураг. Виртуаль орчинд үйлдлийн системүүд болон IDS/IPS-ийг суулгах

Командууд: [5]

sudo add-apt-repository ppa: oisf/suricata-stable

sudo apt update

sudo apt-get update && sudo apt-get install suricata

B. IDS/IPS тохиргоо хийх

6-р зураг. Халдлага илрүүлэх, сэргийлэх системд тохиргоо хийх

Командууд: [5]

cd /etc/suricata/

sudo nano suricata.yaml

Тохиргоо хийсэн байдал:

```
address-groups:
  HOME_NET: "[192.168.152.0/24]"
```

```
af-packet:
  - interface: ens33
```

```
nfq:
  mode: accept
  repeat-mark: 1
  repeat-mask: 1
```

```
  route-queue: 2
```

C. Suricata-д тохиргоо хийх

7-р зураг. Suricata болон rules директор шинээр үүсгэж, хяналтын дүрмүүдийг бичих

Командууд: [5]

cd /var/lib/

sudo mkdir suricata

cd suricata

sudo mkdir rules

sudo mv custom.rules /var/lib/suricata/rules

cd /var/lib/suricata/rules

sudo nano custom.rules

Тохиргоо хийсэн байдал:

```
alert icmp any any -> $HOME_NET any (msg:"ICMP uildel ilerlee!"; sid:123; rev:1;)
```

```
drop icmp any any -> $HOME_NET any (msg:"ICMP Drop hiilee"; sid:124; rev:1;)
```

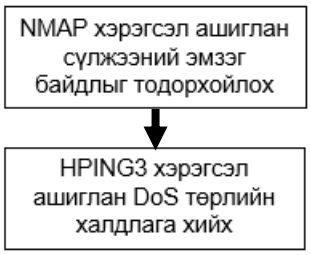
Сүлжээний халдлага илрүүлэх системийн хувьд виртуал орчинд үүсгэсэн Windows 10 үйлдлийн системээс сүлжээний урсгал (Ping) шалгахад дараах байдлаар харагдаж байна.

```
03/12/2025-02:30:40.503411  [**] [1:123:1] ICMP uildel ilerlee! [**] [Classifica
tion: (null)] [Priority: 3] {ICMP} 192.168.152.136:8 -> 192.168.152.135:0
03/12/2025-02:30:40.503442  [**] [1:123:1] ICMP uildel ilerlee! [**] [Classifica
tion: (null)] [Priority: 3] {ICMP} 192.168.152.135:0 -> 192.168.152.136:0
```

Сүлжээний халдлагаас сэргийлэх системийн хувьд дараах байдлаар харагдаж байна.

```
03/12/2025-02:30:40.503411  [**] [1:123:1] ICMP uildel ilerlee! [**] [Classifica
tion: (null)] [Priority: 3] {ICMP} 192.168.152.136:8 -> 192.168.152.135:0
03/12/2025-02:30:40.503442  [**] [1:123:1] ICMP uildel ilerlee! [**] [Classifica
tion: (null)] [Priority: 3] {ICMP} 192.168.152.135:0 -> 192.168.152.136:0
03/12/2025-02:53:37.011301  [Drop] [**] [1:124:1] ICMP Drop hiilee [**] [Classif
ication: (null)] [Priority: 3] {ICMP} 192.168.152.136:8 -> 192.168.152.135:0
```

D. Сүлжээний халдлага хийж туршиж



8-р зураг. Nmap хэрэгсэл ашиглан сүлжээний эмзэг портыг олж, халдлага үйлдэж турших

Командууд: [5]

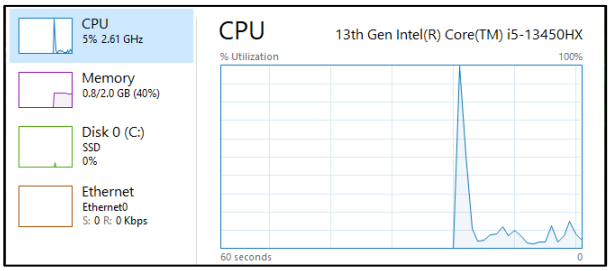
nmap -Pn 192.168.152.136

Гарсан үр дүн:

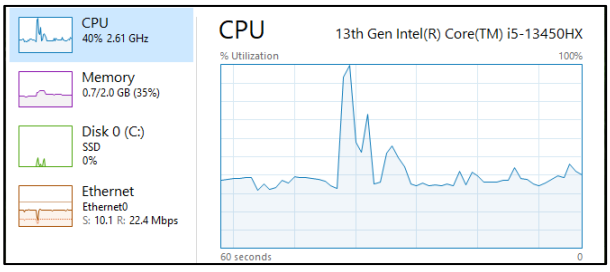
```
Nmap scan report for 192.168.152.136
Host is up (0.00059s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

sudo hping3 -S –flood -V -p 135 192.168.152.136

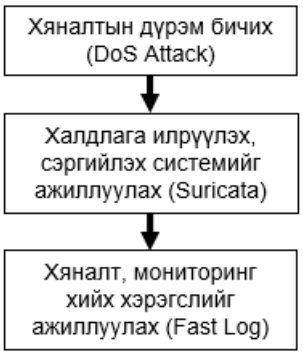
Өмнө:



Дараа:



E. Сүлжээний халдлагыг Suricata ашиглан хянах



9-р зураг. DoS халдлагыг илрүүлэх дүрмийг бичиж, лог бүртгэлийн хэсэгт үр дүнг харах

Командууд: [5]

alert tcp any any -> $HOME_NET any (msg:”Possible Denial-of-Service attack!”; flags:S; flow:stateless; threshold:type both, track by_dst, count 200, seconds 1; sid:10001; rev:1;)

sudo suricata -c /etc/suricata/suricata.yaml -i ens33

sudo tail -f /var/log/suricata/fast.log

Гарсан үр дүн:

```
03/12/2025-22:47:44.088124  [**] [1:10001:1] Possible Denial-of-Service attack!
[**] [Classification: (null)] [Priority: 3] {TCP} 192.168.152.135:31052 -> 192.1
68.152.136:135
03/12/2025-22:47:45.086664  [**] [1:10001:1] Possible Denial-of-Service attack!
[**] [Classification: (null)] [Priority: 3] {TCP} 192.168.152.135:52762 -> 192.1
68.152.136:135
```

СУДАЛГААНЫ ҮР ДҮН

Дээрх туршилтаар бид сүлжээний халдлага илрүүлэх, халдлагаас сэргийлэх нээлттэй эхийн системд өөрт тохирох, дурын дүрмүүдийг бичиж, хүссэн хяналтаа зохион байгуулах боломжтойг харуулж байна.

Туршилтын хэрэглэгч рүү зөвхөн нэг хостоос халдлага хийхэд процессорын болон сүлжээний ачаалал 8-10 дахин нэмэгдсэн байна. Үүнээс дүгнэхэд олон тооны хостоос зэрэг халдлага хийсэн тохиолдолд тухайн хэрэглэгч эсвэл серверийг үйлчилгээнээс бүр мөсөн гаргах боломжтой гэсэн үг юм. Уг халдлагыг Distributed Denial of Service гэж нэрлэдэг.

Уг нээлттэй эхийн системийг зөвхөн халдлага илрүүлэхэд ашиглахаас гадна хамгаалах байдлаар ашиглаж болох юм.

ДҮГНЭЛТ

Дэлхий дахины хэмжээнд кибер аюулгүй байдлыг хангах асуудал хурцаар тавигдаж байгаа өнөө үед байгууллагын болон хувийн сүлжээний аюулгүй байдлыг хамгаалах, халдлагаас урьдчилан сэргийлэх маш амар, хялбар шийдэл бол нээлттэй эхийн IDS/IPS шийдэл юм.

Хувь хүн болон албан байгууллагууд зардал гаргалгүй ашиглах, программ хангамжийн эх кодуудыг өөрсдөдөө тохируулах, хөгжүүлэлт хийх, хамгаалалтын дүрмүүдийг зохиох боломжийг олгоно.

Уг халдлагын эсрэг системийг илүү хөгжүүлэн хэрэглэгчид ээлтэй (User-friendly) интерфейстэй болгон ашиглах боломжтой.

IV. АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] https://www.statista.com/statistics/617136/digital-population-worldwide [Хандсан: 2025.03.08]

[2] https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024 [Хандсан: 2025.03.08]

[3] https://www.verizon.com/business/resources/reports/dbir/ [Хандсан: 2025.03.08]

[4] https://www.gminsights.com/industry-analysis/intrusion-detection-prevention-system-ids-ips-market [Хандсан: 2025.03.14]

[5] https://docs.suricata.io/en/suricata-7.0.2/rules/index.html

[6] Rødfoss, J. T. (2011). Comparison of open source network intrusion detection systems (Master's thesis).

[7] Asad, H., & Gashi, I. (2018). Diversity in Open Source Intrusion Detection Systems. Lecture Notes in Computer Science, 267–281. doi:10.1007/978-3-319-99130-6_18

[8] Sperotto, Anna, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras, and Burkhard Stiller. "An overview of IP flow-based intrusion detection." IEEE communications surveys & tutorials 12, no. 3 (2010): 343-356.

[9] Li, Wan, and Shengfeng Tian. "Preprocessor of intrusion alerts correlation based on ontology." In 2009 WRI International Conference on Communications and Mobile Computing, vol. 3, pp. 460-464. IEEE, 2009.

[10] Sivaraman, Vijay, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. "Network-level security and privacy control for smart-home IoT devices." In 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 163-167. IEEE, 2015.

ИХ СУРГУУЛИЙН ХОТХОНЫ ДОТООД СҮЛЖЭЭГ IPv6 ХУВИЛБАРТ ШИЛЖҮҮЛЭХ СУДАЛГАА

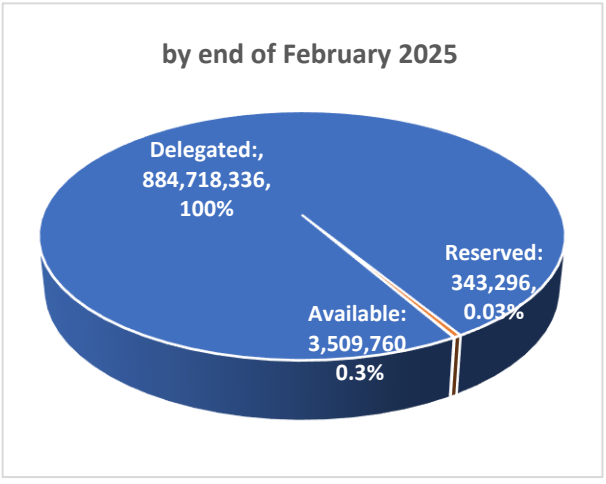
Дугарын ЖАВХЛАНТӨГС[1], Цогтбаатарын ЭНХТӨР[2], Лхагваагийн ОДОНЧИМЭГ[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар
Холбоо барих зохиогчийн и-мэйл хаяг: javkhlantugs@gmit.edu.mn[1], odno@must.edu.mn[2]

***Хураангуй*: Монгол германы хамтарсан ашигт малтмал, технологийн их сургуулийн хотхон нь Монголдоо анхны их сургуулийн хотхон загвар болон хөгжиж байна. Интернэтийн эцсийн хэрэглэгч нь суурин болон зөөврийн компьютероор хязгаарлагдахгүй мобайл, ухаалаг гэр ахуйн төхөөрөмжүүд, юмсын интернэт, цахилгаан машин зэрэгт ашиглагдаж улам бүр хэрэглээ нэмэгдэж байгаа өнөө үед интернэт сүлжээний ирээдүй болсон IPv6 хувилбарын IPv4 хувилбараас давуу тал, онцлогуудыг гаргаж ашиглан хотхоны дотоод сүлжээнд нэвтрүүлэх судалгааг хийлээ. Хичээлийн байр, лабораторийн байр, дотуур байрнууд гээд байнгын оршин суух 400+ оюутан, 70 багш ажилчдын хэрэглээний утастай, утасгүй интернэтийн, сургуулийн дагалдах системүүдийн сервер, ашигладаг тоног төхөөрөмжүүдийн сүлжээг IPv6 хувилбар нэвтрүүлэх, ирээдүйд бэлэн байдлыг хангах боломжийг судалж хэрэгжүүллээ.**

Түлхүүр үг: IPv4, IPv6, Хотхоны дотоод сүлжээ, Интернэт сүлжээний дараагийн үе.

I. УДИРТГАЛ

IPv4 протоколд суурилсан интернэт сүлжээ нь дэлхий нийтийг хамарсан өргөн хэрэглээтэй ч 2011 оноос хаягийн нөөцийн хомсдол орсон бөгөөд үүний шийдэл нь олон хаягуудыг цөөн тооны нийтийн хаяг руу хөрвүүлэх технологи (NAT Network Address Translation) хөгжүүлсэн нь IPv4 хаягийн нөөцийн ашиглалтыг түр хугацаанд уртасгасан ч [1] төгсгөлийн хэрэглэгчид хоорондын шууд холболт хийж чадахгүй, төгсгөлийн хэрэглэгчийг тодорхойлоход хүндрэлтэй зэрэг сул талууд ажиглагдсаар байна. APNIC буюу Ази Номхон Далайн орнуудын сүлжээний мэдээллийн төвөөс нийт олгох хаягийн 0,03% нөөцөлж 99,56% ийг шилжүүлсэн ба 0,39% нь ашиглах боломжтой байна.



1-р зураг. Ази номхон далайн бүсийн сүлжээний төвийн IPv4 хэрэглээ, нөөцийн мэдээлэл [5]

IPv6 протокол руу шилжих шилжилт дэлхий дахинд дунджаар 43%-тай үргэлжилж байгаа бол монгол улсын хувьд 30% - д хүрснээрээ дэлхийн хэмжээнд эхний 35 улсад багтаж байна [6]. IPv4 хувилбарыг халж IPv6 хэрэглээнд нэвтрүүлснээр хаягийн хомсдолыг шийдвэрлэхээс гадна сүлжээний түвшний хамгаалалт, гүйцэтгэлийг сайжруулна. Энэ нь интернэт хаягийн бүтцийг дахин тодорхойлж, юмсын интернэт болон бусад төхөөрөмжүүдийн шинэ шийдлийг гаргаж байгаа юм. МГТИС-ийн хотхоны байнгын оршин суух 400+ оюутан, 70 багш ажилчдын интернэт сүлжээг IPv4 протоколоос IPv6 шилжүүлэх нь зөвхөн хотхоны сүлжээний тохиргоог өөрчлөх биш, мөн бүх тоног төхөөрөмж, хаягийн менежмент болон аюулгүй байдлын бодлогыг шинэчлэх шаардлагатай ажил юм.

II. IPv6 ХУВИЛБАРТ ШИЛЖИХИЙН АЧ ХОЛБОГДОЛ, ШИЛЖИЛТИЙН ТЕХНОЛОГИУД

IPv6 нь дараах давуу талуудтай. IPv6 протокол нь нь 128 бит ($3.402.823.669*10^{38}$ = Их онон одох -100 ундециллион) бол IPv4 нь 32 бит (4.294.967.296 буюу 2^{32}=4.3 тэрбум хаяг) тай [3]. Энэ нь IPv6 нь IPv4 ээс 2^{96} дахин их нөөцтэй тул хаягийн хомсдолыг шийдсэн, ирээдүйд тэсвэртэй давуу талтай.

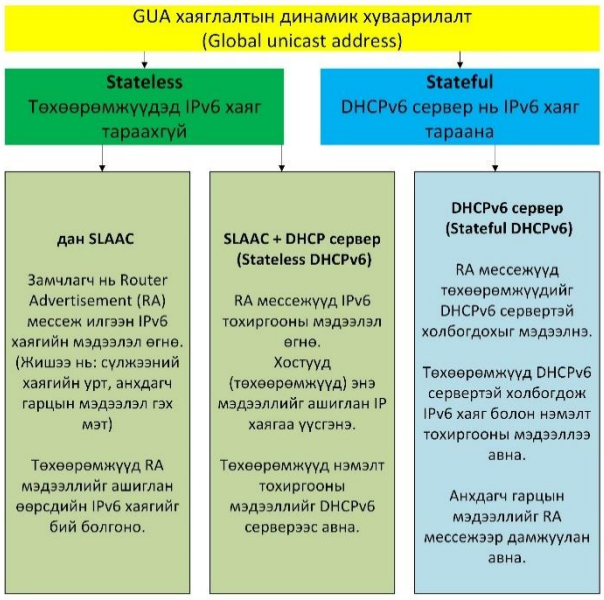
A. *Хаягын хомсдол*
B. *Замчлалыг нэгтгэх боломжгүй байдал*
C. *Хугацааны хоцролт /NAT, пакет боловсруулалт/ өгөгдлийг илүү хурдан дамжуулах боломж.*
D. *Төгсгөлийн төхөөрөмжөөс төгсгөлийн төхөөрөмж хооронд өгөгдөл дамжуулах боломж*

E. SLAAC Автоматаар хаягийн тохиргоо хийх боломжтой

IPv4 протоколоос IPv6 протокол руу шилжих шилжилтийн гурван үндсэн технологи байдаг.

1. Хос стек: IPv4 болон IPv6 тай сүлжээ сүлжээний дэд бүтцээр нэг зэрэг дамжих боломжтой.
2. Туннел: IPv4 сүлжээгээр дамжиж IPv6 сүлжээ хоорондоо холбогдоно. Энэ технологийг үндсэн хоёр хэсэгт ангилдаг.
   - Цэгээс цэг рүү
   - Цэгээс олон цэг рүү
3. NAT64 хөрвүүлэх: IPv6 протокол нь IPv4 протколруу хөрвөх, хөрвүүлсэн IPv4 протокол NAT64 ашиглаж гарцаар гарна [4].

IPv6 динамик хаяг олголт нь төхөөрөмжүүдэд динамик болон статик аргаар хаяг олгох бөгөөд динамик хаяг хуваарилалтыг хийхдээ SLAAC болон Stateful ашиглан гүйцэтгэнэ. SLAAC нь хост төхөөрөмжүүдийг төвлөрсөн серверээс хамааралгүйгээр өөрсдийн IPv6 хаягийг автоматаар олгодог бол Stateful нь нэгдсэн удирдлагаар IPv6 хаяг болон нэмэлт мэдээлэл хуваарилдаг.

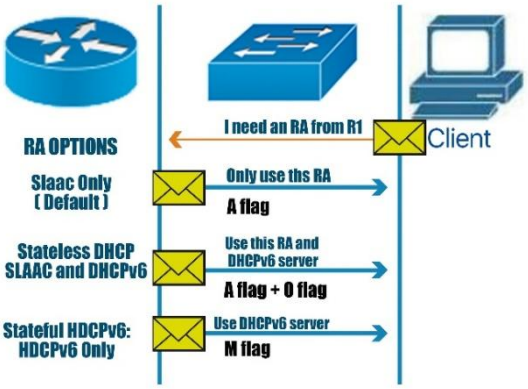


2-р зураг. *GUA* ***хаяглалтын*** *динамик хуваарилалтын аргууд*

SLAAC нь хостын төвлөрсөн сервер ашиглалгүйгээр Router Advertisement (RA) мессежийн мэдээлэлд үндэслэн автоматаар Global Unicast Address IPv6 хаяг үүсгэдэг. Энэхүү аргачлал нь төхөөрөмжүүдэд өөрийн интерфейсийн ID болон рүүтерээс ирсэн prefix мэдээллийг хослуулан хаяг үүсгэх боломжийг олгодог.

Router Advertisement (RA) мессеж нь 3 төрөл байдаг ба динамикаар хаяг үүсгэхэд A флаг + O флаг ашиглана.

A флаг (Autonomous Address-Configuration flag) нь Stateless Address Autoconfiguration (SLAAC) ашиглан IPv6 GUA хаяг үүсгэх боломжийг зааж өгдөг бол O флаг (Other Configuration flag) нь нэмэлт сүлжээний мэдээлэл (DNS гэх мэт)-ийг Stateless DHCPv6 сервер-ээс авах боломжтой.



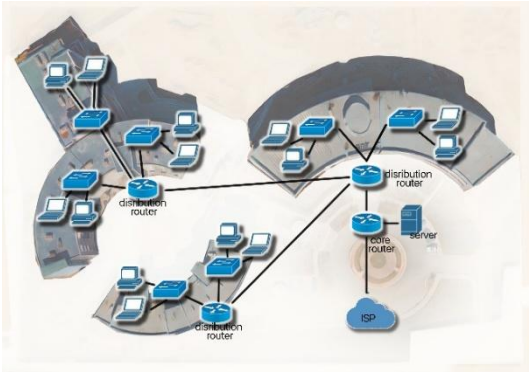
3-р зураг. IPv6 RA мессежын флагуудын ажиллагааны диаграм

III. МГТИС-ИЙН ДОТООД СҮЛЖЭЭГ IPv6 ПРОТОКОЛД ШИЛЖҮҮЛЭХ

Дэлхийн томоохон ISP компаниудын амжилттай шилжсэн туршлага болон урт хугацааны шилжилтийн стратегид үндэслэж хос стекийн аргыг ашиглаж IPv6 хувилбарт шилжилт хийнэ.

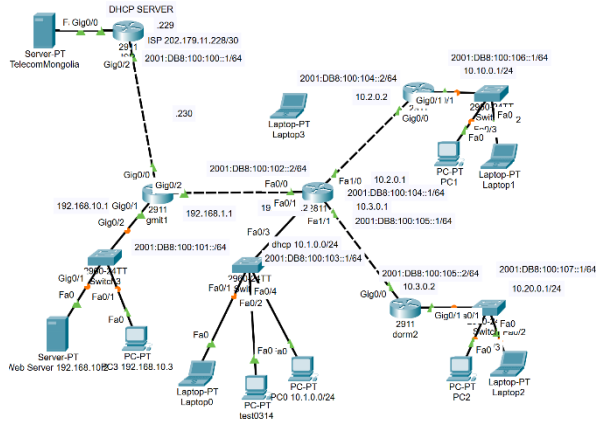
Өнөөгийн сүлжээний бүтэц:

Монгол германы хамтарсан ашигт малтмал, технологийн их сургууль нь Монголын цахилгаан холбоо ХХК-ны шилэн кабелийн интернэт үйлчилгээ ний хүрээнд IPv4 протоколын нэг хаяг түрээсэлж ашигладаг. Энэ нь сервер дээр портоор ялгах proxy сервер ашиглах шаардлага бий болгож байдаг.



4-р зураг. МГТИС-ийн сүлжээний ерөнхий бүтэц

Гарцын роутерын дараа байрлах gmit1 “1 POOL” роутер нь DHCP хаяг тараах ба gmit2 роутертэй холбогдсон dorm1, dorm2 роутерүүд тус бүр “1 POOL” -ээс DHCP хаяг авна. Хотхоны сүлжээ нь 12 рүтер, 35 свич, 4 удирдлагатай свич, 35 аксес пойнтоос бүрддэг. Иймээс бидний хэрэгжүүлэлт дараах бодит топологи дээр хийгдэж IPv6 хаяглалтыг gmit1 роутерыг сервер болгон SLAAC аргаар тохируулж бүх салбар луу хаягийг тарааж байна. Харин gmit1 сервер маань TelecomMongolia-гаас хаягаа түрээслэн авдаг.



5-р зураг. МГТИС хотхоны интернэт сүлжээний топологи

gmit1 серверийн тохиргоо:

```
ip cef
ipv6 unicast-routing
!
ipv6 cef
!
ipv6 dhcp pool gmit1-stateless
 dns-server 2001:DB8:100:100::1
 domain-name gmit1.local
!
```

```
!
interface GigabitEthernet0/0
 ip address 202.179.11.230 255.255.255.252
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:100::2/64
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 ipv6 traffic-filter gmit1_acl in
 ip nat inside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:101::1/64
 ipv6 nd managed-config-flag
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/2
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:102::1/64
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
ip nat inside source list gmit1nat interface GigabitEthernet0/0 overload
ip classless
!
ip flow-export version 9
!
ipv6 route ::/0 2001:DB8:100:100::1
```

6-р зураг. Gmit1 серверийн тохиргоо

Gmit2 роутерын тохиргоо:

```
ipv6 unicast-routing
!
no ipv6 cef
!
ipv6 dhcp pool gmit1-stateless
 dns-server 2001:DB8:100:100::1
 domain-name gmit2.local
'
```

```
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:102::2/64
 ipv6 ospf 1 area 0
!
interface FastEthernet0/1
 ip address 10.1.0.1 255.255.255.0
 ipv6 traffic-filter gmit2_acl in
 ip nat inside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:103::1/64
 ipv6 ospf 1 area 0
!
interface FastEthernet1/0
 ip address 10.2.0.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:104::1/64
 ipv6 ospf 1 area 0
!
interface FastEthernet1/1
 ip address 10.3.0.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
 ipv6 address 2001:DB8:100:105::1/64
 ipv6 ospf 1 area 0
!
interface Vlan1
 no ip address
!
router rip
!
ipv6 router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
'
```

7-р зураг. Gmit2 серверийн тохиргоо

Unicast routing протокол идэвхжүүлж, порт тус бүрд нь хаягийн хүснэгтээс хаяглаж, static route-р гарцын төхөөрөмжийн дараагийн hop-ийг зааж өгсөн. Хэрэглэгчдэд хаягаа SLAAC ашиглаж тараана. SLAAC нь гараар сүлжээний тохиргоо хийх эсвэл DHCP ашиглах шаардлагагүй автоматаар хаягийг тохируулдаг давуу талтай.

8-р зураг. IPv6 хаяг автоматаар авч байгаа жишээ

Одоогийн байгаа замчлагч төхөөрөмжөөр Микротик брэндийг ашигладаг ба Монгол улсын хувьд IPv6 хувилбарт бүрэн шилжээгүй тул хос стекийн аргаар шилжүүлэх аргыг сонгосон. Микротик рүүтер IPv4 ба IPv6 протокол хоёуланг зэрэг дэмжиж ажилладаг тул сүлжээний төхөөрөмжүүдийн шинэчлэл бага шаардагдана.

Шилжилтийн төлөвлөгөө

Интернэтийн үйлчилгээ үзүүлдэг Монголын цахилгаан холбоо ХХК нь IPv6 протоколын үйлчилгээ үзүүлдэггүй [7] тул Юнивишн ХХК-аас IPv6 протоколын үйлчилгээ авахаар төлөвлөлөө.

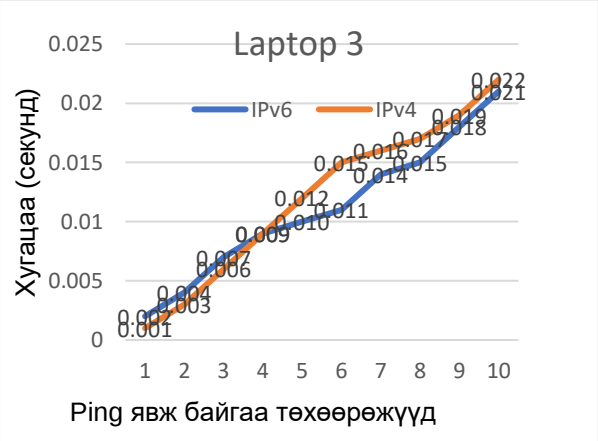
1-Р ХҮСНЭГТ. МОНГОЛ УЛСЫН IPS-НУУДЫН IPV6 НЭВТРЭЛТ

ASN	AS Name	IPv6 Capable	IPv6 Preferred
AS13335	CLOUDFLARENET	90.00%	86.00%
AS14593	SPACEX-STARLINK	69.57%	64.79%
AS17882	UNIVISION-AS-AP UNIVISION LLC	61.90%	57.40%
AS9484	MOBINET-AS-MN Mobinet LLC. AS Mobinet Internet Service Provider	19.51%	17.79%
AS141681	IMNL-AS-AP ONDO LLC	4.70%	4.45%
AS152337	NUM-AS-AP National University of Mongolia	3.43%	2.26%
AS55408	UNIVISION-AS-AP Univision LLC. To TTK STM1 UPSTREAM PROVIDER	5.65%	1.13%

IPv4-ийг өнөөдөр халаад оронд нь IPv6 хэрэглэх техникийн нөхцөлгүй тул хос стекийн [2] технологийг сонгон ашиглаж IPv6 протоколд шилжих хэрэгжүүлэлтийн топологид ашиглаж туршлаа. IPv6 протоколын хаягийн хүснэгтийг интернэтийн үйлчилгээ үзүүлэгч байгууллагаас 2001:db8:100:100::/56 prefix -тэй хаяг авч, дотоод сүлжээндээ 2001:db8:100:100::://64 prefix-тэй хаяг хэрэглэгчдэд олгохоор тооцоолж гаргалаа.

Туршилт, гүйцэтгэлийн хэмжилтүүд

IPv6 шилжилтийн өмнөх болон дараах сүлжээний гүйцэтгэлийг хэмжиж харьцуулалт хийв. Сүлжээнд илгээж, хүлээн авах траффикийн хугацааны хэмжилтийг симуляторын latop2-оос ISP -ийн чиглүүлэгч хүртэл ping ашиглаж гаргалаа.



9-р зураг. ICMP протоколын гүйцэтгэл: IPv6 ба IPv4-ийн харьцуулалт

2-Р ХҮСНЭГТ. ICMP ПРОТОКОЛЫН ГҮЙЦЭТГЭЛ: IPV6 БА IPV4-ИЙН ХАРЬЦУУЛАЛТ

	IPv6			
	Хугацаа (сек)	Сүүлийн төхөөрөмж	Очих төхөөрөмж	Төрөл
1	0.002	laptop2	swich5	ICMPv6
2	0.004	switch5	dorm2	ICMPv6
3	0.007	dorm2	gmit2	ICMPv6
4	0.009	gmit2	gmit1	ICMPv6
5	0.010	gmit1	isp	ICMPv6
6	0.011	isp	gmit1	ICMPv6
7	0.014	gmit1	gmit2	ICMPv6
8	0.015	gmit2	dorm2	ICMPv6
9	0.018	dorm2	swich5	ICMPv6
10	0.021	switch5	laptop3	ICMPv6

	IPv4			
	Хугацаа (сек)	Сүүлийн төхөөрөмж	Очих төхөөрөмж	Төрөл
1	0.001	laptop2	swich5	ICMP
2	0.003	switch5	dorm2	ICMP
3	0.006	dorm2	gmit2	ICMP
4	0.009	gmit2	gmit1	ICMP
5	0.012	gmit1	isp	ICMP
6	0.015	isp	gmit1	ICMP
7	0.016	gmit1	gmit2	ICMP
8	0.017	gmit2	dorm2	ICMP
9	0.019	dorm2	swich5	ICMP
10	0.022	switch5	laptop3	ICMP

Throughput (kbps) нь дараах томьёогоор тооцоологдоно:

$$\text{Throughput} = \frac{\text{TCP WindowSize}}{\text{RTT}} \quad [8]$$

Ping statistics for 202.179.11.229:
Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 24ms, Average = 3ms
Ping statistics for 2001:DB8:100:100::1:
Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 23ms, Average = 1ms

3-Р ХҮСНЭГТ. IPV4 БА IPV6 THROUGHPUT ХАРЬЦУУЛАЛТ

Сүлжээ	RTT (дундаж, ms)	Packet Size (bytes)	Throughput (kbps)
IPv4	3 ms	32	85.33 Kbps
IPv6	1 ms	32	256 Kbps

Аюулгүй байдлын шинжилгээ:

IPv6 ACL (Access Control List) тохиргоо, сүлжээний бодлого, хандалтын хяналтын механизмуудыг дараах байдлаар боловсруулна. Мөн алсын холболт үүсгэхээр бол IPSec VPN тохируулахаар төлөвлөж байна.

IPv6 ACL тохиргоо:

ipv6 access-list BLOCK_ICMP
deny icmp any
permit ipv6 any any

ДҮГНЭЛТ

Судалгааны хүрээнд МГТИС-ийн хотхоны дотоод сүлжээнд IPv6 хувилбарыг нэвтрүүлэх боломж, үр нөлөөг судаллаа. Судалгаанаас харахад IPv4-ээс IPv6 руу шилжих нь байгууллагын сүлжээний ирээдүй, аюулгүй байдал, уян хатан ажиллагааг дэмжихэд чухал ач холбогдолтой байна. Ж нь:

Хаягийн өргөтгөл: IPv4 нь хязгаарлагдмал хаяг гарцтай тул олон төхөөрөмж холбогдох үед дутагдал үүсдэг. IPv6 нь маш өргөн хаягийн санг санал болгож, ирээдүйд нэмэлт төхөөрөмж, IoT төхөөрөмжүүдийг дэмжих боломжийг нэмэгдүүлж байна.

Сүлжээний оновчтой байдал ба хурдасгуур сайжруулалт: IPv6 нь өгөгдөл дамжуулах болон чиглүүлэх үйлдлийг илүү үр дүнтэй зохицуулдаг учраас сүлжээний уян хатан ажиллагааг, хурдыг дээшлүүлдэг.

Аюулгүй байдлын дэмжлэг: IPv6 нь IPsec-ийн тусламжтайгаар сүлжээний аюулгүй байдлыг сайжруулах, өгөгдлийг нууцлах боломжийг нэмэгдүүлдэг.

Автомат тохиргоо: IPv6 нь Stateless Address Autoconfiguration (SLAAC) зэрэг технологийн тусламжтайгаар төхөөрөмжүүдийг автоматаар сүлжээгээр холбох боломжийг олгодог.

Ирээдүйн дэмжлэг ба инновац: Шилжилт нь байгууллагын сүлжээний ирээдүйд тулгарч болох технологийн шинэчлэл, олон талт хэрэглээнд бэлэн байхын тулд чухал алхам юм.

Эдгээр хүчин зүйлс нь байгууллагын сүлжээ илүү уян хатан, аюулгүй, болон өргөтгөлтэй байдлыг хангаж, бизнесийн үйл ажиллагааг тасралтгүй, үр дүнтэй байлгахад нөлөөлдөг.

Хугацааны хоцролтын симуляторын үр дүнгээр хугацааны хоцролтоор IPv4 хувилбараас IPv6 хувилбар бага байх нь харагдаж байна. Дотоод сүлжээнд холбогдож ажилладаг төхөөрөмжүүдээс IPv6 протоколыг дэмжидгүй төхөөрөмжийг солих, хаягийн түрээсийн төлбөр зэрэгт байгууллагаас нэмэгдэл зардал гарна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Ц.Энхтөр, Д.Эрдэнэтуяа, А.Гэрэлцэцэг, Ц.Манлайбаатар, Б.Нямлхам , “Монгол улсын IPv6 протоколруу шилжих үйл явцын өнөөгийн байдлын судалгаа” Хүрэл Тогоот Улаанбаатар, 2014.

[2] Gereltsetseg A, Enkhtur.Ts, Dashdorj.Y “Performance analysis on IPv6 transition technologies and transition metod

[3] Т.Наранмандах “Монгол улсын мэдээллийн сүлжээг интернэт протокол хувилбар 6-д шилжүүлэх судалгаа” 2011.

[4] Guan Xu, “Research on the Application of the IPv6 Network Protocol,” 2021.

[5] https://www.apnic.net/

[6] https://www.univision.mn/

[7] http://www.telecommongolia.mn/

[8] Sonal Telang Chandel, Sanjay Sharma, "Performance Evaluation of IPv4 and IPv6 Routing Protocols on WIred, Wireless and Hybrid Networks" 2016.

СҮЛЖЭЭНИЙ ТРАФФИКТ СУУРИЛСАН ХАЛДЛАГА ИЛРҮҮЛЭХ ХЭРЭГСЛИЙН ЭМЗЭГ БАЙДЛЫН СУДАЛГАА

Есөнжингийн ЭНХЗАЯА[1], Дондогмэгдийн БЯМБАДОРЖ[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: enkhzayayesunjin@gmail.com[1], d.byambadorj@must.edu.mn[2]

***Хураангуй*: Сүлжээний аюулгүй байдал нь өнөө үед хамгийн чухал асуудлуудын нэг болж, олон төрлийн халдлага илрүүлэх систем Intrusion Detection System – IDS хөгжиж байна. Гэвч эдгээр хэрэгслүүд өөрсдөө тодорхой эмзэг байдалтай байх магадлалтай бөгөөд үүнийг хакерууд ашиглах боломжтой. Энэхүү судалгааны ажил нь сүлжээний траффикт суурилсан халдлага илрүүлэх хэрэгслийн NIDS эмзэг байдлыг судалж, халдлагын илрүүлэлтийн үр ашиг, хязгаарлалтыг тодорхойлох, сүлжээний аюулгүй байдлыг сайжруулах шинэ арга боловсруулахыг зорьж байна. Үүний тулд халдлагын төрөл, арга техникийг судлан, орчин үеийн IDS технологийн давуу болон сул талуудыг тодорхойлно. Судалгааны эцсийн зорилго нь кибер аюулгүй байдлын шинэ шийдлүүдийг боловсруулах, байгууллага болон хувь хүмүүсийн мэдээллийг хамгаалахад хувь нэмэр оруулах явдал юм. Үүний үр дүнд сүлжээний аюулгүй байдлыг илүү үр дүнтэй хамгаалах боломж бүрдэх юм.**

Түлхүүр үг: malware, сүлжээний траффик шинжилгээ, кибер аюулгүй байдал, халдлага илрүүлэх аргачлал.

I. УДИРТГАЛ

Сүүлийн жилүүдэд мэдээллийн технологийн хурдацтай хөгжил нь байгууллагуудын үйл ажиллагааг цахим орчинд шилжихэд хүргэсэн. Үүний зэрэгцээ кибер халдлагын тоо, төрөл, нарийсал нэмэгдэж, байгууллагын сүлжээний аюулгүй байдал нэн тэргүүний асуудал болоод байна. Сүлжээний халдлага илрүүлэх систем (Network Intrusion Detection System – NIDS) нь сүлжээний траффикт шинжилгээ хийж, сэжигтэй үйл ажиллагааг илрүүлэх замаар хамгаалалтын чухал хэрэгсэл болж хөгжиж ирсэн. Гэвч одоогийн халдлага илрүүлэх системүүд нь шинэ төрлийн халдлагыг таних, хуурамч дохиоллын (false positive) түвшнийг бууруулах, бодит халдлагыг орхигдуулахгүй байх (false negative) зэрэг асуудлуудад тулгарч байна. Мөн траффикт суурилсан халдлага илрүүлэх хэрэгслүүд өөрсдөө эмзэг байдлуудтай байх магадлалтай, энэ нь хакеруудын хувьд бай болох боломжийг нэмэгдүүлдэг.

Энэхүү судалгааны ажил нь сүлжээний траффикт суурилсан халдлага илрүүлэх хэрэгслийн эмзэг байдлыг судалж, сул талуудыг тодорхойлох, улмаар сайжруулах боломжуудыг санал болгоход чиглэгдэнэ. Судалгааны хүрээнд:

Халдлага илрүүлэх аргачлалуудын үр ашиг, хязгаарлалтыг тодорхойлох

Сүлжээний траффикт шинжилгээ хийж, халдлагын төрлүүдийг ангилах

NIDS-ийн эмзэг байдлыг үнэлэх, сайжруулах боломжуудыг тодорхойлох зэрэг асуудлуудыг хөндөнө.

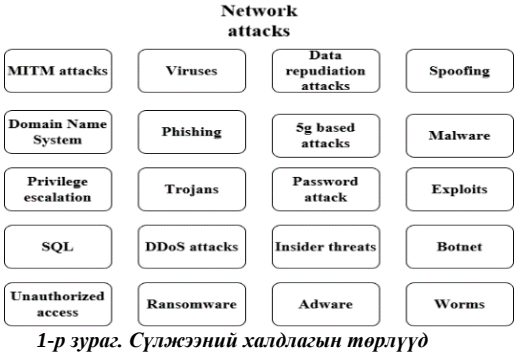
Судалгааны дүнд гарсан үр дүн нь сүлжээний аюулгүй байдлын хамгаалалтыг сайжруулах, байгууллагын мэдээллийн системийг хамгаалах бодлого боловсруулахад ач холбогдолтой байх болно.

II. ОНОЛЫН ҮНДЭС

A. *Сүлжээний траффик*

Сүлжээний халдлага нь байгууллагын сүлжээнд зөвшөөрөлгүй нэвтэрч, мэдээлэл хулгайлах эсвэл бусад гэмт үйлдэл хийх зорилготой оролдлого юм. Сүлжээний халдлагын хоёр үндсэн төрлүүд байдаг:

- Идэвхгүй (Passive): Халдагчид сүлжээнд нэвтэрч, мэдээллийг хянаж эсвэл хулгайлах боломжтой боловч өгөгдөлд ямар ч өөрчлөлт оруулахгүй, түүнийг хэвээр нь орхино.
- Идэвхтэй (Active): Халдагчид зөвшөөрөлгүй нэвтэрч, өгөгдлийг өөрчилж, устгах, шифрлэх эсвэл бусад байдлаар халдах үйлдлийг хийдэг.[7]



1-р зураг. Сүлжээний халдлагын төрлүүд

B. *Халдлага илрүүлэх системийн IDS үндсэн ойлголт*

Халдлага илрүүлэх систем (IDS) нь сүлжээний орчинд болзошгүй халдлагыг илрүүлж, урьдчилан сэргийлэх чухал хэрэгсэл юм.

•**Траффикийн шинжилгээ (Traffic Analysis)**: Сүлжээний өгөгдлийн урсгалыг хянаж, ерөнхийдөө ашуултай үйлдлүүдийг олох.

• **Хэрэглэгчийн үйлдлүүд (User Behavior Analysis)**: Хэрэглэгчдийн үйлдлийг хянаж, хэт олон хандах, сэжигтэй өөрчлөлтүүдийг илрүүлэх.

a. IDS-ийн төрөл:

- Томоохон системийн (Host-based IDS, HIDS): Энэ төрлийн IDS нь зөвхөн тухайн сервер эсвэл компьютерын үйлдлийг хянаж, үйлдлийн систем, программ хангамж болон бусад ашуултай үйлдлүүдийг илрүүлдэг.
- Сүлжээний (Network-based IDS, NIDS): Энэ төрлийн IDS нь сүлжээнд хөдөлж буй өгөгдөл болон мэдээллийг хянаж, сүлжээн дээрх халдлагуудыг илрүүлнэ.
- Олог төрөлт (Hybrid IDS): Хоёр системийг хослуулсан IDS нь хослуулан хэрэглэж болно.

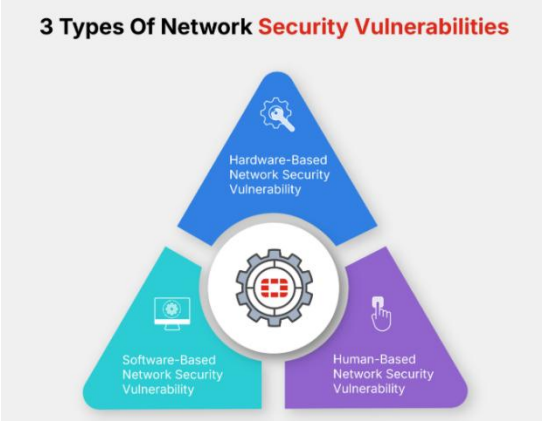
b. IDS нь ерөнхийдөө доорх хоёр үндсэн аргаар ажилладаг:

- Гарын үсэгт суурилсан (Signature-based) арга – Өмнө нь тодорхойлогдсон халдлагын загваруудтай харьцуулан халдлагыг илрүүлдэг. Энэ арга нь мэдэгдэж буй халдлагыг үр дүнтэй илрүүлдэг боловч шинэ, үл мэдэгдэх халдлагын хувьд сул талтай.
- Шинж чанарт суурилсан (Anomaly-based) арга – Сүлжээний хэвийн хөдөлгөөний загварыг тодорхойлж, түүнээс хазайсан траффикийг халдлага гэж ангилан илрүүлдэг. Энэ нь шинэ төрлийн халдлагыг таних боломжтой ч хуурамч сэрэмжлүүлэг өгөх магадлалтай.[8]

C. *Сүлжээний ашуултүй байдлын эмзэг байдлын ерөнхий ангилал*

Сүлжээний ашуултүй байдлын эмзэг байдал нь системийн техник хангамж, программ хангамж, удирдлага, байгууллагын бодлого, ашиглагдах боломжтой сул талуудыг багтаасан өргөн хүрээний ойлголт юм. Сүлжээний ашуултүй байдлын эмзэг байдлын үнэлгээ нь байгууллагуудад чухал ач холбогдолтой байдаг. Учир нь вирус эсвэл хортой программ хангамж (malware) системд нэвтэрч, бүхэл бүтэн сүлжээг халдварлуулах эрсдэлтэй. "Common Vulnerabilities and Exposures" (CVE) гэх мэт эмзэг байдлууд нь сүлжээнд холбогдсон төхөөрөмжүүд болон бусад сүлжээнүүдэд халдлага хийх боломжийг бүрдүүлж, ноцтой хохирол учруулж болзошгүй. Бүрэн хэмжээний сүлжээний ашуултүй байдлын үнэлгээ нь сүлжээний ашуултүй байдлын аудит хийх, эрсдэлийн үнэлгээг зохион байгуулах зорилгоор эмзэг байдлын эрсдэлийн хүснэгт боловсруулах зэрэг үйл ажиллагааг багтаана. Мэдээллийн технологийн (IT) хэлтэс болон кибер ашуултүй байдлын мэргэжилтнүүд сүлжээний ашуул занал, эмзэг байдал, халдлагуудыг байнга хянаж байдаг. Ялангуяа өндөр ур чадвартай, төрийн дэмжлэгтэй хакеруудын зүгээс учирч болзошгүй ашуулыг анхааралтай ажиглах шаардлагатай. Сүлжээний ашуултүй байдлын 3 төрлийн эмзэг байдлыг дараах гурван үндсэн ангилалд хуваж болно:

- Техник хангамжийн (hardware) эмзэг байдал
- Программ хангамжийн (software) эмзэг байдал
- Хүний хүчин зүйлээс (human security) үүдэлтэй эмзэг байдал [9]



2-р зураг. Сүлжээний ашуултүй байдлын эмзэг байдлын төрлүүд [9]

D. Ашуултүй байдлын мэргэжилтнүүдийн түгээмэл ашиглаж байдаг хэрэгслийн эмзэг байдлын судалгааны ажлын хүрээнд сүлжээний хяналтын хэрэгслүүд уруу чиглэсэн халдлагууд нь мэдээллийн ашуултүй байдалд хэрхэн нөлөөлж байгааг судалсан. Уг халдлага нь ихэвчлэн сүлжээний мониторинг болон ашуултүй байдлын хяналтын системүүдийн үйл ажиллагааг доголдуулах, хуурамч мэдээлэл тараах, эсвэл тухайн системийг бүрэн ажиллагаагүй болгоход чиглэдэг. Энэхүү халдлагын зорилго нь сүлжээний ашуултүй байдлыг хангах, халдлага илрүүлэх болон урьдчилан сэргийлэх үүрэг бүхий системүүдийг (жишээлбэл, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Security Information and Event Management (SIEM) системүүд, NetFlow анализатор зэрэг) хэвийн ажиллах боломжгүй болгох явдал юм.

III. СУДАЛГААНЫ АРГАЧЛАЛ

А. *Судалгаанд ашигласан өгөгдөл ба орчин*

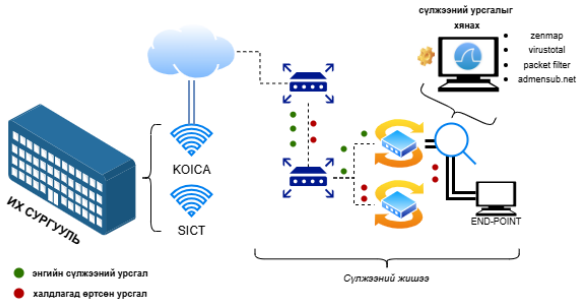
Энэхүү судалгаа нь туршилт, анализ, халдлага илрүүлэх аргачлалд суурилсан бөгөөд судалгааны хүрээнд сүлжээний траффикт шинжилгээ хийх, порт сканер ашиглах, аномали илрүүлэх аргыг хэрэгжүүлсэн. Судалгааны эхний шатанд Wireshark ашиглан сургуулийн public утасгүй сүлжээний урсгалыг барьж авсан бөгөөд үүний дараа Zenmap (Nmap) ашиглан сүлжээнд нээлттэй портуудыг илрүүлсэн. Барьж авсан траффикт статистик шинжилгээ хийж, хэвийн бус (аномали) үйлдлүүдийг тодорхойлсноор бодит халдлагыг илрүүлэх боломж бүрдсэн. Халдлагыг илрүүлэхэд ашигласан хэрэгслүүдийг 1-р хүснэгтээр харуулав.

1-Р ХҮСНЭГТ

№	Туршилтад ашигласан хэрэгслүүд
1	Wireshark
2	Zenmap (Nmap)
3	Windows 11 laptop
4	Advanced IP Scanner

А. *Судалгаанд ашигласан арга техник*

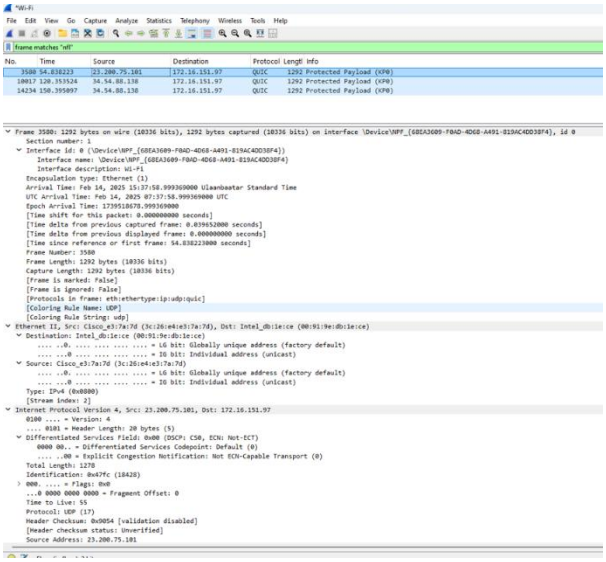
Судалгаанд сургуулийн public утасгүй сүлжээний орчинд Wireshark болон Zenmap (Nmap) хэрэгслүүдийг ашиглан өгөгдөл цуглуулж, траффикт анализ хийсэн. Илэрсэн бодит халдлагын шинж чанарыг тодорхойлж, боломжит халдагчийг үнэлэх зорилгоор урсгалын хандалтыг судалж, нээлттэй портуудын аюулгүй байдлыг үнэлэв. Судалгааны явцад сүлжээнд орж ирсэн болон гарсан урсгалын хандалтыг шинжилж, хэвийн бус загваруудыг ялган таньж, бодит халдлагыг тодорхойлох аргачлалыг ашигласан. Гэвч судалгаа сургуулийн public сүлжээнд хязгаарлагдсан тул халдлагын нарийвчилсан мөрдлөг хийх боломж хязгаарлагдмал байлаа. Илрүүлсэн бодит халдлагын эх сурвалжийг бүрэн тодорхойлохын тулд нэмэлт мөрдлөг хийх шаардлагатай тул 3-р зурагд дэлгэрэнгүй орчны диаграмм харуулав.



3-р зураг. Туршилтын орчны сүлжээний топологи

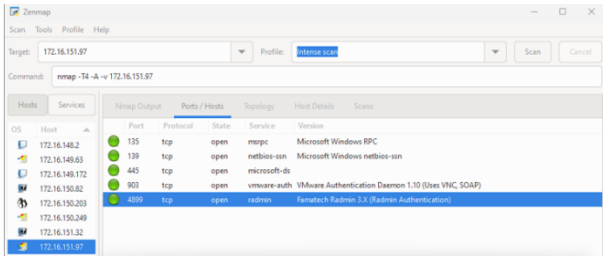
IV. ТУРШИЛТ, ҮР ДҮН

Бид энэхүү ажлын хүрээнд Wireshark хэрэгслийн тусламжтай сүлжээгээр дамжиж байгаа өгөгдлөөс халдлагатай пакет байгаа эсэхийг шалгахын тулд frame matches “nfl” шүүлтүүрийн тусламжтай IP 23.200.75.10-аас IP 172.16.151.97 хаяг руу QUIC өгөгдөл илгээж байгааг 4-р зурагд харуулав.



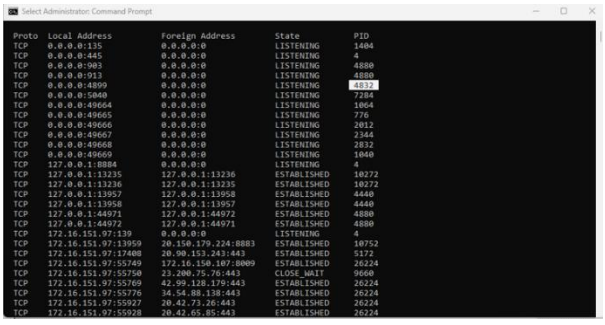
4-р зураг. IP 23.200.75.10-аас IP 172.16.151.97 хаяг руу QUIC өгөгдөл илгээж байгаа байдал

IP 172.16.151.97 IP хаягийг Zenmap хэрэгслийн тусламжтай дүн шинжилгээ хийж үзэхэд порт 4899 гэсэн radmin сэжиг бүхий программ байгааг 5-р зурагд харуулав.



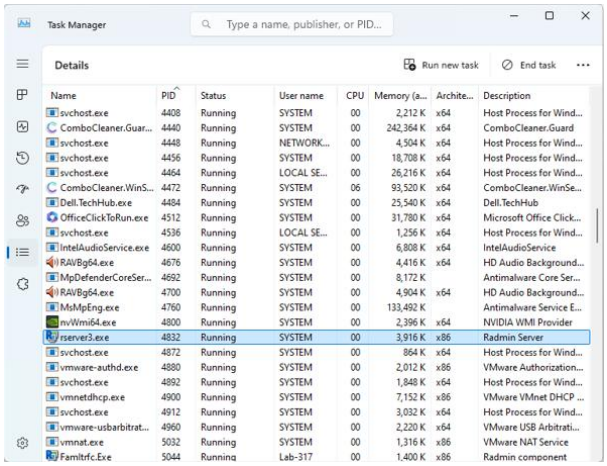
5-р зураг. порт 4899 гэсэн radmin сэжиг бүхий программ

Цаашид бид уг хост дээр нарийвчилсан дүн шинжилгээ хийхийн тулд сүлжээний холболтын төлөв байдал болон TASK менежер дээр динамик дүн шинжилгээ хийсэн үр дүнг 6-р зураг болон 7-р зурагд харуулав.



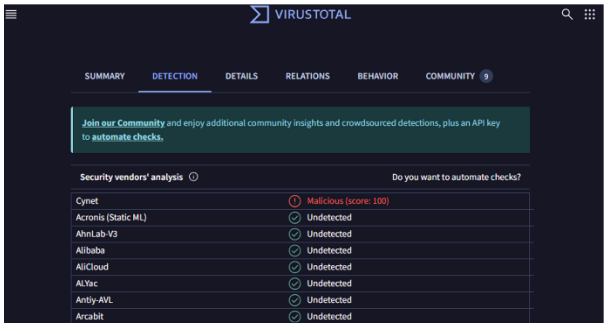
6-р зураг. Windows үйлдлийн системийн сүлжээний холболтын төлөв байдал

6-р зурагд харуулсан сүлжээний төлөв байдал дээр дүн шинжилгээнээс харахад порт 4899-ийг системийн PID 4832 бүхий программыг чагнаж байгааг тодорхойлсон. PID 4832-ийг нарийвчлан судалж үзэхийн тулд үйдлийн системийн TASK менежер дээрээс нарийвчилсан судалгааг 7-р зурагд харуулав.



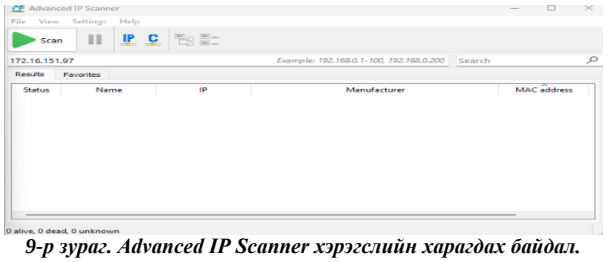
7-р зураг. PID 4832 дээрх rserver3.exe программ ачаалгаж байгаа байдал

7-р зурагд харуулсан rserver3.exe программыг анхан шатны статик дүн шинжилгээний арга болох нээлттэй эхийн хорт программ илрүүлэх аргачлалаар сэжиг бүхий rserver3.exe программыг www.virustotal.com сайтад ачааллаж үзсэн үр дүнг 8-р зурагд харуулав.



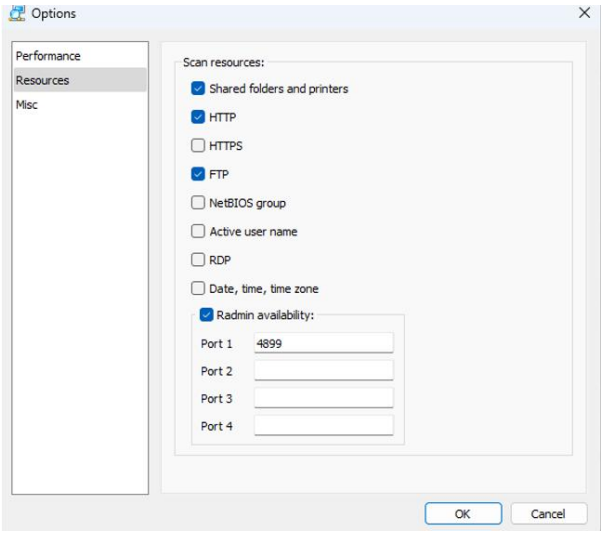
8-р зураг. rserver3.exe программ нь хортой код агуулж байгаа байдал

8-р зураг харуулсан Rserver3.exe нь хортой код агуулж байгааг тодорхойлсон уг программыг нарийвчлан судлахын тулд интернэт хайлт хийх замаар шалгахад Advanced IP Scanner хэрэгсэл болохыг 9-р зурагд харуулав.



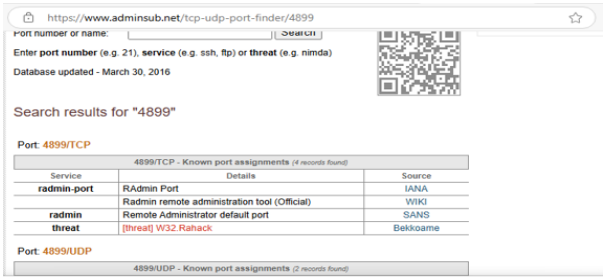
9-р зураг. Advanced IP Scanner хэрэгслийн харагдах байдал.

9-р зурагд харуулсан Advanced IP Scanner хэрэгслийн нарийвчилсан судалгаа хийж үзэхэд тохиргооны хэсэг порт 4899-аар тохируулсан байгааг 10-р зурагд харуулав.



10-р зураг. Advanced IP Scanner хэрэгслийн тохиргооны хэсэг

10-р зурагд харуулсан Advanced IP Scanner хэрэгслийн тохиргооны хэсэг дээрх порт 4899-ийг онлайн хайлтын тусламжтай шалгаж үзэхэд W32 Rahack хортой программ болохыг 11-р зурагд харуулав.



11-р зураг. www.adminsub.net онлайнаар тандалт хийж байгаа байдал

11-р зурагд харуулсан Rahack нь компьютерын системд нэвтэрч, хортой үйлдлүүдийг гүйцэтгэх зорилготой хортой программ хангамж юм. Энэ төрлийн хортой программууд нь ихэвчлэн хэрэглэгчийн мэдэлгүйгээр суулгагдаж, хувийн мэдээлэл хулгайлах, системийн ажиллагааг алдагдуулах зэрэг сөрөг нөлөө үзүүлдэг.

ДҮГНЭЛТ

Бид судалгааны ажлын хүрээнд сүлжээний инженерүүдийн түгээмэл хэрэглэж байгаа Advanced IP Scanner хэрэгслийн эмзэг сул талын судалгааг статик болон динамик дүн шинжилгээний аргачлалаар шинжилгээ хийж үзсэн. Уг хэрэгсэл нь хостод порт 4899-ын тусламжтай хакеруудад өгөгдөл дамжуулах болон хуурамч мэдээлэл илгээж байгааг тодорхойлсон. Иймээс бид цаашид уг судалгаан дээр

тулгуурлаж халдлага илрүүлэх программ хөгжүүлэх шаардлагатай гэж дүгнэж байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA, USA: Pearson, 2023. W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA, USA: Pearson, 2023.

[2] S. Bhuyan, D. Bhattacharyya, and J. Kalita, "Network anomaly detection: Methods, systems and tools," IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 303–336, Mar. 2014.

[3] P. W. Singer and A. Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford, UK: Oxford University Press, 2014.

[4] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive dataset for network intrusion detection systems (NIDS)," in Proceedings of the Military Communications and Information Systems Conference (MilCIS'15), Canberra, ACT, Australia, 2015, pp. 1–6.

[5] A. Abbas, "Subject review: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)," ResearchGate, Sep. 207

[6] J. Lee, M. Kim, and S. Park, "A deep learning-based network intrusion detection system: A comprehensive performance analysis," *Data in Brief*, vol. 48, p. 109293, Apr. 2023.

[7] Cynet, "Network attacks and network security threats," *Cynet*, [Online].

[8] Fortinet, "Intrusion Detection System," Fortinet, [Online].

[9] Fortinet, "Network Security Vulnerability," *Fortinet,* [Online].

ТӨРИЙН АЛБАНЫ МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ХҮНИЙ НӨӨЦИЙН ӨНӨӨГИЙН БАЙДАЛ, БОДЛОГО, ТУЛГАМДАЖ БУЙ АСУУДАЛ, ШИЙДЭЛ

Дүгэржавын ДАВААСАМБУУ[1], Дамдинсүрэнгийн ЛХАМСҮРЭН[2]

[1]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

[2]Монгол улс, Улаанбаатар, Статистикийн үндэсний хороо

Холбоо барих зохиогчийн и-мэйл хаяг: davaasambuu163131@gmail.com[1]

***Хураангуй*: 21-р зуунд мэдлэгт суурилсан нийгэм, цахим засаглал, өгөгдөлд суурилсан удирдлага, хиймэл оюун ухаан зэрэг дэвшилтэт технологиудын хөгжил нь төрийн байгууллагын үйл ажиллагаанд мэдээллийн технологийн гүйцэтгэх үүрэг, ач холбогдлыг улам бүр нэмэгдүүлж байна. Үүнтэй уялдан төрийн байгууллагын мэдээллийн технологийн чиг үүргийг хэрэгжүүлэгч хүний нөөцийн төлөв байдал, тэдний чадавх, ур чадвар, хөгжлийн хэрэгцээ нь байгууллагын үр ашигтай, ил тод, хүртээмжтэй үйл ажиллагааны үндэс суурь болж байна. Монгол Улсын төрийн байгууллагууд сүүлийн жилүүдэд МТ-ийн шинэчлэл, цахим шилжилтийг эрчимжүүлэхэд анхаарч байгаа ч энэ үйл явцыг хэрэгжүүлэгч хүний нөөцийн төлөвшил, хөгжлийн бодлого, түүний хэрэгжилт, үр дүнг цогцоор нь авч үзэх шаардлага тулгарсаар байна. Төрийн байгууллагын МТ-ийн чиг үүргийг гүйцэтгэгч ажилтнуудын ур чадвар, тасралтгүй хөгжлийн бодлого, сургалтын хүртээмж зэрэг нь байгууллагын мэдээллийн аюулгүй байдал, системийн найдвартай ажиллагаа, инновацын хэрэглээнд шууд нөлөөлдөг. Иймд энэхүү судалгаагаар төрийн байгууллагын мэдээллийн технологийн чиг үүргийг хэрэгжүүлэгч хүний нөөцийн одоогийн байдал, хөгжлийн бодлого, сургалт, нийгмийн баталгааны хөтөлбөрийн хэрэгжилт, үр нөлөөг тодорхойлж, тулгамдаж буй асуудлыг илрүүлэн, хөгжлийн бодлогын төлөвлөлтөд ашиглахуйц санал, зөвлөмж боловсруулахыг зорьж байна.**

Түлхүүр үг: дижитал шилжилт, цахим ур чадвар, сургалт хөгжүүлэлт, нийгмийн баталгаа, хүний нөөцийн бүрдүүлэлт.

I. УДИРТГАЛ

Төрийн байгууллагын үйл ажиллагааны шинэчлэлийн нэг хэлбэр нь мэдээллийн технологийн дэвшлийг үйл ажиллагаандаа нэвтрүүлж, цахим засаг буюу ухаалаг засаглалын тогтолцоог бүрдүүлэн, хөгжүүлэх явдал юм.

“Алсын хараа 2050” Монгол улсын урт хугацааны хөгжлийн бодлого, “Монгол Улсыг хөгжүүлэх таван жилийн үндсэн чиглэл”, “Шинэ сэргэлтийн бодлого”, Монгол Улсын Засгийн газрын 2024-2028 оны үйл ажиллагааны хөтөлбөр зэрэг дунд хугацааны хөгжлийн бодлогын баримт бичигт нийгэм, эдийн засгийн бүх салбарт мэдээллийн технологийн инновац, их өгөгдлийн шинжилгээ, хиймэл оюун ухаан ашиглах боломжийг нээх, төрийн үйлчилгээ, үйл ажиллагаанд дахин инженерчлэл хийж, оновчтой, үр ашигтай засаглалыг бэхжүүлэх, төрийн их өгөгдлийн мэдээллийн санг бүрдүүлэн түүнийг бодлого боловсруулах, шийдвэр гаргах, тоон эдийн засгийн хөгжлийг эрчимжүүлэхэд ашиглаж, үндэсний эдийн засгийн үр ашгийг нэмэгдүүлэх зорилтыг тавин ажиллаж байна.

Дээрх арга хэмжээг хэрэгжүүлэн ажиллахад төрийн байгууллагад ажилладаг мэдээллийн технологийн чиглэлийн хүний нөөцийн бүрдүүлэлт, сургалт хөгжил, нийгмийн баталгааг хангах зэрэг хүний нөөцийн бодлого, үйл ажиллагаа, түүний үр дүн чухал ач холбогдолтой юм.

Иймд Төрийн албаны зөвлөлөөс Төрийн захиргааны байгууллагуудын мэдээллийн технологийн чиг үүрэг хэрэгжүүлдэг хүний нөөцийн бүрдүүлэлт, сургалт хөгжлийн бодлогын хэрэгжилт, үр дүнд хийсэн энэхүү аудит нь төрийн захиргааны байгууллагуудын мэдээллийн технологийн чиг үүргийг хэрэгжүүлж байгаа хүний нөөцийн бүрдүүлэлтийн өнөөгийн нөхцөл байдал, мэдлэг, ур чадварын түвшнийг тогтоох, үйл ажиллагааны удирдлага, зохион байгуулалт, гүйцэтгэлийн явцад гарч байгаа ололт болон сул байдлыг чухалчлан тэмдэглэж үр дүнгийн байдлыг тодорхойлох, цаашид хэрэгжүүлэх сургалт, хөгжлийн хэрэгцээ шаардлагыг тодорхойлох, илэрсэн сөрөг үр дагаврыг арилгаж, эрсдэлийг бууруулахад чиглэв.

II. ХҮНИЙ НӨӨЦИЙН ТӨЛӨВ БАЙДАЛ

Төрийн албаны нэгдсэн тоо бүртгэл /2023онд/-д бүртгэлтэй 4239 байгууллагын 2692 нь төрийн үйлчилгээний, 117 нь төрийн тусгай, 1430 нь төрийн захиргааны байгууллага байна.

Судалгаанд төрийн үйлчилгээний 2692 байгууллага болон мэдээллийн технологийн орон тоогүй төрийн захиргааны байгууллагууд, бүтэц, орон тоо, чиг үүрэг нь төрийн болон албаны нууцад хамаарах

төрийн тусгай чиг үүргийн байгууллагуудыг хамруулаагүй болно.

Төрийн захиргааны 1430 байгууллагын 443 байгууллага нь мэдээллийн технологийн чиг үүргийг хэрэгжүүлэх батлагдсан 728 орон тоотой бөгөөд тус орон тоонд 578 албан хаагч ажиллаж байна. (Нийт 728 орон тооны 150 нь сул орон тоо байна.)

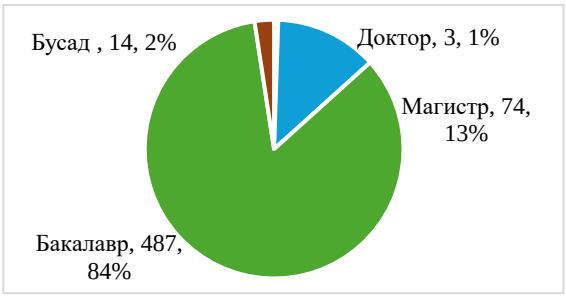
Судалгаанд төрийн захиргааны 443 байгууллагын 578 албан хаагчийг хамруулсан болно.

Үүнээс гадна төрийн байгууллагууд мэдээллийн технологийн зарим чиг үүргийг төрийн өмчийн оролцоотой байгууллагуудаар хэрэгжүүлж байна. Тухайлбал: Цахим хөгжил, инновац, харилцаа холбооны яамны харьяа И Монгол академи, Үндэсний дата төв УТҮГ-аар, Сонгуулийн ерөнхий хороо, Сангийн яам, Боловсролын ерөнхий газар Мэдээллийн технологийн төвөөр гүйцэтгүүлж байгаа бөгөөд уг мэргэжлийн 5 байгууллагад мэдээллийн технологийн чиг үүрэг хэрэгжүүлдэг 307 албан хаагч ажиллаж байна. Судалгаанд хамрагдсан төрийн албан хаагчдын 211 буюу 36.5% нь төрийн захиргааны, 67 буюу 11,6% нь төрийн тусгай, 280 буюу 48,4% нь төрийн үйлчилгээний, 20 буюу 3,4% нь гэрээт ажилтнууд байна.

Мэдээллийн технологийн чиг үүрэг хэрэгжүүлж байгаа төрийн үйлчилгээний 280 албан тушаалтны 33 нь өндөр ур чадвартай албан хаагчид байна.

Мэдээллийн технологийн чиг үүргийг хэрэгжүүлж байгаа 578 албан хаагчийн 25 нь удирдах, 553 нь гүйцэтгэх албан тушаалтан, 264 нь эмэгтэй, 313 нь эрэгтэй албан хаагч байна.

Судалгаанд хамрагдсан төрийн албан хаагчдын **84% нь бакалаврын боловсролтой**, 13% нь магистрын, 1% нь докторын зэрэгтэй, 2% нь техникийн болон бүрэн дунд боловсролтой байна.



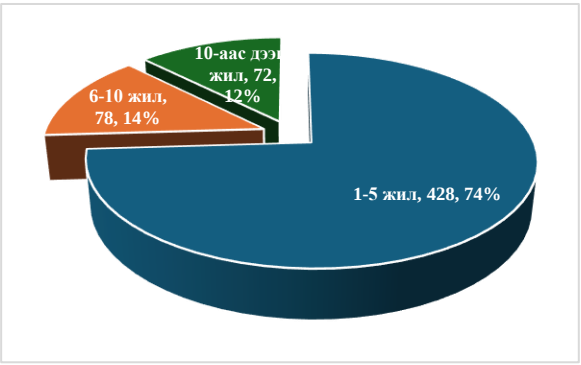
1-р зураг. МТ-ын албан хаагчдын боловсролын байдал /2023-2024 он/

Мэдээллийн технологийн чиг үүрэг хэрэгжүүлж байгаа 578 албан хаагчийн 436 буюу 75 хувь нь мэргэжлийн, 142 буюу 25 хувь нь автозам, барилгын инженер, нягтлан бодогч, эрх зүйч, сэтгүүлч зэрэг бусад мэргэжлийн мэргэжлийн бус албан хаагчид байна.

2-р зураг. МТ-ын албан хаагчдын мэргэжлийн байдал /2023-2024 он/

Мэргэжлийн бус 142 албан хаагчийн албан тушаалын 97 нь мэдээллийн технологийн чиг үүргийг дангаар хэрэгжүүлэх албан тушаал бол 45 нь бусад чиг үүрэгтэй хавсран хэрэгжүүлэх албан тушаал байна.

Төрийн албаны мэдээллийн технологийн хүний нөөцийн 428 буюу 74 хувь нь тухайн албан тушаалдаа 5 хүртэл жил ажилласан туршлагатай байна.



3-р зураг. МТ-ын албан хаагчдын туршлагын байдал /2023-2024 он/

III. СУРГАЛТ, НИЙГМИЙН БАТАЛГААГ ХАНГАХ БОДЛОГО, ХЭРЭГЖИЛТ

“Алсын хараа-2050” урт хугацааны хөгжлийн бодлогын баримт бичигт “Цахим Монгол” зорилтыг дэвшүүлж, үүнтэй уялдуулан дунд, богино хугацааны бодлогын баримт бичигт цахим шилжилтийн үеийн 86 зорилт, арга хэмжээ тусгагдсан байна.

Эдгээр зорилт арга хэмжээний 89.6 хувь нь мэдээллийн технологийн дэд бүтцийг бий болгох, техник технологийг хөгжүүлэх, мэдээллийн нэгдсэн сан бий болгох, орон зайн болон газар зүйн мэдээллийн системийг шийдвэр гаргалтад ашиглах, төрийн байгууллагуудын мэдээлэл солилцох үйл ажиллагааг дэмжих, төрийн үйлчилгээг хялбаршуулах, цахимжуулахад чиглэсэн **мэдээллийн технологийн техник хангамж болон программ хангамжийг хөгжүүлэх** талын үйл ажиллагааг төлөвлөсөн бол 10.4 хувь нь төрийн албан хаагчдыг сургах, мэдээлэл технологийн ур чадварыг хөгжүүлэхэд чиглэсэн үйл ажиллагаа байна.

Монгол Улсын урт, дунд хугацааны бодлогын баримт бичигт төрийн албаны мэдээллийн технологийн чиглэлийн хүний нөөцийг бэлтгэх, сургах, хөгжүүлэх, тогтвортой ажил эрхлэлтийг дэмжсэн урт хугацааны, нэгдсэн бодлого зорилт, арга хэмжээг тусгаагүй боловч төрийн албаны мэдээллийн технологийн чиг үүргийг хэрэгжүүлж буй албан хаагчдын ажиллах нөхцөл, нийгмийн баталгааг хангах, хүний нөөцийг бүрдүүлэх зорилгоор Засгийн газрын 2023 оны 05 дугаар сарын 31-ний өдрийн 213 дугаар тогтоолыг баталсан байна. Уг тогтоолоор төрийн албанд ажиллах мэдээлэл технологийн чиглэлээр нарийн мэргэшсэн, өндөр ур чадвар бүхий ажилтны албан тушаалын цалингийн хэмжээ, түүнийг ажиллуулах төрийн байгууллагын жагсаалт, ажилтны орон тооны дээд хязгаарыг баталсан ч мэдээллийн технологийн чиглэлээр нарийн мэргэшсэн, өндөр ур чадвар бүхий ажилтны эзэмшсэн байх мэдлэг, ур чадвар, нөхцөл, шалгуур, төрийн байгууллагуудын тухайн үеийн орон тооны хүрээнд зохицуулалт хийх эсэхийг тодорхой заагаагүй, “мэдээллийн технологийн чиглэлээр нарийн мэргэшсэн, өндөр ур чадвар”-тай хүнийг сонгон шалгаруулах үйл явц, шаардагдах санхүүжилтийг шийдвэрлэх зэрэг арга замыг тодорхой тусгаагүйгээс төрийн албанд ажиллах мэдээллийн технологийн чиглэлийн хүний нөөцийг оновчтой бүрдүүлэх, тогтоон барих, тогтвор суурьшилтай ажиллуулахад тодорхой ахиц гараагүй байна.

Тогтоолд 75 байгууллагын нарийн мэргэшсэн, өндөр ур чадвар шаардах 181 албан тушаалын жагсаалтыг баталсан. Энэ жагсаалтад дурдсанаар аудитад хамрагдсан нийт байгууллагын 67 байгууллага нь 160 албан тушаалд нарийн мэргэшсэн, өндөр ур чадвартай албан хаагчийг ажиллуулах боломжтой бөгөөд 2024 оны 09 дүгээр сарын 26-ны байдлаар судалгаанд хамрагдсан 8 яам, 13 агентлаг, Дундговь аймгийн ЗДТГ зэрэг нийт 22 байгууллага, 33 албан тушаалд нарийн мэргэшсэн, өндөр ур чадвартай албан хаагчийг ажиллуулж байна.

Төрийн албаны зөвлөл, Засгийн газар төрийн албан хаагчийн богино, дунд хугацааны болон мэргэшүүлэх багц сургалтын агуулга хөтөлбөрийг баталж, хэрэгжүүлдэг.

Сургалтын агуулгын 9.3%-д мэдээлэл, харилцаа холбооны технологи ашиглах арга зүй, хэрэглээ, төлөвлөлт, удирдлагын талаар тусгагдсан байх боловч тухайн сургалтад хамрагдах шаардлагатай албан хаагчдыг бүрэн хамруулах, сургалтаар өгсөн мэдлэгийг төрийн албан хаагчид албан үүргээ хэрэгжүүлэхдээ бүрэн ашиглах чадвар суусан эсэхийг тодорхойлох тогтолцоо бүрдээгүй байна.

4-р зураг. МТ-ын албан хаагчдын мэргэшүүлэх сургалтад хамрагдсан байдал /2023-2024 он/

Төрийн албаны тухай хуульд заасан төрийн албан хаагчийн нийгмийн баталгааг хангах хүрээнд төрийн байгууллагууд мэдээллийн технологийн чиг үүрэг хэрэгжүүлдэг 1 албан хаагчид дотоодын их, дээд сургуулийн докторын хөтөлбөрийн, 11 алан хаагчид магистрын хөтөлбөрийн сургалтын төлбөрийн дэмжлэг үзүүлсэн бол гадаадын их дээд сургуулийн докторын хөтөлбөрт 1, магистрын хөтөлбөрт 6 албан хаагч Засгийн газрын тэтгэлгээр суралцаж төгссөн байна.

Төрийн албаны мэдээллийн технологийн хүний нөөцийн 41 буюу 7 хувь нь мэргэжлээр нь чадавхжуулах дотоодын богино хугацааны зорилтот сургалтад, 31 буюу 3.4 хувь нь Олон улсын мэргэжлийн богино хугацааны сургалтад хамрагдсан байна.

Хамрагдсан сургалтуудын дийлэнх нь богино хугацааны, ихэнхдээ **ерөнхий чиглэлийн сургалтууд** (оффис хэрэглээ, мэдээллийн аюулгүй байдал гэх мэт) байна.

Төрийн байгууллагууд Төрийн албаны тухай хуульд заасан төрийн албан хаагчийн нийгмийн баталгааг хангахад 2019-2024 онд нийт 1,4 тэр бум төгрөг зарцуулсан байна. Тухайлбал: 161 албан хаагчид 281,7 сая төгрөгийн нөхөн төлбөр олгож, 21 албан хаагчид орон байр худалдан авахад 329,9 сая төгрөгийн дэмжлэг үзүүлж, өндөр насны тэтгэвэрт гарч байгаа 6 албан хаагчид 163,1 сая төгрөгийн буцалтгүй тусламж, бусад.

IV. МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ЧИГ ҮҮРЭГ ХЭРЭГЖҮҮЛДЭГ АЛБАН ХААГЧДЫН МЭДЛЭГ, УР ЧАДВАРЫН ҮНЭЛГЭЭ

Төрийн албаны мэдээллийн технологийн чиг үүрэг хэрэгжүүлдэг албан хаагчдын мэдлэг, ур чадварын түвшин, цаашдын сургалтын хэрэгцээ шаардлагыг тодорхойлох зорилгоор олон улсад хүлээн зөвшөөрөгдсөн мэдээллийн технологийн инженерийн шалгалтын агуулга, хамрах хүрээ, Монголд нэвтэрсэн байдлыг судалж, Япон улсад төвтэй Мэдээллийн технологийн мэргэжилтнүүдийн шалгалтын зөвлөл (ITPEC)-ийн мэдээллийн технологийн инженерийн паспорт болон суурь шалгалтыг сонгож Мэдээллийн технологийн үндэсний парктай гэрээ байгуулж хамтран ажиллалаа.

Шалгалтын агуулгын 62 хувийг технологи, 22 хувийг стратеги, 16 хувийг менежментийн мэдлэг, ур чадварыг үнэлэх асуулт эзэлдэг байна.

Сорилыг дээрх 3 бүлгийн хүрээнд 9 агуулгаар 50 асуулттай 1 цагийн сорилыг боловсруулан 2024 оны 10 дугаар сарын 04-ны өдөр улсын хэмжээнд нэгдсэн байдлаар Төрийн албаны зөвлөлийн тусгай шалгалтын Open exam цахим системээр зохион байгууллаа.

Сорилд 13 яамны 82, 11 агентлагийн 198, нутгийн захиргааны 245 байгууллагын 290, нийт 570 төрийн албан хаагч хамрагдлаа.

Сорилд хамрагдсан төрийн албаны мэдээллийн технологийн чиг үүрэг хэрэгжүүлдэг албан хаагчдын мэдээллийн технологийн стратегийн мэдлэг бусад улсын дундаж түвшинтэй ойролцоо байгаа бол менежментийн болон технологийн мэдлэг харьцангуй доогуур байна.

Төрийн албаны мэдээллийн технологийн чиг үүргийг хэрэгжүүлж буй албан хаагчдын мэдээллийн технологийн мэдлэг 37.8 хувьтай байна.

1-Р ХҮСНЭГТ. ШАЛГАЛТЫН ТӨВҮҮДЭЭР ДАМЖУУЛАН МТ-ИЙН МЭДЛЭГ, УР ЧАДВАРЫН ШАЛГАЛТ ӨГСӨН 12 ОРНЫ БОЛОН МОНГОЛ УЛСЫН ИРГЭДИЙН ТҮВШИН, ХАРЬЦУУЛСНААР

Шалгалтын төв бүхий улсын нэр	Технологи /62%/	Менежмент /16%/	Стратеги /22%/	Нийт /100%/
Филиппин дэх	**38.6**	**9.3**	**12.5**	60.4
Мьянмар дахь	**41.6**	**9.6**	**11.5**	62.7
Тайланд дахь	**36.8**	**10.3**	**14.0**	61.1
Вьетнам дахь	**40.3**	**12.7**	**14.6**	67.6
Бангладеш дахь	**41.7**	**10.0**	**14.8**	66.5
Шалгалт өгсөн 12 улсын иргэдийн дундаж	**39.8**	**10.4**	**13.48**	**63.67**
Монгол улс дахь шалгалтын төв	**38.7**	**8.9**	**11.3**	58.9
ТАЗ туршилтын сорилын үр дүн	**19.2**	**6.0**	**12.6**	**37.8**

Шалгалтын нийт үр дүнгээс харахад яам, агентлагийн мэдээллийн технологийн албан хаагчдын тооллын системийн суурь, олонлог, магадлал, статистик, мэдээллийн тоон хувиргалт болон алгоритмын тухай зэрэг суурь онолын мэдлэг дунджаар 7-11 хувийн үнэлгээтэй байгаа нь инженерийн суурь мэдлэгийг их, дээд сургуульд сурснаас хойш дахин сэргээж, мэдлэгээ бататгаагүй, нөгөө талаар ажлын байранд тэр болгон хэрэглээд байдаггүйтэй холбоотой гэж үзэж байна.

2-Р ХҮСНЭГТ. СОРИЛД ХАМРАГДСАН МТ-ИЙН АЛБАН ХААГЧДЫН МЭДЛЭГИЙН ТҮВШИН, ШАЛГАЛТЫН АГУУЛГААР

Яамдын нэр	Технологи				Менежмент		Стратеги		
	Суурь онол	Компьютерын систем	Технологийн элемент	Систем хөгжүүлэх технологи	Төслийн удирдлага	Үйлчилгээний удирдлага	Байгууллага ба эрх зүй	Бизнесийн стратеги	Системийн стратеги
Яам	11 %	30 %	57 %	40 %	48 %	50 %	63 %	57 %	100 %
Агентлаг	7%	24 %	50 %	32 %	35 %	47 %	66 %	49 %	100 %
Нутгийн захиргааны байгууллага	30 %	25 %	33 %	30 %	22 %	26 %	27 %	37 %	29 %
Дундаж үнэлгээ	**16 %**	**26 %**	**47 %**	**34 %**	**35 %**	**41 %**	**52 %**	**47 %**	**76 %**

Мөн яам, агентлагийн мэдээллийн технологийн албан хаагчдын технологийн элемент, менежмент, стратегийн талаарх мэдлэг 49-63 хувьтай буюу хамгийн өндөр байгаа нь салбарын бодлого тодорхойлох, дүрэм журам боловсруулах, байгууллагын систем, сүлжээ, тоног төхөөрөмжийн

бэлэн байдлыг хангаж ажилладаг чиг үүрэгтэй нь холбоотой байна.

Нутгийн захиргааны байгууллагын мэдээллийн технологийн албан хаагчдын суурь онолын мэдлэг яам, агентлагаас өндөр байгаа нь тухайн байгууллагуудад дөнгөж сургууль төгссөн, төгсөөд удаагүй залуу боловсон хүчнүүд ажилладагтай холбоотой гэж үзэж болохоор байна.

ДҮГНЭЛТ

Судалгааны үр дүнгээс дараах гол дүгнэлтүүд гарлаа:

1. **Хүний нөөцийн төлөв байдал** нь бүрдүүлэлт хангалтгүй, хомсдол үүссэн, мэргэжлийн ур чадвар сул байна. Төрийн байгууллагуудын батлагдсан бүтэц дэх мэдээллийн технологийн чиг үүрэг хэрэгжүүлэх 728 орон тооны 150 орон тоо сул, 142 орон тоонд мэргэжлийн бус албан хаагч ажиллаж байгаа нь нийт орон тооны 40,1 хувийг эзэлж байна. Мэргэшсэн ажилтны эзлэх хувь ердөө 14.5 хувьтай байна.
2. **Сургалт хөгжил, нийгмийн баталгааны бодлого нь бодит хэрэгцээнд суурилаагүй**, зохицуулалт, хэрэгжилтийн механизм дутмаг байна. Төрийн албаны мэдээллийн технологийн салбарын хүний нөөцийн дутагдалтай байдлыг шийдвэрлэх, нийгмийн баталгааг хангах арга хэмжээг авсан боловч, өндөр ур чадвартай албан хаагчид байх мэдлэг, ур чадвар, туршлага, хэрэгжүүлэх чиг үүргийг тодорхойлоогүй, батлагдсан орон тоонд хэрхэн зохицуулалтыг хийх, шаардагдах санхүүжилтийг хэрхэн шийдвэрлэх арга замыг тодорхой тусгаагүйн улмаас хэрэгжилтийн түвшинд тодорхойгүй нөхцөл байдлыг үүсэж, нэг удаагийн шинжтэй, нэгдсэн, цогц байдлаар төлөвлөж, шийдвэрлээгүй учир салбарын хүний нөөцийн эрэлт, хэрэгцээг хангахуйц үр дүн үзүүлээгүй байна.
3. **Олон улсын шалгуурт нийцэх чадвар дутмаг.** Мэдээллийн технологийн инженерийн олон улсын шалгалтад оролцсон төрийн албан хаагчдын мэдлэгийн түвшин доогуур байгаа нь хүний нөөцийн чадвар, сургалт, хөгжлийн бодлого хангалтгүй байгааг харуулж байна.

ЗӨВЛӨМЖ

1. Төрийн байгууллагын мэдээллийн технологийн чиг үүргийг хэрэгжүүлэгч хүний нөөцийг бэлтгэх, сургах, хөгжүүлэх, мэргэшүүлэх, тогтвортой байдлыг хангах үр дүнд суурилсан хөгжлийн **стратегийг боловсруулах.**
2. Урт **хугацааны мэргэшүүлэх сургалт**, олон улсын гэрчилгээтэй хөтөлбөрт хамруулах бодлого боловсруулах, **төр-их, дээд сургууль-хувийн хэвшлийн хамтын ажиллагаа** бий болгох.
3. **Сургалтын дараах үнэлгээ, үр нөлөөний хяналт-шинжилгээний тогтолцоо** бүрдүүлэх.
4. Цахим шилжилтийн бодлого хэрэгжүүлэгч МТ-ийн ажилтнуудын нийгмийн баталгааг хангах зорилгоор мэдээллийн технологийн албан тушаалын шинэ ангилал, зэрэглэл бий болгох, урамшууллын системийг боловсронгуй болгох.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Төрийн албаны тухай хууль. Улаанбаатар хот, 2017он.

[2] Хөдөлмөрийн тухай хууль. Улаанбаатар хот, 2022 он.

[3] Киберь аюулгүй байдлын тухай хууль. Улаанбаатар хот. 2021 он.)

[4] Төрийн албаны зөвлөлийн 2021 оны 80 дугаар тогтоолоор батлсан “Төрийн байгууллагын үйл ажиллагаанд хүний нөөцийн аудит хийх журам. 2021 он.

АУТИЗМ СПЕКТРИЙН ЭМГЭГИЙН АНГИЛАЛД ӨГӨГДЛИЙН ШИНЖИЛГЭЭ ХИЙСЭН СУДАЛГАА

Эрдэнэбатын БУЯНТӨГС[1], Амарсайханы ТҮВШИНБАЯР[2]
Монгол Улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: e.buyantugs@gmail.com[1], tuvshinbayar@must.edu.mn[2]

***Хураангуй*: Аутизмын хүрээний эмгэг(autism spectrum disorder, ASD)[1] нь хүн амын аль ч бүлэгт илэрдэг төв мэдрэлийн тогтолцооны хөгжлийн эмгэг бөгөөд нийгмийн харилцаа, бусадтай харилцах чадварын дутагдал болон давтагдмал, хэвшмэл зан үйлээр илэрдэг[1]. Дэлхийн хэмжээнд 100 хүүхдийн 1 орчим нь ASD-р оношлогддог бөгөөд бага насны хөгжлийн явцад сөрөг нөлөө үзүүлдэг нь тогтоогдсон[2]. Иймд уг эмгэгийг эрт шатанд илрүүлж, оношлох нь урт хугацааны хөгжлийн хоцрогдлын эрсдэлийн бууруулж, хүүхдийн эрүүл мэнд, гэр бүлийн ачаалалд эергээр нөлөөлнө[3]. Энэхүү судалгаанд өгөгдөлд суурилсан машин сургалтын(ML) аргачлалуудыг ашиглан ASD-ийн эрт илрүүлэлт, тохиолдлын таамаглалыг (forecasting) боловсронгуй болгохыг зорьсон. Forecasting загваруудыг ARIMA, SARIMA, Prophet, sNaive, ETS зэрэг time series загваруудыг ашиглан 5 жилийн дата хоорондын давтамжийн улирал болон трендийг урьдчилан таамагласан. Мөн өгөгдлийг ангилах зорилгоор Random Forest Classifier, Gradient Boosting Classifier, Decision Tree Classifier, Logistic Regression зэрэг supervised машин сургалтын загваруудыг харьцуулан туршсан.**

Түлхүүр үг:* Өгөгдлийн шинжилгээ, time serious, *таамаглах, өгөгдөл дүрслэх

I. УДИРТГАЛ (10PT, BOLD)

Энэхүү судалгааны ажлын зорилго нь аутизмын хүрээний эмгэгийн тархалтын динамик өөрчлөлт, түүний өсөлтөд нөлөөлөх хүчин зүйлсийг тодорхойлох, мөн өгөгдөлд суурилсан шинжилгээ хийж, стратеги бодлого төлөвлөлтийг дэмжихэд оршино. Үүний хүрээнд цаг хугацааны өгөгдлийг цуглуулж, боловсруулан, статистик болон машин сургалтын аргачлалуудыг ашиглан нарийвчилсан дүн шинжилгээ хийх бөгөөд дараах зорилтуудыг хэрэгжүүлнэ. Үүнд:

1. Аутизмын өгөгдөлд үндэслэж анализ үр дүн гаргах,

2. Аутизмын өсөлтөд нөлөөлөх хүчин зүйлсийг тодорхойлох,

3. Ирээдүйн аутизмын тоон таамаглал гаргах, оновчлолд хийх бөгөөд ашиглах өгөгдлийн боловсруулалт хийх санг тодорхойлсон, загваруудын үнэлгээг харьцуулсан үнэлэх юм. Судалгааны үр дүн эрүүл мэндийн бодлогын боловсруулалт, нийгмийн дэмжлэгийн механизм, олон нийтэд чиглэсэн мэдээлэл сурталчилгааны стратегийг сайжруулахад онолын болон практикийн үнэтэй хувь нэмэр оруулна.

A. Аутизм өгөгдөл

Энэхүү судалгаанд ашигласан өгөгдлийн сан нь бага насны хүүхдүүдийн аутизмын эрсдэлийг урьдчилан илрүүлэх зорилгоор боловсруулагдсан олон нийтэд нээлттэй Toddler Autism Dataset (July 2018) өгөгдлийн сан [4] бөгөөд уг өгөгдлийг F.Thabtah өөрийн судалгааны ажилд [5] зориулан боловсруулсан болно. 1-р хүснэгтэд 1054 оролцогчоос бүрдэх, 19 хүчин зүйл бүхий аутизмын оношилгоонд хамаарах зан үйлийн асуумжийн хариултуудыг харууллаа.

TODDLER ASD DATASET ӨГӨГДЛИЙН САНГИЙН ХҮЧИН ЗҮЙЛС

1-Р ХҮСНЭГТ.

Obj ref	Obj нэр	Тайлбар
1	Case_No	Судалгаанд оролцогчийн дугаар
2-11	A1–A10	Асуумжийн 10 зан үйлийн шалгуурт өгсөн хариулт (1: тийм, 0: үгүй)
12	Age_Mons	Хүүхдийн нас (сараар)
13	Qchat-10-Score	Q-Chat асуумжийн нийлбэр оноо
14	Sex	Хүүхдийн хүйс (m – эрэгтэй, f – эмэгтэй)
15	Ethnicity	Хүүхдийн үндэс угсаа
16	Jaundice	Шар өвчтэй байсан эсэх (yes/no)
17	Family_mem_with_ASD	Гэр бүлийн гишүүдийн дунд аутизмтай хүн байгаа эсэх
18	Who_completed_the_test	Асуумжийг бөглөсөн хүний мэдээлэл
19	Class/ASD Traits	Аутизмын эрсдэлийн ангилал (Yes–эрсдэлтэй, No – эрсдэлгүй)

Он цагийн таамаглал гаргах зорилгоор 20. ASD evaluated date object үүсгэн өгөгдлийг нэмсэн.

B. Аутизмын өгөгдлийг анализ хийхийн ач холбогдол

Сүүлийн жилүүдэд ASD-ийн оношилгоо болон эрт илрүүлэлтийн үр нөлөөг сайжруулахад өгөгдөлд суурилсан дүн шинжилгээ, ML-ын арга зүй чухал үүрэгтэй болон нь олон судалгаагаар нотлогдож байна.

- ***Нэгдүгээрт,*** ASD-ийн тархалт, өсөлтийн динамикийг өгөгдөлд суурилан судалж, тухайн эмгэгийн он цаг, газарзүйн болон нийгэм-демографийн хэв шинжийг тодорхойлох боломж бүрддэг [7]. Энэ нь эрт илрүүлэлтийн стратеги боловсруулалт, нийгмийн дэмжлэгийн

хүртээмжийг сайжруулахад чухал ач холбогдолтой юм.

- ***Хоёрдугаарт,*** өгөгдлийн шинжилгээ нь ASD-ийн эрсдэлийн хүчин зүйлсийг тодорхойлох, тухайн хүчин зүйлсийн хоорондын уялдаа холбоог илрүүлэхэд үр нөлөөтэй. Статистик болон ML-ын арга зүйг ашиглан гэр бүлийн өвчний түүх, шар өвчин, нас, хүйс зэрэг object-ын нөлөөллийг нарийвчлан судлах боломжтой [8].
- ***Гуравдугаарт,*** ASD-ийн өгөгдлийн дүн шинжилгээ нь эрт оношилгооны үнэн зөвийг нэмэгдүүлэх, оношилгооны загваруудыг хөгжүүлэхэд чухал суурь болдог. Ялангуяа өгөгдөлд суурилсан загварчлал нь уламжлалт асуумж болон эмнэл зүйн үнэлгээний үр дүнг баяжуулж, оношилгооны системийг тайлбарлах чадварыг нэмэгдүүлдэг [9].

Мөн өгөгдлийг үр дүнтэй ашигласнаар эрүүл мэндийн бодлого боловсруулалт, олон нийтэд чиглэсэн мэдээлэл сурталчилгааны стратеги, нийгмийн халамжийн үйлчилгээг хүртээмжтэй, оновчтой болгон үндэс суурийг бүрдүүлнэ [10].

Түүнчлэн ASD-ийн талаарх өгөгдөл, түүний үндэслэлтэй дүн шинжилгээ нь аутизмтай хүүхэд болон тэдний гэр бүл нийгэмд гадуурхагдах, ялгаварлан гадуурхалт, боловсролын болон эрүүл мэндийн үйлчилгээний тэгш бус байдлын асуудлыг шийдвэрлэхэд чухал үүрэгтэй юм. ASD-ийн оношилгоо, үйлчилгээний хүртээмжийн ялгаатай байдал нь хүний эрхийн зөрчил, хүүхдийн эрүүл мэнд, хөгжлийн боломжийг хязгаарлах хүчин зүйл болдог[11],[12]. Иймээс өгөгдөлд суурилсан бодит баримтад тулгуурласан дүн шинжилгээ нь аутизмтай хүүхдийн эрүүл, аюулгүй амьдрах эрх, боловсролын үйлчилгээ авах боломж, нийгмийн оролцоог дэмжихэд чухал ач холбогдолтой гэж үзнэ [13].

II. ОНОЛЫН ХЭСЭГ

A. ASD тодорхойлох үндсэн ойлголт

ASD-ийн эрт илрүүлэлт, оношилгоонд скрининг буюу анхан шатны үнэлгээний аргачлал чухал үүрэг гүйцэтгэдэг. Скрининг нь ASD-ийн шинж тэмдгийг хөгжлийн эрт үед илрүүлж, оношилгоо болон оролцооны дараагийн алхмуудыг тодорхойлоход тусалдаг чухал үе юм [14]. Энэ нь оношт тавих ажиллагааг орлохгүй хэдий ч оношилгооны үр ашгийг нэмэгдүүлж, хүүхдийн хөгжлийн хоцрогдлыг бууруулахад чиглэдэг.

Скринигт хамгийн өргөн хэрэглэгддэг хэрэгслүүдийн нэг бол Modified Checklist for Autism in Toddler, Revised(M-CHAT-R) бөгөөд энэ нь 16-30 сартай хүүхдүүдэд зориулагдсан, 20 асуултаас бүрдсэн анхан шатны үнэлгээний асуумж юм. Асуумж нь хүүхдийн нийгмийн харилцаа, анхаарал төвлөрөл, зан үйлийн хэв маягт төвлөрч, эцэг эхийн мэдээлэлд үндэслэн эрсдэлийн оноо тооцдог. Үр дүнгээс хамааран хүүхдийг “эрсдэлгүй”, “дунд эрсдэлтэй”, эсвэл[18 “өндөр эрсдэлтэй” гэж ангилж, цаашид нарийвчилсан үнэлгээ хийх шаардлагатай эсэхийг тодорхойлдог[14],[16].

M-CHAT-R асуумжийн нийт оноо (S) нь дараах байдлаар тодорхойлогдоно:

$$S = \sum_{i=1}^{20} x_i \quad (1)$$

$x_i = 1$ хэрэв тухайн асуултын хариулт аутизмын эрсдэлийн шинж тэмдгийг илэрхийлж байвал.
$x_i = 0$ хэрэв тухайн асуултын хариулт аутизмын эрсдэлийн шинж тэмдгийг илрээгүй бол.

Онооны интервалын үндсэн дээр эрсдэлийн түвшнийг дараах байдлаар тодорхойлно.

$$\text{Эрсдэлийн түвшин} = \begin{cases} \text{"Бага эрсдэл", Хэрэв } S \leq 2 \\ \text{"Дунд эрсдэл", Хэрэв } S \leq 2 \\ \text{"бага эрсдэл", Хэрэв } S \leq 2 \end{cases} \quad (2)$$

Энэ судалгааны хүрээнд “Toddler ASD Dataset” өгөгдлийн санд суурилсан, Q-Chat-10 загварт тулгуурласан скринингийн аргачлалыг ашиглана. Энэхүү өгөгдлийн сан нь 1054 point-ийн Q-Chat-10(A1-10)-д өгсөн хариултын binary(0,1) кодчилж, нийт онооны үндсэн дээр “ASD traits” ангиллыг автоматаар тогтоосон байдаг
Q-Chat-10 асуумжийн нийт оноо (Q) дараах байдлаар тооцогдоно:

$$Q = \sum_{j=1}^{10} y_j \quad (3)$$

y_j = хэрэв тухайн асуултын хариулт “Sometimes”, “Rarely”, “Never” (A1–A9) эсвэл “Always”, “Usually”, “Sometimes” (A10) бол;
$x_i = 0$ эсвэл бусад хариулт өгсөн бол.

Онооны ангилалыг дараах байдлаар тодорхойлогдоно.

$$\text{ASD Traits} = \begin{cases} \text{"No"}, \text{Хэрэв } Q < 4 \\ \text{"Yes"}, \text{Хэрэв } Q \geq 4 \end{cases} \quad (4)$$

1) ASD өгөгдлийн төрлүүд

ASD өгөгдлийг ангилснаар шинжилгээ хийх арга зүйг оновчтой болгох, төрөл бүрийн үзүүлэлтийг уялдуулан судлах боломж бүрддэг. 2-р хүснэгтэд үндсэн төрлүүдийг харууллаа.

ASD ӨГӨГДЛИЙГ АНГИЛСАН ТӨРӨЛ

2-Р ХҮСНЭГТ.

Багана нэр	Өгөгдлийн төрөл	Тайлбар
Case_No	Nominal	Зөвхөн таних дугаар; хэмжих утгагүй
A1 – A10	Ordinal	Бинар (0,1) утгатай боловч “хандлага байгаа эсэх” гэх мэт шатлал илэрхийлнэ
Age_Mons	Ratio	Нас нь тэг утгатай эхлэлтэй, харьцаа тооцох боломжтой
Qchat-10-Score	Interval / Ordinal	Онооны интервал байна, гэхдээ шалгуур тул ordinal гэж үзэх тохиолдол бий
Sex	Nominal	Ангилал, утгад дэс дараалал байхгүй
Ethnicity	Nominal	Үндэс угсаа нь ялгаатай боловч шатлалгүй
Jaundice	Nominal	“Yes” / “No” — ангиллын утга
Family_mem_with_ASD	Nominal	Мөн адил — “Yes” / “No”
Who completed the test	Nominal	Бөглөсөн этгээдийн ангилал, дэс дараалалгүй
Class/ASD Traits	Ordinal	“Yes” / “No” боловч онооны босгоос үүдэлтэйгээр эмгэгийн түвшний утгатай гэж үзэж болно

B. Өгөгдлийн дүн шинжилгээний аргачлалууд

ASD-ийн өгөгдөлд суурилсан шинжилгээ нь судалгааны зорилгоос хамааран дараах үндсэн чиглэлүүдэд хуваагдана: тайлбарлах, оношлох, таамаглах, зөвлөмж гаргах.

a) Тайлбарлах анализ (Descriptive Analytics):

Өнгөрсөн хугацаанд гарсан ASD өгөгдөлд суурилсан хандлагыг тодорхойлж, "юу болсон бэ?" гэсэн асуултад хариу өгдөг. Жишээ: ASD улирлын хэлбэлзэл, дундаж орлогын түвшин.

b) Оношлох анализ (Diagnostic Analytics): ASDалт яагаад өссөн эсвэл буурсан шалтгааныг тодорхойлж, хүчин зүйлсийн уялдаа холбоог тайлбарлахад ашиглагддаг. Жишээлбэл, маркетингийн кампанит ажлын үр нөлөөг харьцуулах.

c) Тайлбарлах анализ (Descriptive Analytics): Статистик загвар болон машин сургалтын аргуудыг ашиглан ирээдүйн ASD урьдчилан таамагладаг. Жишээлбэл, он цаг үргэлжилсэн хугацааны цуваа (TS) загвар, Random Forest, XGBoost зэрэг алгоритм ашиглан ирэх саруудын ASD төсөөлөх [5], [7].

d) Зөвлөмж өгөх анализ (Prescriptive Analytics): Аль стратегийг хэрэгжүүлбэл илүү үр дүнтэй болох талаар шийдвэр гаргагчдад санал, шийдэл өгөхөд чиглэдэг. Энэ нь ихэвчлэн оновчлолын аргууд, симуляци, шийдвэрийн мод ашигладаг [9].

III. СУДАЛГААНЫ АРГА ЗҮЙ

Энэхүү судалгааны ажлын арга зүй нь ASD-г өндөр нарийвчлалтай урьдчилан таамаглахын тулд өгөгдөлд суурилсан шинжилгээ, машин сургалтын загварчлал, хэрэглэгчдийн сегментчлэлийг хослуулан ашигласан болно. Өгөгдөл цуглуулалт ба бэлтгэл, Хэрэглэгчийн сегментчлэл болон ASD урьдчилан таамаглах загварууд гэсэн дэд хэсгүүдээр арга зүйн товч тайлбарыг хүргэж байна.

A. Өгөгдөл цуглуулалт ба эх үүсвэр

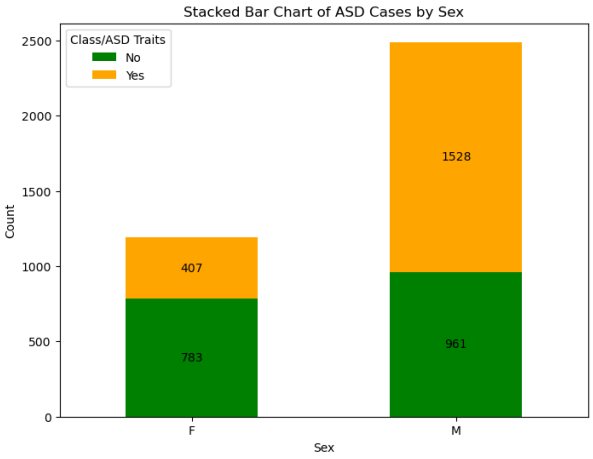
1) Олон нийтэд нээлттэй өгөгдлийн сан ашиглах (Kaggle, UCI Machine Learning Repository, Google Dataset Search).

2) Өгөгдлийн сан боловсруулах – ASD өгөгдлийг цэвэрлэх, нэгтгэх.

B. ASD өгөгдөлд анализ хийх аргачлал

1) Өгөгдлийн дүрслэл

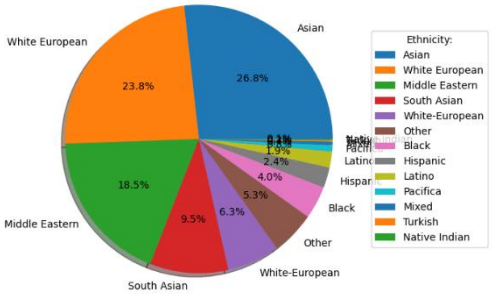
Нэгтгэсэн 3 дата сет өгөгдлийн хүйсээр нь ASD шинж тэмдэг илэрсэн байдлыг баганан графикт дүрслэхэд эрэгтэй 735 тохиолдлоос 534 нь аутизмын шинж илэрсэн. Харин эмэгтэй 309 сорьцоос 184 буюу 60 орчим хувь нь аутизмын шинж илэрсэн үр дүн гарсан.



1-р зураг. Нийт эрэгтэй, эмэгтэй хүйс ASD тоо

ASD тохиолдлуудыг ян үндсийн бүлгээр харьцуулбал:

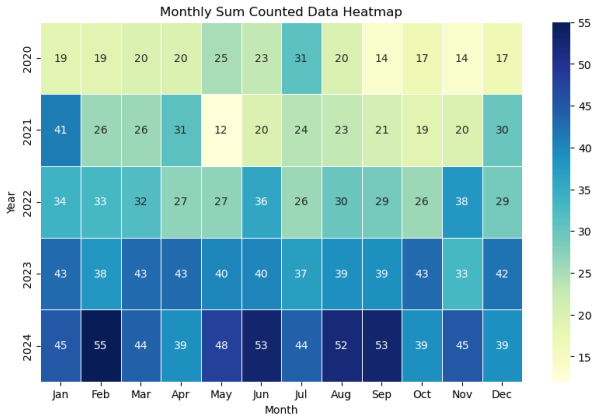
- Asian (Ази): 26.8%,
- *White European: 23.8%*
- *Middle Eastern: 18.9%*
- *South Asian: 9.5%*
- *Black, Hispanic, Latino 2%–6% орчим*
- *Бусад бүлгүүд (Polynesian г.м) нийлээд 6%*



2-р зураг. ASD илэрсэн яс үндэсийн эзлэх хувь

Аутизмын тохиолдлын Ази болон Европ гаралтай хүмүүсийн тоо хэмжээ их байгаа нь тухайн үндэсний гарал үүслээс гадна, нийгмийн оролцоо мэдээлэлтэй байгаагаас хамаарч судалгаанд их хамрагдсан байх боломжтой юм.

Нэгтгэсэн өгөгдлийн бүтцэд хамаарах он цагийн мэдээлэл илэрхийлэх object байхгүй тохиолдолд кейс тус бүрд харгалзах сард random функцыг ашиглаж утга оноож, гаргасан үр дүнг зураг 3-с харна уу



3-р зураг. 2020-2024 онд гэж random функцээр тодорхойлсон тоон үзүүлэлт

2) *Машин сургалтын алгоритмууд ашиглах*

а) ASD таамаглал хийх (ASD Forecasting) ARIMA, SARIMA

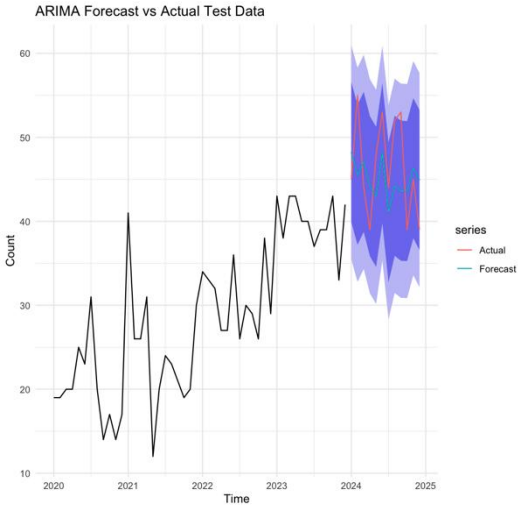
Sample random date өгөгдөлд үндэслэн ARIMA (0,0,0) (1,1,0) [12] with dirft загварыг ашиглан 2024 оны сар бүрийн аутизмын тохиолдын тоог урьдчилан таамаглалт хийв. Сүүлийн 12 сарын өгөгдөлд харьцуулалт хийхэд хооронд MAPE 11 буюу accurancy rate 89% таамаглалын нарийвчлалттай үр дүн гарсан.

$$\text{MAPE} = \frac{100}{n}\sum_{t=1}^{n}\left|\frac{A_t - F_t}{A_t}\right| \quad (5)$$

A_t *"Actual" тухайн үеийн бодит утга*

F_t *"Forecast" – загварын таамаглаан утга*

n *нийт ажилалт буюу хугацааны цэгүүдийн тоо*



4-р зураг. ARIMA загварын таамаглал гаргсан график дүрслэл

3-р хүснэгтэл загварын метрик үзүүлэлт болон үр дүнгийн тайлбарлав.

ЗАГВАРЫН МЕТРИК ҮЗҮҮЛЭЛТ

3-Р ХҮСНЭГТ.

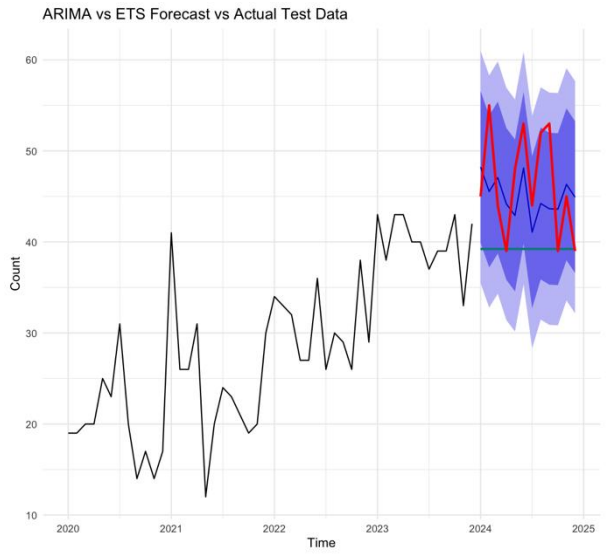
Үзүүлэлт	Training Set	Test Set	Тайлбар
ME	-0.204	1.348	*Mean Error* – дундаж алдаа; сургалтын үед бага (-0.2), тест бага зэрэг хазайсан (1.35).
RMSE	5.48	5.77	*Root Mean Squared Error* – алдааны квадрат дундаж; сургалт ба тестийн зөрүү бага, загвар тогтвортой..
MAE	3.61	5.23	*Mean Absolute Error* – алдааны дундаж; тестийн үед өссөн
MPE	-4.31	1.58	Mean Percentage Error – сургалтын үед загвар бууралттай таамаглаж, тестэд дутуу таамагласан.
MAPE	13.2	11.1	Mean Absolute Percentage Error – харьцангуй алдааны хувь; <15% байгаа нь загвар харьцангуй сайн үздэг[] ба accurancy 88.9% таамаглалттай загвар гарсан.
MASE	0.405	0.587	Mean Absolute Scaled Error – ARIMA загвар 1-с бага байгаа нь энгийн baseline-аас илүү сайн таамагласан.
ACF1	0.126	-0.001	1-р лаг ACF үлдэгдэл – үлдэгдэл корелляци бараг байхгүй, random буюу тохиромжтой загвар.
Theil's U	NA	0.73	Theil U индекс 1-с бага байх нь ARIMA загвар илүү сайн таамаглалт өгч байгааг илтгэнэ.

SARIMA загварын хувь тооцоолол ижил тодорхойлогдсон. (Traning.set=ARIMA, Traning.set.1=SARIMA)

	ME	RMSE	MAE	MPE	MAPE	MASE	ACF1	Theil's
Training.set	−0.204	5.48	3.61	−4.31	13.2	0.405	0.12662	
Test.set	1.348	5.77	5.23	1.58	11.1	0.587	−0.00111	
Training.set.1	−0.204	5.48	3.61	−4.31	13.2	0.405	0.12662	
Test.set.1	1.348	5.77	5.23	1.58	11.1	0.587	−0.00111	

5-р зураг. SARIMA загварын хувь тооцоолол

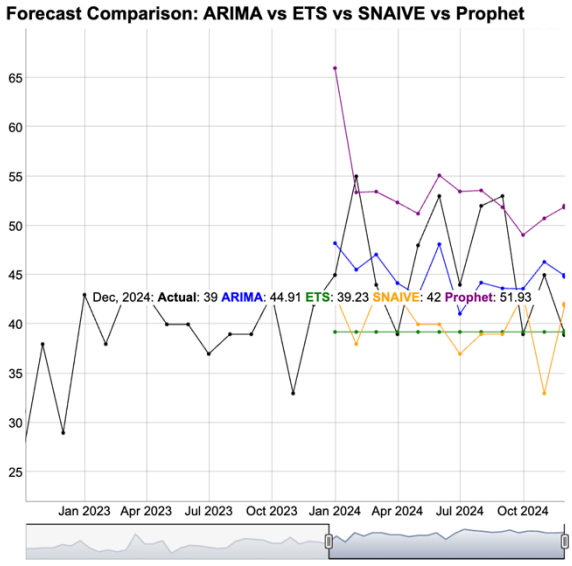
- *ETS*



6-р зураг. ETS загварын таамаглал гаргасан график дүрслэл

- *Prophet (Facebook's forecasting tool*

Prophet санг ашиглаж, ASD таамаглал гаргасан байдал periods = 31, dyplot.prophet



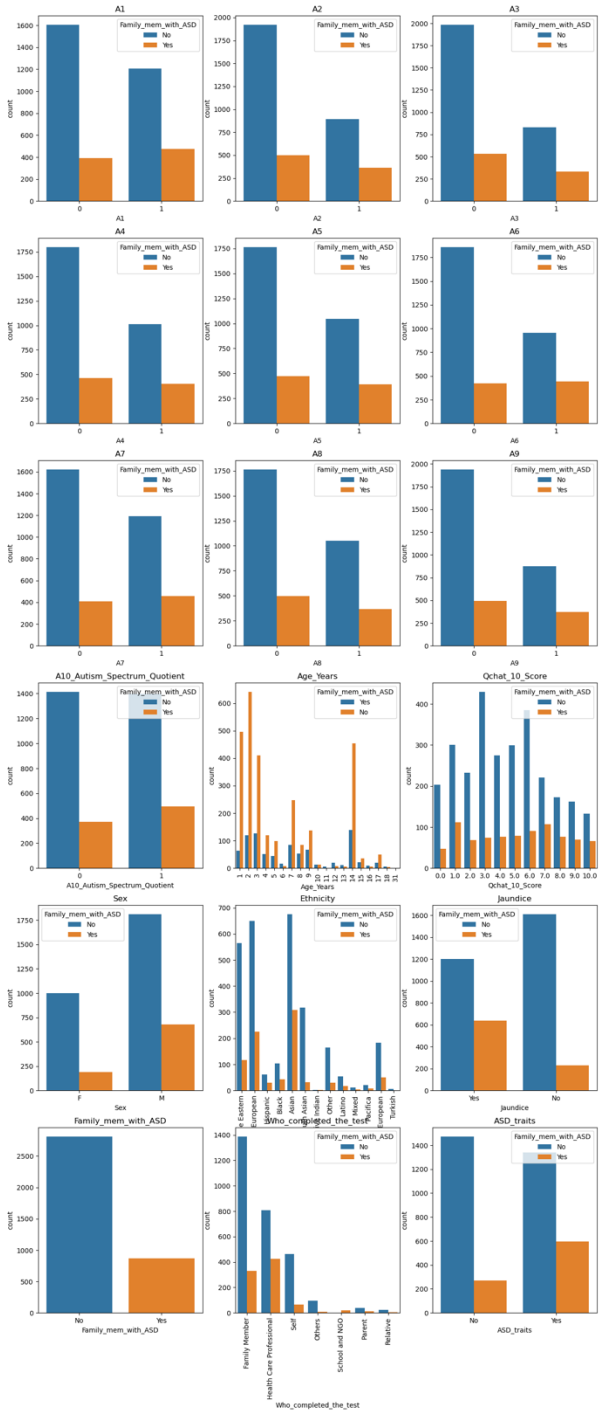
7-р зураг. Prophet болон бусад загварын таамаглал гаргасан график дүрслэл

b) Ангилалтын функцыг ашигласан байдал

АНГИЛАЛТЫН ФУНКЦЫГ АШИГЛАСАН БАЙДАЛ

4-Р ХҮСНЭГТ.

	Accuracy	Precision	Recall	F1_Score
Random Forest Classifier	0.9851	0.9798	0.9923	0.9861
Gradient Boosting Classifier	0.9769	0.9676	0.9898	0.9786
Decision Tree Classifier	0.9755	0.9746	0.9796	0.9771
Logistic Regression	0.8995	0.9056	0.9056	0.9056



8-р зураг. Ангилалтын функцыг ашигласан байдал

c) ASD нөлөөлөгч хүчин зүйлсийг тодорхойлох

Correlation Analysis (Харьцааны шинжилгээ)

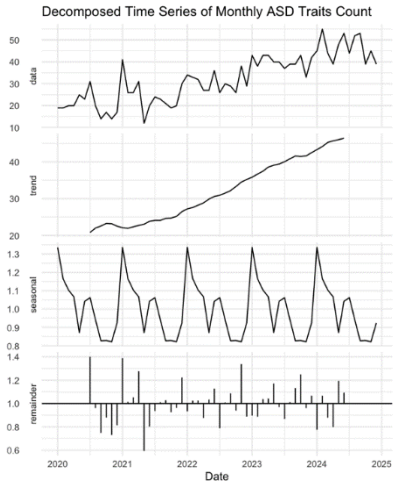
Feature Importance (Шинж чанарын ач холбогдол)

ADS улирлын чанар, хэрэглэгчийн төрөл, хямдралын нөлөө гэх мэт.

IV. ТУРШИЛТ, ҮР ДҮН

Бэлтгэсэн өгөгдлийн багцад шууд сургалтыг хэрэгжүүлэхэд дараах үр дүнг гарган авсан.

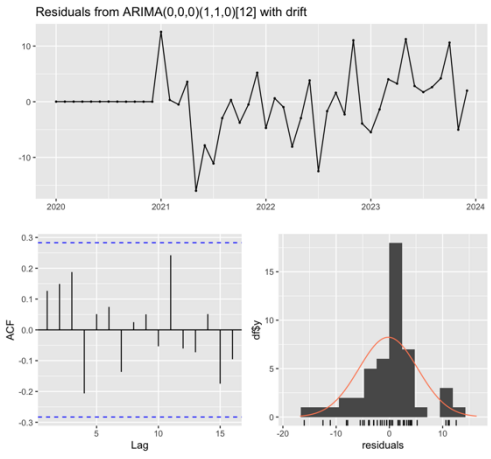
A. ASD өгөгдлийг ашиглан тренд болон улирлын шинжилгээ хийх.



9-р зураг. ASD он цагийн визуаль дүрслэл, түүний улирлын тренд ялгаатай байдлын дүрсэлсэн байдал.

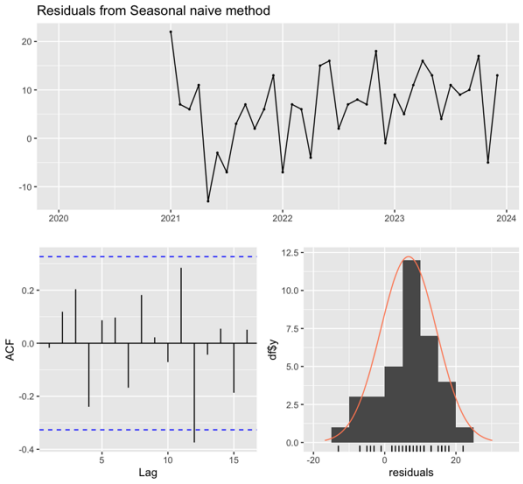
B. ASD загваруудын гүйцэтгэлийг харьцуулах

1) ARIMA, SARIMA загвар



10-р зураг. ARIMA, SARIMA benchmark

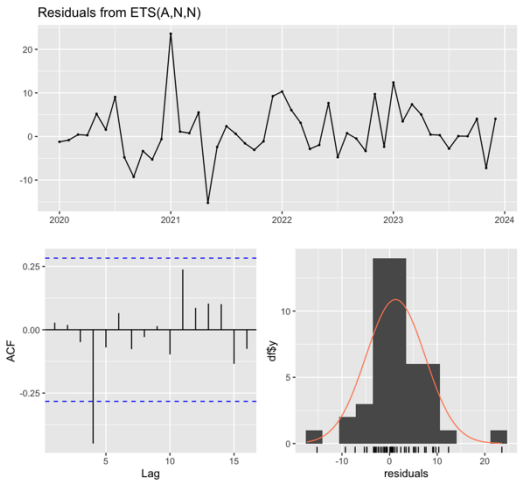
2) Seasonal naive benchmark



11-р зураг. Naïve

seasonal naive benchmark хийсэн/auto cor-тэй, Residual SD = 371.90 -өндөр/.

3) ETS



12-р зураг. ETS

C. ASD таамаглал гаргах

Нийт хугацааны өгөгдөлд дараагийн 3 жилийн ASD орлогын таамаглалыг гаргаж дүрслэв.

```
Forecasts:
         Point Forecast    Lo 80    Hi 80    Lo 95    Hi 95
Dec 2024       4733.914 4418.227 5049.602 4251.112 5216.717
Jan 2025       4312.148 3932.167 4692.129 3731.017 4893.279
Feb 2025       3965.692 3530.821 4400.563 3300.615 4630.770
Mar 2025       4891.391 4407.821 5374.960 4151.835 5630.947
Apr 2025       4809.994 4282.200 5337.788 4002.802 5617.185
May 2025       4902.203 4333.614 5470.791 4032.621 5771.784
Jun 2025       4768.954 4162.307 5375.601 3841.168 5696.740
Jul 2025       5125.485 4483.031 5767.939 4142.937 6108.034
Aug 2025       4956.595 4280.226 5632.963 3922.179 5991.011
Sep 2025       4804.709 4096.047 5513.370 3720.905 5888.513
Oct 2025       4913.590 4174.044 5653.135 3782.552 6044.627
Nov 2025       4746.061 3976.824 5515.297 3569.615 5922.507
Dec 2025       4733.914 3936.135 5531.694 3513.816 5954.012
Jan 2026       4312.148 3486.813 5137.484 3049.907 5574.390
Feb 2026       3965.692 3113.691 4817.693 2662.669 5268.715
Mar 2026       4891.391 4013.534 5769.247 3548.825 6233.957
Apr 2026       4809.994 3907.021 5712.966 3429.016 6190.971
May 2026       4902.203 3974.794 5829.611 3483.854 6320.551
Jun 2026       4768.954 3817.737 5720.171 3314.194 6223.714
Jul 2026       5125.485 4151.042 6099.929 3635.203 6615.768
Aug 2026       4956.595 3959.465 5953.724 3431.617 6481.572
Sep 2026       4804.709 3785.398 5824.019 3245.808 6363.610
Oct 2026       4913.590 3872.571 5954.609 3321.488 6505.691
Nov 2026       4746.061 3683.744 5808.378 3121.387 6370.735
```

13-р зураг. ASD таамаглал

ДҮГНЭЛТ

Энэхүү судалгааны ажлаар "Toddler ASD Dataset (2018)" өгөгдлийг ашиглан аутизмын спектрийн эмгэг (АСЭ)-ийг эрт илрүүлэх, ангилах боломжийг машин сургалтын (ML), гүн сургалтын (DL), тайлбарлагдах хиймэл оюуны (XAI) аргуудаар судаллаа. Судалгаанд логистик регресс, шийдвэрийн мод, санамсаргүй ой, нейрон сүлжээ, XGBoost зэрэг хэд хэдэн ангилах загваруудыг ашигласан бөгөөд тэдгээрийн гүйцэтгэлийг нарийвчлал, мэдрэг чанар, онцлог шинж чанар, AUC зэрэг үзүүлэлтүүдээр харьцуулан үнэлсэн.

Судалгааны үр дүнд XGBoost загвар хамгийн өндөр нарийвчлалтай (96%) ажиллаж, ASD-тай болон ASD-гүй хүүхдийг ялгахдаа хамгийн сайн үзүүлэлттэй байгааг тогтоов. Түүнчлэн SHAP болон LIME зэрэг тайлбарлагдах хиймэл оюуны аргуудаар тухайн загваруудын шийдвэр гаргах үйл явцад чухал нөлөөтэй шинж чанаруудыг тодорхойлсон нь эмнэлгийн мэргэжилтнүүдийн хувьд тухайн загварыг ойлгомжтой, итгэл төрүүлэхүйц байхад тус дэмжлэг үзүүлж байна.

Судалгаанаас дараах гол дүгнэлтүүдийг хийж болно:

ASD-ийн эрт илрүүлэлтэд ML, DL загварууд үр дүнтэй хэрэгжих боломжтой – Ялангуяа эцэг эх, асран хамгаалагчдын өгсөн асуумж, зан төлөвийн мэдээлэл дээр суурилсан ангилал нь ASD-ийг оношлоход анхан шатны нарийвчлалтай арга болж чадна.

XAI аргууд нь хиймэл оюуны шийдвэр гаргалтыг тайлбарлах, ойлгомжтой болгоход чухал үүрэгтэй – SHAP болон LIME аргууд нь эмнэлгийн мэргэжилтнүүд, судлаачдын хувьд тухайн загварын шийдвэр гаргалтыг итгэлтэйгээр хүлээн зөвшөөрөхөд дэмжлэг үзүүлж байна.

Бодлого боловсруулагч, эмч, сэтгэл зүйч нарт өгөгдөлд суурилсан шийдвэр гаргалтыг дэмжих боломж бүрдэнэ – Судалгааны загваруудыг эрүүл мэндийн салбарын бодлого, скрининг хөтөлбөр, оношилгооны чиглэлд ашиглах боломжтой.

Цаашдын судалгаанд илүү өргөн хүрээний өгөгдөл, хэлбэржилт бүхий загварчлал (multimodal learning), урт хугацааны хяналт (longitudinal data), мөн эмнэлзүйн туршилт дээр үндэслэсэн баталгаажуулалт хийх шаардлагатай бөгөөд энэ нь хиймэл оюуныг хүүхдийн сэтгэцийн эрүүл мэндийн оношилгоонд үр дүнтэй, хариуцлагатай хэрэглэх үндэс болох юм..

НОМ ЗҮЙ

[1] American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders (DSM-5)*, 5th ed. Washington, DC, USA: American Psychiatric Publishing, 2013.

[2] J. Zeidan, E. Fombonne, J. Scorah, A. Ibrahim, M. S. Durkin, S. Saxena, A. Yusuf, A. Shih, and M. Elsabbagh, "Global prevalence of autism: A systematic review update," Autism Research, vol. 15, no. 5, pp. 778–790, May 2022. [Online]. Available: https://doi.org/10.1002/aur.2696

[3] Z. S. Warren, D. R. Stone, and J. L. Sweeney, "Early diagnosis and treatment of autism spectrum disorder: The importance of early intervention," *Pediatrics*, vol. 135, no. 5, pp. 971–982, 2015.

[4] F. Thabtah, "Toddler Autism Dataset," Kaggle, 2018. [Online]. Available: https://www.kaggle.com/datasets/fedesoriano/autism-screening-for-toddlers

[5] F. Thabtah, "Autism Spectrum Disorder Screening: Machine Learning Adaptation and DSM-5 Fulfillment," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 6, pp. 1–10, 2018.

[6] K. Duda, A. Kosmicki, and M. Wall, "Testing the accuracy of an observation-based classifier for rapid detection of autism risk," *Translational Psychiatry*, vol. 6, no. 10, pp. 1–9, 2016.

[7] S. Lai, A. Lombardo, and S. Baron-Cohen, "Prevalence of autism spectrum conditions in individuals of different ethnicities and socioeconomic backgrounds," *The Lancet Psychiatry*, vol. 6, no. 5, pp. 351–362, 2019.

[8] Y. Chen and P. Zhao, "Early screening of autism spectrum disorder based on machine learning models and feature selection," *IEEE Access*, vol. 8, pp. 227107–227115, 2020.

[9] D. Bone et al., "Opportunities and challenges in developing predictive models of autism spectrum disorder using machine learning," *npj Digital Medicine*, vol. 4, no. 1, pp. 1–11, 2021.

[10] S. Shephard et al., "Autism spectrum disorder diagnosis: Challenges and opportunities for public health and policy," *International Review of Psychiatry*, vol. 30, no. 1, pp. 34–48, 2018.

[11] United Nations, "Convention on the Rights of Persons with Disabilities," 2006. [Online]. Available: https://www.un.org/disabilities/documents/convention/convoptprot-e.pdf

[12] J. Pellicano, D. Crane, E. K. Hill, and L. Goodley, "The right to diagnosis: The social and ethical implications of ASD diagnosis for children and their families," *Journal of Autism and Developmental Disorders*, vol. 50, no. 1, pp. 1–10, 2020.

[13] World Health Organization, "Autism spectrum disorders & other developmental disorders: From raising awareness to building capacity," WHO Report, Geneva, Switzerland, 2013.

[14] Autism Speaks, "Autism Screening," [Online]. Available: https://www.autismspeaks.org/autism-screening. [Accessed: 10-Mar-2025].

[15] F. Thabtah, *Toddler ASD Dataset Description*, Manukau Institute of Technology, Auckland, 2018.

[16] L. Nygren et al., "A systematic review of screening tools for autism spectrum disorder in toddlers aged 12 to 36 months," *Acta Paediatrica*, vol. 101, no. 1, pp. 12–24, 2012.

АЮУЛТАЙ АЧАА ТЭЭВРИЙН МАРШРУТЫГ ГРАФ БҮТЭЦ АШИГЛАН ОНОВЧЛОХ НЬ

Хишигбаярын АРИУНЗАЯА[1], Батжаргалын ДОЛГОРСҮРЭН[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: b.dolgorsuren@must.edu.mn[2]

Хураангуй: **Аюултай ачаа тээвэрлэх нь олон нийтийн аюулгүй байдал, хүрээлэн буй орчинд эрсдэл учруулж болзошгүй учир тээврийн маршрутыг оновчлох шаардлагатай. Энэхүү судалгааны зорилго нь замын хөдөлгөөний өгөгдөл, хориглосон бүс болон хяналтын постуудын мэдээлэл, холбогдох хууль дүрэм журам, стандартууд, мөн богино зам тооцоолох алгоритмуудыг ашиглан хамгийн аюулгүй бөгөөд үр ашигтай маршрутыг тодорхойлох явдал юм. Судалгаанд OSM замын өгөгдөл, NetworkX санг ашиглаж, маршрутыг олон шалгуурт болон олон зорилтот оновчлолын аргачлалыг шинээр танилцууллаа. Судалгааны үр дүнд маршрутын аюулгүй байдлыг сайжруулж, нийт тээвэрлэлтийн үр ашгийг өсгөх, тээвэрлэлтийн цагийг бууруулах боломжтойг харууллаа.**

***Түлхүүр үг*: аюултай ачаа тээвэр, тээврийн маршрут, богино замын бодлого, оновчлолын алгоритм**

I. УДИРТГАЛ

Техник, технологийн хөгжилтэй холбоотойгоор логистик, тээвэрлэлт, нийлүүлэлтийн сүлжээнд олон шинэчлэлүүд хийгдэж, илүү үр ашигтай шийдлүүдийг эрэлхийлэх шаардлага нэмэгдсээр байна. Ялангуяа аюултай ачаа тээвэрлэлт нь онцгой анхаарал шаарддаг бөгөөд зам тээврийн осол, байгаль орчинд үзүүлэх нөлөө, хүн амын аюулгүй байдал зэрэг олон эрсдэлийг дагуулдаг. Иймээс аюултай ачаа тээвэрлэх маршрутыг оновчлох нь тээврийн салбарын амжилттай хөгжлийн түлхүүр болно. Монгол Улсын хувьд, Улаанбаатар хотын замын нөхцөл байдал нь өндөр ачаалалтай, хөдөлгөөний эрчим болоод түгжрэл ихтэй, улирал, цаг агаарын байдалд хүчтэй нөлөөлдөг онцлогтой. Аюултай ачаа тээвэрлэх нь замын түгжрэл, хүн ам төвлөрсөн бүсүүд, сургуулийн орчин, эмнэлэг зэрэг цэгүүдийг дайран өнгөрөх нь эрсдэлийг улам нэмэгдүүлдэг. Стандарт бус маршрут төлөвлөлт нь замын ачааллыг нэмэгдүүлэх, зам тээврийн осол, байгаль орчинд үзүүлэх сөрөг нөлөөг ихэсгэх шалтгаан болдог. Тиймээс аюултай ачаа тээвэрлэлтийн оновчтой маршрутыг тодорхойлох нь Монгол Улсад тулгамдаж буй асуудлуудын нэг. Энэхүү судалгааны гол зорилго нь хортой, шатамхай ачаа тээвэрлэх маршрутыг оновчлох замаар осол, эрсдэлийг багасгах, замын хөдөлгөөний урсгалыг сайжруулах явдал юм. Зорилгодоо хүрэхийн тулд бид OpenStreetMap (OSM) замын өгөгдөл, замын хөдөлгөөний мэдээлэл, хориглосон буюу эрсдэлтэй бүсийн байршил дээр үндэслэн маршрут төлөвлөх богино зам тооцоолох аргачлалыг ашигласан. Судалгаанд NetworkX, OSMnx сангуудыг ашиглаж, маршрутыг оновчлохдоо Dijkstra болон A* алгоритмуудын хослолыг ашиглаж системийг хөгжүүлсэн. Энэхүү алгоритм нь бодит өгөгдөлд тулгуурлан оновчтой маршрут гаргах бөгөөд бодит цагийн хөдөлгөөний өгөгдлийг ашигласнаар цаашид алгоритмыг сайжруулах боломжтой. Судалгааны үр дүнд аюултай ачаа тээвэрлэх эхлэлийн цэгээс, хүргэх эцсийн цэг хүртэлх хамгийн оновчтой маршрутыг тодорхойлох аргачлал боловсруулсан бөгөөд энэ нь Монгол Улсын аюултай ачаа тээвэрлэлтийн замын нөхцөл байдалд тохирсон анхны суурь судалгааны ажил болно хэмээн харж байна.

II. ОНОЛЫН ХЭСЭГ

2.1 Аюултай ачаа тээврийн ангилал, маршрут

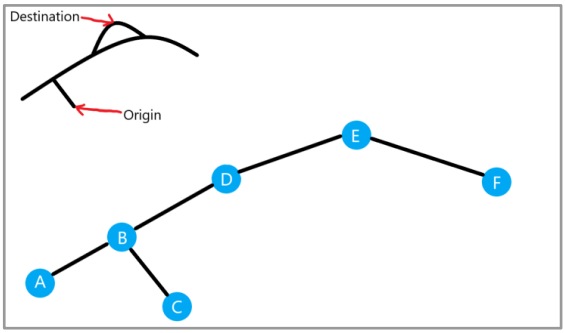
“Аюултай ачаа” - тээвэрлэлтийн үед хүний амь нас, эрүүл мэнд, байгаль орчинд хор хөнөөл тарих, эд хөрөнгийн хохирол учруулж болзошгүй элдэв бодис, түүгээр хийсэн эд зүйл, үйлдвэрийн хаягдал, аж ахуйн зориулалт бүхий бусад зүйл болон тэдгээрийн ариутгаагүй сав, баглаа, боодлыг; гэж Монгол Улсын Замын хөдөлгөөний дүрэмд заасан байдаг. Аюултай ачаа тээврийн 9 ангилал байдгаас Монгол улсад авто замаар 2,3,4,6-р ангиллын аюултай ачааг түлхүү тээвэрлэдэг. Аюултай ачаа тээвэрлэх аж ахуйн нэгж байгууллага нь аюултай ачаа тээвэрлэх талаарх мэдээллийг цагдаагийн байгууллагад урьдчилан гарган өгч, тээвэрлэлтийн хөдөлгөөний замнал, цагийн хуваарийг тохиролцож зөвшөөрөл авах бөгөөд аймаг, нийслэлийн авто тээврийн талаарх бодлого шийдвэрийн хэрэгжилтийг зохион байгуулах байгууллагаас баталгаажуулсан замын хуудас авч тээвэрлэлт гүйцэтгэнэ; хэмээн Авто тээврийн хэрэгслээр хүний амь нас, эрүүл мэнд, хүрээлэн буй орчинд аюул, хохирол учруулж болзошгүй ачаа тээвэрлэх журамд заасан байдаг.

1-р зураг. Аюултай ачааны ангилал

Гэвч бодит байдал дээр тээвэрлэгч байгууллагууд жин тонн хэтрүүлж, нэгдсэн маршрутгүй замаар аюултай ачааг тээвэрлэж ард иргэдийг аюултай байдалд оруулсаар байна.

2.2 Граф

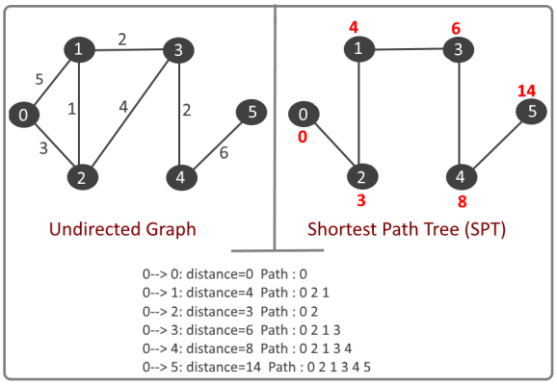
Граф (Graph) нь математик загвар бөгөөд түүний бүтэц нь зангилаа (nodes) болон эдгээр зангилаануудын хоорондох холболт (edges) -оос бүрддэг. Графын бүтэц нь төрөл бүрийн сүлжээг загварчлахад ашиглагддаг бөгөөд аюултай ачаа тээвэрлэлтийн маршрутыг оновчлох асуудалд ч мөн тохиромжтой байдаг. Графын онцлог нь тусгай нөхцөл шаардлагатай замууд болон зангилаануудыг илэрхийлэх чадвартай бөгөөд энэ нь аюулгүй байдлыг хангах, ачааны тээвэрлэлтийн хамгийн тохиромжтой маршрутыг олоход чухал үүрэг гүйцэтгэнэ. Зангилаа (Nodes) нь графын үндсэн нэгж бөгөөд ачаа тээвэрлэх замын оновчлолд агуулах, шатахуун түгээх станц, хянах цэг зэргийг илэрхийлнэ. Ирмэг (Edges) нь зангилаануудыг холбосон замууд бөгөөд аюултай ачааны тээвэрлэлтэд зориулагдсан зам, гүүр, туннел зэрэг элементүүдийг илэрхийлнэ. Холболтууд нь чухал үзүүлэлтүүдийг агуулж болох бөгөөд энэ нь хурд, замын нөхцөл, аюулгүй байдлын хязгаарлалтууд, эрсдэл зэрэг үзүүлэлтүүдийг хэмжих боломжтой. Графыг аюултай ачаа тээвэрлэлтийн маршрутыг оновчлох, аюулгүй байдалд суурилсан шийдлүүдийг боловсруулж, хамгийн тохиромжтой замыг олоход ашиглана. Замын нөхцөл, төрөл, хориглосон бүсүүд, аюултай бүсүүдийг граф дээр тусгайлан тэмдэглэж, эрсдэлтэй бүсүүдээс зайлсхийх замыг тодорхойлж, аюултай ачаа тээвэрлэхэд тохирсон өргөнтэй замыг санал болгож, хамгийн боломжит богино замыг тодорхойлоход ашиглана.



2-зураг. Граф хэрэглээ

2.3 Богино зам тооцоолох алгоритм

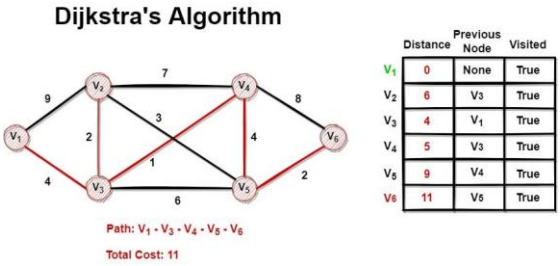
Богино зам тооцоолох алгоритм нь графын дотор хамгийн богино замыг олох, маршрутыг оновчлох, аюулгүй байдал, хугацаа, зардал гэх мэт үзүүлэлтүүдийг хамгийн бага байлгах зорилготой математик аргачлал юм. Энэ төрлийн алгоритмууд нь аюултай ачаа тээвэрлэгч болон аюултай ачааны аюулгүй байдалд ихээхэн ач холбогдол өгдөг бөгөөд маршрут оновчлолд хамгийн өргөн ашиглагддаг.



3-р зураг. Богино зам тооцоолох алгоритм

2.3.1 Dijkstra's Algorithm

Дейкстрийн алгоритм нь нэг эхлэлээс бусад бүх зангилаа руу хамгийн богино замыг олохын тулд өргөн хэрэглэгддэг хамгийн алдартай алгоритм юм. Энэ алгоритм нь жингийн граф дээр хамгийн бага зардалтай замыг олох боломжийг олгодог. Граф дахь эхлэх оройг сонгоно. Энэ оройд хамгийн бага зайг 0 гэж тохируулна. Эхлэх оройгоос гарах бүх холболтод хамгийн бага зайг тооцоолно. Эдгээр зайг шинэчлэн хамгийн бага утгыг сонгоно. Тухайн оройгоос гарах хамгийн бага зайтай оройг сонгоно, шаардлагатай тохиолдолд шинэчлэн зайн утгыг тодорхойлно. Эдгээр алхмуудыг дахин давтах хүртэл бүх оройнуудад хүрэх хамгийн богино замуудыг олно.



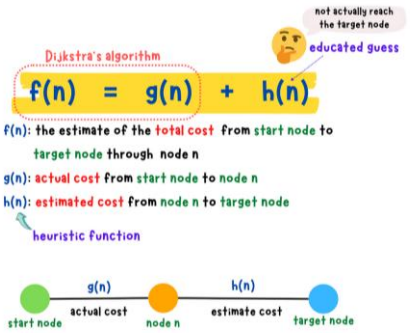
	Distance	Previous Node	Visited
V1	0	None	True
V2	6	V3	True
V3	4	V1	True
V4	5	V3	True
V5	9	V4	True
V6	11	V5	True

4-р зураг. Dijkstra's Algorithm ажиллах зарчим

f(n) = g(n) буюу эхлэлийн зангилаанаас n-д хүрэх хамгийн бага зардлыг g(n) тодорхойлогдоно.

2.3.2 A (A star) алгоритм*

A* алгоритм нь хамгийн богино замыг олох зорилготой, хэрэглэгчийн шаардлагад нийцсэн шийдлийг тодорхойлохыг зорьдог хайлтын алгоритм юм. Энэ нь тухайн нөхцөлд хамгийн оновчтой, хамгийн бага зардалтай замыг олохын тулд эвристик функц (Heuristic function) болон зан төлөв (Cost function) хоёрын хослолыг ашигладаг. f(n) = g(n) + h(n) томьёогоор илэрхийлэгдсэн хамгийн бага замыг оновчилно. g(n) буюу эхлэлээс тухайн зангиллаа хүртэлх бодит хамгийн бага зардал, h(n) буюу тухайн зангилаанаас зорилтот цэг хүртэлх heuristic буюу ойролцоогоор тооцоолсон зардал байна. Аюултай ачаа тээвэрлэлтийн хувьд тус зардал нь замын төрөл, тээвэрлэлттэй холбоотой аюулын эрсдэл орж болно.



5-р зураг. A* алгоритм ажиллах зарчим

III. ТУРШИЛТЫН ХЭСЭГ

Туршилтын судалгаанд Улаанбаатар хотын шатахуун түгээх станцуудын байршил, агуулахуудын мэдээлэл, замын сүлжээний өгөгдөл болон хориглосон бүсүүдийн мэдээллийг ашигласан. Өгөгдлийг OpenStreetMap болон холбогдох төрийн байгууллагын өгөгдлийн сангаас авсан.

3.1 Замын хөдөлгөөний нөхцөл

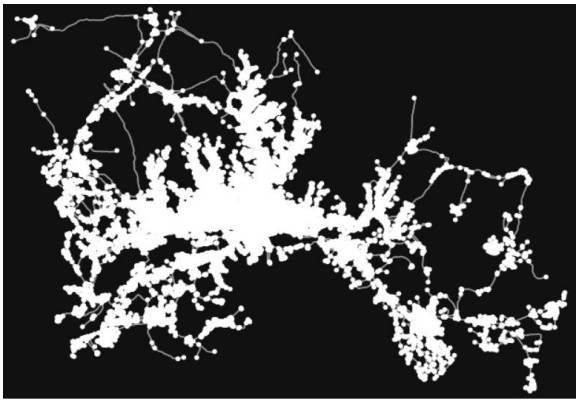
Улаанбаатар хотод аюултай ачаа тээвэрлэх нь тодорхой бөгөөд төвлөрсөн хүн ам, ачаалалтай замын сүлжээ, байгаль орчны эрсдэл зэрэг олон хүчин зүйлсийг анхаарах шаардлагатай. Монгол улсын замын хөдөлгөөний дүрэмд, чиргүүлтэй автомашин суурин газарт 60 км/цаг хурдаас хэтрэхгүй зорчих; эсрэг хөдөлгөөнтэй хоёр эгнээгээр зорчдог замд, түүнчлэн дунд эгнээ нь сөрөг хөдөлгөөнтэй гурван эгнээгээр зорчдог замд овор ихтэй буюу урт тээврийн хэрэгслийн жолооч нь зорчих хэсгийн баруун гар талын захад аль болох ойр явах бөгөөд араас яваа тээврийн хэрэгсэл өөрийг нь аюулгүй гүйцэж түрүүлэх боломжтой байх хоорондын зайг урд яваа тээврийн хэрэгслээс барьж явах; MNS 4978:2000 (Аюултай ачааны авто тээврийн ерөнхий шаардлага) стандартад аюултай ачаа тээвэрлэх авто зам нь 2 ба түүнээс дээш эгнээтэй байх ёстой хэмээн заасан байдаг. Иймд, OSMx -ээс гаргаж авсан замын төрөл, замын өргөн буюу эгнээний тоо, хурдны хязгаарлалт, хүн ам төвлөрсөн суурин бүс (хориглосон) бүсээс 50 метрээс хол байхаар шаардлагуудыг тусгаж өгсөн. Мөн Улаанбаатар хотын одоогийн түгжрэлийн нөхцөл байдлыг нэмж, хугацааны хувьд хамгийн хурдан, хамгийн аюулгүй, хамгийн зардал багатай маршрут тус бүрийг оновчлох боломжтой.

3.2 OSMnx, NetworkX сангууд

OSMx болон NetworkX сангууд нь замын сүлжээний өгөгдлийг боловсруулж, граф дээр тооцоолол хийхэд өргөн ашиглагддаг Python сангууд юм.

3.2.1 OSMnx

OSMnx (OpenStreetMapX) нь OpenStreetMap-ийн өгөгдлийг боловсруулж, авто замын сүлжээ үүсгэх, зангилаа болон ирмэгүүдийг тодорхойлох, газарзүйн байршлыг боловсруулахад хэрэглэгддэг. Энэ сангийн тусламжтайгаар замын төрөл ("motorway", "trunk", "primary", "secondary"), эгнээний тоо, хурдны хязгаар зэрэг шинж чанаруудыг авч ашигласан.



6-р зураг. OSMnx ашиглан Улаанбаатар хотын замын өгөгдөл татсан байдал

3.2.2 NetworkX

NetworkX нь графын өгөгдлийн бүтэцтэй ажиллахад зориулагдсан бөгөөд зам тооцоолох, оновчтой маршрут гаргах, зангилаануудын холболтыг шалгах зэрэгт ашиглагддаг. Энэхүү судалгаанд NetworkX-ийг ашиглан хамгийн богино болон аюулгүй маршрутыг тодорхойлж, холбоост граф үүсгэж, хязгаарлагдмал бүсүүдийг шалгасан. Энэ нь тээврийн төлөвлөлтийг оновчтой болгох, замын хөдөлгөөний аюулгүй байдлыг сайжруулахад чухал үүрэг гүйцэтгэдэг. Маршрут тооцоолохдоо бид стандарт хамгийн богино замын алгоритмуудыг ашигласан боловч нэмэлт нөхцөлүүдийг харгалзан үзсэн нь ердийн тээвэрлэлтийн төлөвлөлтөөс ялгаатай гэж харж байна.

7-р зураг. OSMnx, NetworkX ашигласан Агуулахаас ШТС хүртэлх замын маршрут

OSMnx ашиглан доорх өгөгдлийг цуглуулсан.

1-Р ХҮСНЭГТ OSMNX АШИГЛАН ГАРГАЖ АВСАН ӨГӨГДӨЛ

Зангилаа тоо	33885
Ирмэгийн тоо	84468
Замын ангилал, төрөл	motorway, trunk, primary, secondary, tertiary, residential, unclassified
Замын эгнээ	1 болон түүнээс дээш
Хурдны хязгаар	60 км/цагаас бага
Хориглосон бүс	school, kindergarten, hospital

Агуулах, шатахуун түгээх станцын мэдээллийг уртраг, өргөргийн хэмжээгээр оруулж өгсөн.

2-Р ХҮСНЭГТ АГУУЛАХ БОЛОН ШТС КООРДИНАТ

Нэр	Газрын зураг дээрх координат
Шунхлай УБГТБА	47.89167841408549, 106.76833661187626
Улаанбаатар хот, Баянзүрх дүүрэг, 1-р хороо, Шунхлай ШТС	47.9287492067807, 106.93493400026867

IV. ҮР ДҮН

Энэхүү судалгааны хүрээнд OSMx болон NetworkX сангуудыг ашиглан аюултай ачааны тээвэрлэлтийн маршрутыг оновчтой тодорхойлох туршилтыг хэд хэдэн нөхцөлүүд дээр хийсэн. Туршилтын үр дүнг дараах байдлаар харуулав.

 - Агуулах

 - Шатахуун түгээх станц

 - Хориглосон бүс

 - Оновчилсон маршрут

Туршилт 01: Эхний туршилтаар хориглосон бүсүүдээс 50 метрээс хол явах ёстой хэмээн нөхцөл тавьж маршрутыг оновчилсон. Нөхцөлийг дараах томьёогоор илэрхийлбэл:

$$G = (V, E), \forall v \in V$$

$$\text{if } d(v, \text{хориглосон\_бүс}) < 50\text{m}, v \notin V$$

Энд:

- V — Графын оройнуудын олонлог (замын уулзварууд, байршлууд)
- v ∈ V — Графын тодорхой нэг орой буюу байршил

- d (v, хориглосон_бүс) — v орой болон хориглосон бүсийн хоорондох зай
- Нөхцөл: Хэрэв v нь хориглосон бүсээс 50м-ээс ойрхон байвал тухайн оройг графаас хасах буюу v∉V

7-р зураг. Туршилтын үр дүн - 01

Туршилт 02: Дараагийн туршилтад аюултай ачаа тээвэрлэлт хийх замыг хязгаарласан ба үүнд, замын төрөл нь "motorway", "trunk", "primary", "secondary" зэрэг байхаар нөхцөлийг зааж өгсөн. Нөхцөлийг дараах байдлаар томьёолбол:

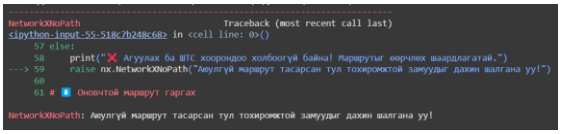
G = (V, E) , ∀e ∈ E

If type(e) ∉ {"motorway", "trunk", "primary",

"secondary"}, e ∉ E

Энд:

- **e** - зам (ирмэг), хэрэв тухайн замын төрөл зөвшөөрөгдсөн ангилалд багтахгүй бол маршрутаас хасна.



8-р зураг. Туршилтын үр дүн - 02

Туршилт 03: Энэхүү туршилтаар аюултай ачаа тээвэрлэлт хийх хязгаарлалтыг замын урсгал нь 2 ба түүнээс дээш байхаар нөхцөлийг зааж өгсөн. Нөхцөлийг томьёолбол:

$$G = (V, E)\ ,\ \forall e \in E\ ,\ if\ lanes(e) < 2,\ e \notin E$$

Энд:

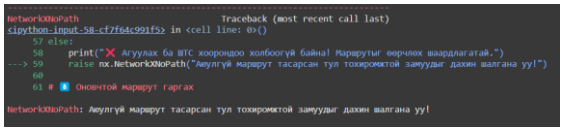
- e - Графын ирмэг (зам)
- lanes(e) - Тухайн замын урсгалын тоо. Хэрэв замын урсгал хоёроос бага бол тухайн замыг маршрутын сүлжээнээс хасна.

Энэ тохиолдолд аюултай ачаа тээвэрлэх тохиромжтой маршрут гарч ирээгүй буюу нөхцөл тавигдсаны дараа маршрутын сүлжээнээс бүх боломжит замууд хасагдаж, тээвэрлэх боломжтой маршрут олдоогүй. Үүнийг дараах байдлаар томьёолж болно:

∀p ∈ P,if P=∅, Not found map

Энд:

- P - Боломжит маршрутуудын олонлог Хэрэв бүх боломжит маршрут устаж P = ∅ (хоосон олонлог) болсон бол тохиромжтой зам байхгүй.



9-р зураг. Туршилтын үр дүн - 03

Туршилт 04: Туршилт 03 дээрх нөхцөлийг сулруулж, замын урсгал нь 1 ба түүнээс дээш байхаар нөхцөлийг зааж өгсөн.

G = (V, E) , ∀e ∈ E , if lanes(e) < 1, e ∉ E

Энд:

- e - Графын ирмэг (зам)
- lanes(e) - Тухайн замын урсгалын тоо. Хэрэв замын урсгал нэгээс бага бол тухайн замыг маршрутын сүлжээнээс хасна.

Энэхүү шинэ нөхцөл нь маршрутын боломжийг нэмэгдүүлнэ. Өөрөөр хэлбэл:

$$P=\emptyset$$

Энд:

- P - Боломжит маршрутуудын олонлог Хэрэв маршрутын сүлжээн дэх замууд үлдэж байвал тохиромжтой маршрут олдох боломжтой.

10-р зураг. Туршилтын үр дүн - 04

Туршилт 3, 4-ийн үр дүнгээс харахад Улаанбаатар хотод аюултай ачаа тээвэрлэх стандартын шаардлага хангасан 2 ба түүнээс дээш эгнээ бүхий зам байхгүй байгаа нь харагдаж байна.

Туршилт 05: Сүүлийн туршилтад хориглосон бүсээс 50 метрээс хол, замын төрөл нь "motorway",

"trunk", "primary", "secondary" байх, замын урсгал нь 1 ба түүнээс дээш байх, хурдны хязгаарлалт 60 км/цагаас бага байхаар нөхцөлүүдийг зааж өгсөн.

∀e ∈ E, if (d (v,хориглосон_бүс) ≥ 50m) ∧ (type (e) ∈ {"motorway","trunk","primary", "secondary"}) ∧ (lanes(e) ≥ 1) ∧ (speedLimit(e) < 60km/h), e ∈ E

Энд:

- e - Зам (ирмэг)
- d (v,хориглосон_бүс) ≥ 50m - Замын орой (байршил) хориглосон бүсээс 50м-ээс хол байх
- type(e)∈{"motorway","trunk","primary","secondary"} - Замын төрөл нь зөвхөн эдгээр ангилалд хамаарах
- lanes(e) ≥1 - Замын урсгал нь 1 ба түүнээс дээш байх
- speedLimit(e) < 60 km/h - Замын хурдны хязгаарлалт 60 км/цаг-аас бага байх
- Хэрэв эдгээр нөхцөлүүд хангагдвал тухайн зам графын сүлжээнд үлдэнэ.

11-р зураг. Туршилтын үр дүн - 05

ДҮГНЭЛТ

Энэхүү судалгааны зорилго нь аюултай ачаа тээвэрлэх хамгийн аюулгүй, үр ашигтай маршрутыг оновчлох, эрсдэлийг бууруулахад чиглэгдсэн байсан. Судалгааны үр дүнгээс харахад, аюултай ачаа тээвэрлэх маршрутын оновчлол нь замын сүлжээ, хурдны хязгаарлалт, хориглосон бүсүүд, тээвэрлэлттэй холбоотой эрсдэлийг харгалзан үзэх шаардлагатай болохыг баталсан.

Оновчтой маршрутыг тодорхойлохдоо OpenStreetMap (OSM) замын өгөгдлийг ашиглан графын аргачлал, Dijkstra болон A* алгоритмуудын хослолыг ашиглан аюулгүй, богино зам гаргах боломжийг судалсан. Судалгааны явцад харагдсан хамгийн чухал асуудал нь Улаанбаатар хотын замын сүлжээний нөхцөл байдал бөгөөд аюултай ачаа тээвэрлэхэд тохиромжтой зам дутагдалтай байгаа юм. Стандартын шаардлага хангасан 2 ба түүнээс дээш эгнээ бүхий замын хомсдол нь аюултай ачаа тээвэрлэхэд томоохон саад болж байна. Үүнээс үүдэн жолооч нар хүн ам төвлөрсөн шатахуун түгээх станцуудад шөнийн цагаар тээвэрлэлт хийх болсон ба энэ нь жолооч нойрмоглох, анхаарал сулрах зэргээс болж аюул осол үүсгэх эрсдэлтэй.

Туршилт ба үр дүнгээс харахад, аюултай ачааны тээвэрлэлтийн оновчтой маршрут нь хурдны хязгаар, замын төрөл, замын өргөн буюу эгнээ болон хориглосон бүсүүдийг харгалзан зөв зохион байгуулах нь чухал гэдгийг харуулж байна. Одоогийн замын нөхцөлд стандарт шаардлагад нийцсэн маршрут байхгүй ч, тус судалгаа нь аюултай ачаа тээвэрлэлтэд тохирсон замын сүлжээг оновчлон боловсруулж, тээврийн аюулгүй байдлыг сайжруулах боломжтой.

Тус судалгааг бодит цагийн замын өгөгдөл, хугацааг тооцоолон сайжруулж чадвал Монгол Улсад аюултай ачаа тээвэрлэх асуудлыг шийдвэрлэхэд чухал алхам болж, ирээдүйд ийм төрлийн тээвэрлэлтэд тохирсон замын төлөвлөлт, аюулгүй байдлын стандартыг боловсронгуй болгоход тусалж чадна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Монгол улсын замын хөдөлгөөний дүрэм: https://legalinfo.mn/mn/detail?lawId=208663

[2] Замын хөдөлгөөний аюулгүй байдлын тухай хууль: https://legalinfo.mn/mn/detail/11224

[3] АВТО ТЭЭВРИЙН ХЭРЭГСЛЭЭР АЧАА ТЭЭВЭРЛЭХ ДҮРЭМ: https://legalinfo.mn/mn/detail?lawId=210717

[4] MNS 4978:2000 (Аюултай ачааны авто тээврийн ерөнхий шаардлага)

[5] Авто тээврийн хэрэгслээр хүний амь нас, эрүүл мэнд, хүрээлэн буй орчинд аюул, хохирол учруулж болзошгүй ачаа тээвэрлэх журам: https://legalinfo.mn/mn/detail?lawId=205058

И-МЭЙЛ АЮУЛГҮЙ БАЙДЛЫН ПРОТОКОЛУУД: SPOOFING ХАЛДЛАГААС УРЬДЧИЛАН СЭРГИЙЛЭХ

Олзвойн ХАЛИУНАА[1], Нэргүйн ШҮРЭНЦЭЦЭГ[1], Мөнх-Эрдэнийн БОЛОР-ЭРДЭНЭ[1], Бат-Эрдэнийн МӨНХБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Мэдээллийн Сүлжээ, Аюулгүй Байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: khaliunaao758@gmail.com[1], munkhbayar.b@must.edu.mn[2]

Хураангуй: **Энэ судалгааны ажил нь и-мэйл spoofing халдлагын механизмыг судалж, одоо байгаа хамгаалалтын аргачлалуудын үр нөлөөг үнэлэх, шинэ хамгаалалтын стратеги судлахад чиглэгдэнэ. И-мэйл spoofing нь хуурамч илгээгчийн мэдээллийг ашиглан хэрэглэгчийг мэхлэх, залилангийн үйлдэл хийхэд ашиглагддаг бөгөөд кибер аюулгүй байдалд ноцтой эрсдэл учруулдаг. Судалгаанд SPF, DKIM, DMARC зэрэг баталгаажуулалтын аргачлалуудын үр нөлөөг шинжилж, эдгээрийн сул талуудыг тодорхойлсон. Судалгааны үр дүнд и-мэйл spoofing халдлагыг илрүүлэх, урьдчилан сэргийлэх шинэ аргачлалуудыг боловсруулах шаардлагатайг тогтоосон. Түүнчлэн, BIMI, DMARCBox зэрэг нэмэлт хамгаалалтын механизмын хэрэгжилтийг судалж, илүү найдвартай хамгаалалтын загвар боловсруулах боломжийг санал болгов. Энэхүү судалгааны ажлын хүрээнд и-мэйл spoofing халдлагын давтамж, тархалт, түгээмэл хэрэглэгддэг арга техникийг анализ хийж, одоогийн хамгаалалтын механизмуудын үр нөлөөг тодорхойлох, сайжруулсан хамгаалалтын шинэ аргачлал боловсруулах үндэслэлийг гаргасан. Судалгааны үр дүн нь кибер аюулгүй байдлын салбарт хувь нэмэр оруулж, и-мэйл системийн хамгаалалтыг сайжруулахад чиглэнэ.**

Түлхүүр үг: ***И-мэйл spoofing, Кибер аюулгүй байдал, И-мэйл аюулгүй байдлын протоколууд SPF, DKIM, DMARC, BIMI***

I. УДИРТГАЛ

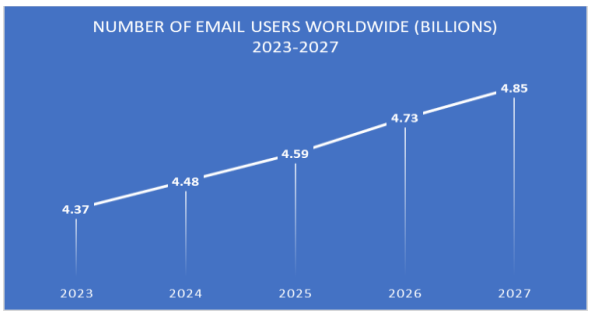
2024 оны байдлаар дэлхий даяар 4.48 тэрбум и-мэйл хэрэглэгч байгаа нь дэлхийн хүн амын талаас илүү хувийг (56.8%) эзэлж байна. Энэ тоо 2027 оны эцэс гэхэд 4.85 тэрбум гаруй болж өсөх төлөвтэй байна [1]. И-мэйлийн хэрэглээ нэмэгдэхийн хэрээр холбоотой халдлагуудын тоо ч мөн өссөөр байгаа бөгөөд өдөрт 3.1 тэрбум spoofing и-мэйл илгээгддэг [2]. И-мэйл статистикийг 1-р зурагт харуулав.

И-мэйл Spoofing[6] нь и-мэйл толгойг (header) хуурамчаар үйлдэж, бусдын и-мэйл хаягтай төстэй хуурамч хаяг ашиглан илгээх үйлдэл юм. Энэ төрлийн халдлага нь фишинг (phishing), спам (spam) болон бусад төрлийн халдлагуудын хамгийн түгээмэл арга техникүүдийн нэг бөгөөд олон тооны хохирогчдыг урьдчилан таамаглах боломжгүй эрсдэлд оруулдаг [3].

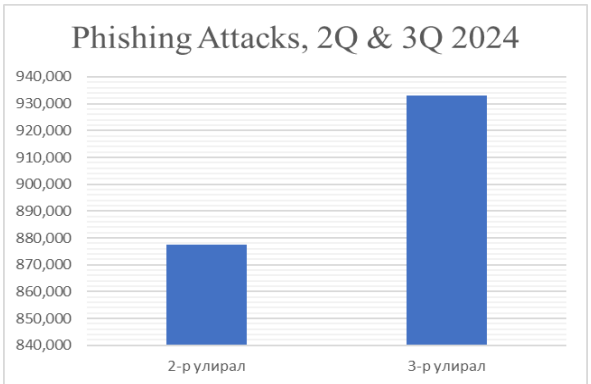
Anti Phishing Working Group (APWG)-ийн тайланд дурдсанаар, 2024 оны гуравдугаар улиралд 932,923 spoofing халдлагууд бүртгэгдсэн бөгөөд энэ нь хоёрдугаар улирлын 877,536 -тай харьцуулахад 6.31% -аар нэмэгдсэн үзүүлэлт юм [4]. График үзүүлэлтийг 2-р зурагт харуулав.

FBI-ийн Internet Crime Complaint Center (IC3)-ийн мэдээлснээр, 2020 онд зөвхөн Arizona мужид энэ төрлийн халдлагад 1,000 гаруй хүн хохирч, нийт 3 сая ам.долларын хохирол амссан байна. АНУ даяар эдгээр залилангийн хохирогчдын тоо 250,000 гаруй, учирсан хохирлын хэмжээ 260 сая ам.доллар хүрсэн байна [5].

И-мэйл spoofing болон phishing халдлагуудын давтамж хурдацтай өссөөр байгаа бөгөөд, хохирлын хэмжээ маш өндөр байгааг харуулж байна.



1-р зураг. ***Email Usage Statistics 2025. 2023-2027 он хүртэлх и-мэйл хэрэглэгчдийн өсөлт***



2-р зураг. ***Phishing халдлага, 2024 оны 2 болон 3-р улирлын phishing халдлагын үзүүлэлт***

II. СЭДЭВ СОНГОСОН ҮНДЭСЛЭЛ

И-мэйл нь дэлхий даяар харилцаа холбооны гол хэрэгсэл болж, олон байгууллага, хувь хүмүүсийн өдөр тутмын амьдралд зайлшгүй шаардлагатай ч, халдлагад өртөх эрсдэлтэй хэвээр байна. И-мэйл spoofing халдлагын тоо хурдацтай нэмэгдэж, мэдээллийн аюулгүй байдалд ноцтой эрсдэл учруулж байгаа нь энэ асуудлыг гүнзгийрүүлэн судлах шаардлагатайг харуулж байна.

A. Кибер аюулгүй байдлын тулгамдсан асуудал

И-мэйл нь мэдээлэл солилцох үндсэн хэрэгсэл болохын зэрэгцээ халдлагад өртөмтгий байна. И-мэйл spoofing нь хуурамч илгээгчийн мэдээллийг ашиглан хэрэглэгчийг мэхлэх, хуурамч мэдээ түгээх замаар хохирол учруулдаг. Үүний улмаас байгууллага, хувь хүнд санхүүгийн хохирол болон мэдээллийн алдагдал үүсэх эрсдэлтэй байдаг.

B. И-мэйл spoofing халдлагын өсөлт

Сүүлийн жилүүдэд и-мэйл spoofing халдлагын тоо нэмэгдэж, улам нарийн, өргөн хүрээтэй болж байна. Өнгөрсөн хугацаанд фишинг болон и-мэйл spoofing халдлага нь олон улсын хэмжээнд хамгийн түгээмэл кибер халдлагуудын нэг болоод байна. Тус төрлийн халдлага нь хэрэглэгчдийн хувийн мэдээлэл, санхүүгийн нууцлалд ноцтой аюул учруулж байна.

C. Одоогийн хамгаалалтын аргуудын сул тал

И-мэйл хамгаалалтын механизмууд, тухайлбал SPF, DKIM, DMARC зэрэг баталгаажуулалтын протоколууд нь spoofing халдлагаас бүрэн хамгаалж чадахгүй хэвээр байна. Эдгээр аргачлалууд нь хамгаалагдсан и-мэйл илгээгчийн хувьд үр дүнтэй ажиллах боловч халдагчид эдгээрийг тойрон гарах олон төрлийн арга техникийг ашиглаж, хамгаалалтын үр нөлөөг бууруулж байна.

D. Шинэ хамгаалалтын стратеги боловсруулах шаардлага

Одоогийн хамгаалалтын аргуудын сул талуудыг сайжруулж илүү үр дүнтэй шинэ аргачлалуудыг хөгжүүлэх шаардлага улам бүр нэмэгдэж байна. И-мэйл spoofing халдлагыг илрүүлэх, урьдчилан сэргийлэх дэвшилтэт арга хэмжээг хөгжүүлэх нь кибер аюулгүй байдлын салбарт чухал ач холбогдолтой.

E. Шинэ судалгааны чиглэлд хувь нэмэр оруулах

И-мэйл spoofing халдлагын талаар илүү гүнзгий судалгаа хийх нь кибер аюулгүй байдлын салбарт эрдэм шинжилгээний шинэ хандлага, шийдлийг нээх боломжийг олгоно. Энэхүү судалгаа нь кибер аюулгүй байдлын чиглэлээр суралцаж буй оюутан, судлаачдад шинэ мэдээлэл, судалгааны эх сурвалжийг бий болгох ач холбогдолтой болно.

III. ӨМНӨ СУДЛАГДСАН АЖИЛ

И-мэйл spoofing халдлага нь кибер аюулгүй байдлын тулгамдсан асуудал бөгөөд үүнээс хамгаалахын тулд олон төрлийн судалгаа, хамгаалалтын аргачлалууд хийгдэж ирсэн.

A. Судлагдсан ажлууд

1. End-to-End Measurements of Email Spoofing Attacks

Hu & Wang (2018) судалгаандаа SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting, and Conformance) зэрэг баталгаажуулалтын протоколуудын хэрэгжилт болон үр нөлөөг судалжээ [6].

Гэвч эдгээр аргачлалууд нь зөвхөн DNS тохиргоонд суурилсан тул хамгаалалт бүрэн хангалтгүй бөгөөд буруу тохиргооны улмаас хуурамч и-мэйлүүд дамжих магадлал өндөр хэвээр байна.

2. Composition Kills: A Case Study of Email Sender Authentication

Jianjun Chen ,Vern Paxson, Jian Jiang (2020) судалгаандаа SPF, DKIM, DMARC гэсэн и-мэйл баталгаажуулалтын протоколуудыг ашиглан и-мэйл spoofing халдлагыг хэрхэн бууруулах боломжийг судалсан байна [7]. Судалгаагаар эдгээр протоколуудын хэрэгжилт, тохиргооны алдаанууд, тэдгээрийн хоорондын харилцан үйлчлэл болон зөрчлүүдийг судалж, хуурамч и-мэйлүүдийг дамжуулах боломжийг хэрхэн нэмэгдүүлж болохыг илрүүлсэн байна.

3. Secure Email Transmission Protocols — A New Architecture Design

Gabriel Chen & Rick Wanner (2022) судалгаандаа SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting, and Conformance) протоколуудын хамтарсан ашиглалтын аюулгүй байдлын үр нөлөөг судалжээ [8]. Эдгээр аргачлалууд нь и-мэйл мессежийг илгээж байгаа домэйн болон түүний агуулгаас хамаарч баталгаажуулалтыг хийнэ. Гэвч судалгаагаар эдгээр аргачлалууд нь зөвхөн DNS тохиргоонд тулгуурладаг бөгөөд энэ нь буруу тохиргоо болон сүлжээний асуудлын улмаас хуурамч и-мэйлүүдийг урьдчилан сэргийлэхэд хүрдэггүй гэсэн дүгнэлтэд хүрсэн байна. Үүнээс гадна, эдгээр аргачлалууд нь мэйл серверийн дотоод тохиргооны алдаа болон хүний алдаанаас болж хамгаалалт сул дорой байж болохыг илрүүлсэн. Тиймээс илүү нарийвчилсан болон нээлттэй систем шаардлагатай байна гэж үзжээ.

Өмнө судлагдсан ажлуудад SPF, DKIM, DMARC зэрэг баталгаажуулалтын аргачлалууд нь spoofing халдлагыг тодорхой хэмжээнд бууруулж байгаа боловч 100% найдвартай хамгаалалт болж чадахгүй байгаа нь судалгаагаар батлагдсан [6,7,8].

Тиймээс, илүү үр дүнтэй хамгаалалтын аргачлалууд боловсруулах шаардлага гарч байна.

B. Судалгааны хувь нэмэр

И-мэйл spoofing халдлагын эсрэг хамгаалалтын шинэ аргачлалуудыг боловсруулах, одоо байгаа SPF, DKIM, DMARC зэрэг баталгаажуулалтын механизмуудын үр дүнтэй байдлыг нэмэгдүүлэхэд

1. И-мэйл spoofing халдлагын сүүлийн үеийн судалгаа, дүн шинжилгээ хийх

a) И-мэйл **spoofing** халдлагын давтамж, төрөл, түгээмэл арга техникийг судалж, бодит кейсүүдэд суурилсан анализ хийх.

b) Өнгөрсөн жилүүдийн халдлагын өгөгдөлд суурилсан статистик судалгаа гаргах.

2. Одоо байгаа хамгаалалтын аргуудын сул талыг тодорхойлох

a) SPF, DKIM, DMARC зэрэг баталгаажуулалтын аргачлалуудын онолын болон практик хэрэглээний хязгаарлалтыг тодорхойлох.

b) Эдгээр хамгаалалтын аргачлалуудыг хэрхэн тойрон гарах боломжтойг анализ хийх.

3. Шинэ хамгаалалтын стратеги, аргачлалыг боловсруулах

a) Одоогийн хамгаалалтын сул талыг нөхөх нэмэлт хамгаалалтын механизм боловсруулах.

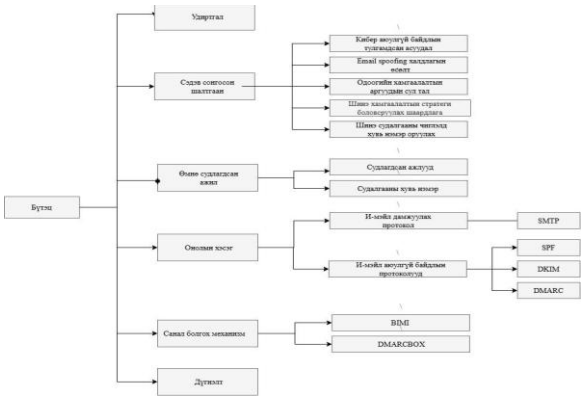
b) Машин сургалт болон хиймэл оюун ухааны аргуудыг ашиглан и-мэйл spoofing халдлагыг илрүүлэх шинэ алгоритм санал болгох.

4. Практик туршилт, үнэлгээ хийх

a) Шинэ аргачлалуудыг бодит орчинд туршиж, үр дүнг харьцуулан шинжлэх.

b) Хамгаалалтын шинэ аргачлалуудын үр нөлөөг SPF, DKIM, DMARC-ийн гүйцэтгэлтэй харьцуулж үнэлэх.

Энэхүү судалгааны ажлын үр дүнд и-мэйл spoofing халдлагын эсрэг илүү үр дүнтэй ажиллах шинэ техникүүдийг ашиглан и-мэйл spoofing халдлагыг илрүүлэх, урьдчилан сэргийлэх аргачлалыг боловсруулах боломжийг нэмэгдүүлж, байгууллага болон хэрэглэгчдэд илүү найдвартай хамгаалалтын шийдэл санал болгоно.



3-р зураг. Судалгааны ажлын бүтцийн схем

IV. ОНОЛЫН ХЭСЭГ

И-мэйл систем нь дамжуулах болон хамгаалах гэсэн хоёр үндсэн чиглэлийн протоколууд дээр суурилдаг. Дамжуулах протоколууд нь и-мэйлийг серверүүдийн хооронд найдвартай дамжуулах үүрэгтэй байдаг бол хамгаалах протоколууд нь и-мэйлийн эх сурвалж, бүрэн бүтэн байдал, найдвартай байдлыг баталгаажуулдаг.

A. И-мэйлийг Дамжуулах Протокол

SMTP (Simple Mail Transfer Protocol) нь и-мэйл мессежийг илгээгчээс хүлээн авагч руу дамжуулах, хүргэх зориулалттай интернэтийн стандарт протокол юм. Энэхүү протокол нь клиент-сервер архитектур дээр суурилж, и-мэйл дамжуулах үйл явцыг зохицуулдаг. SMTP нь 587 (STARTTLS), 465 (SSL/TLS) зэрэг портуудыг ашиглан шифрлэгдсэн холболтоор аюулгүй байдлыг хангадаг. Протоколын үндсэн үүрэг нь и-мэйлийг илгээгчийн серверээс хүлээн авагчийн сервер рүү дамжуулж, улмаар хүлээн авагчийн шуудангийн хайрцагт хүргэх явдал юм[4].

B. И-мэйлийн Аюулгүй Байдлын Протоколууд

1. SPF (Sender Policy Framework) нь и-мэйл илгээх эрх бүхий серверүүдийг тодорхойлох, улмаар илгээгчийн нэрийг ашиглан гүйцэтгэх spoofing, phishing зэрэг халдлагаас урьдчилан сэргийлэх зорилготой баталгаажуулах протокол юм. Энэхүү протокол нь DNS TXT бичлэг дээр суурилж, тухайн домэйнээс зөвшөөрөгдсөн SMTP серверүүдийг тодорхойлох механизмыг ашигладаг[3].

2. DKIM (DomainKeys Identified Mail) нь асимметрик шифрлэлтийн алгоритм дээр суурилсан и-мэйлийн эх сурвалж ба бүрэн бүтэн байдлыг баталгаажуулах криптографийн хамгаалалтын механизм юм. Энэхүү протокол нь илгээгч сервер и-мэйлийн толгойд дижитал гарын үсэг нэмж, хүлээн авагч сервер уг гарын үсгийг баталгаажуулснаар и-мэйлийн хуурамч, өөрчлөгдсөн эсэхийг тодорхойлох боломжтой. DKIM-ийг SPF болон DMARC-тэй хослуулснаар и-мэйлийн хуурамч эх сурвалжаас хамгаалах, халдлагын эсрэг найдвартай байдал нэмэгдүүлэх, өгөгдлийн бүрэн бүтэн байдлыг хадгалах зэрэг давуу талуудыг бүрдүүлнэ[3].

3. DMARC (Domain-based Message Authentication, Reporting & Conformance) нь SPF болон DKIM баталгаажуулалтын үр дүнд үндэслэн и-мэйлийн бодит эх сурвалжийг тогтоох, spoofing, phishing халдлагаас урьдчилан сэргийлэх зориулалттай баталгаажуулах протокол юм. DMARC нь DNS TXT бичлэг дээр суурилдаг бөгөөд и-мэйлийг хэрхэн хүлээн авах, боловсруулах бодлогыг тодорхойлох боломжийг домэйний эзэмшигчид олгодог[3].

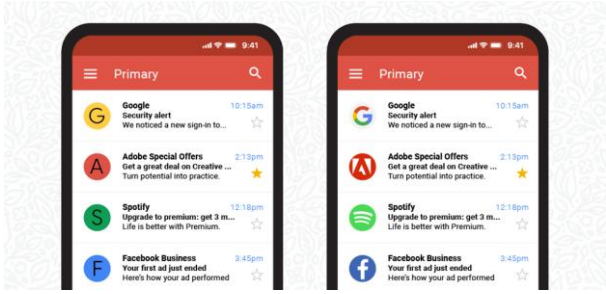
V. САНАЛ БОЛГОХ МЕХАНИЗМ

И-мэйл дамжуулах үндсэн архитектур дах эмзэг сул талууд дээр тулгуурлан цахим шуудангийн архитектурыг илүү сайн зохион байгуулах хэд хэдэн арга механизмуудыг санал болгож байна.

A. BIMI механизм

Фишинг и-мэйлийн хор хөнөөлийг бууруулах үр дүнтэй арга замуудын нэг болох DNS суурьтай и-мэйл аюулгүй байдлын механизмууд, тухайлбал Sender Policy Framework (SPF), Domain Based Message Authentication Reporting and Conformance (DMARC), болон DNS-Based Authentication of Named Entities (DANE) зэрэг нь санал болгогдож, өргөнөөр хэрэглэгдэж байна. Гэсэн хэдий ч фишинг и-мэйлийн хохирогчдын тоо нэмэгдсээр байгаа нь хэрэглэгчдэд ийм төрлийн и-мэйлийг жинхэнэ и-мэйлээс зөв ялгах боломжийг дэмжих механизм шаардлагатай байгааг харуулж байна.

BIMI (Brand Indicators for Message Identification) нь хэрэглэгчдэд баталгаажсан брэндийн логотой и-мэйлийг танилцуулдаг. Энэ нь и-мэйлийг хүлээн авагчид тухайн илгээгчийн үнэн зөв эсэхийг харааны түвшинд ялгаж таних боломж олгодог тул и-мэйлийн гарчиг эсвэл агуулгыг нарийн шалгах шаардлагагүй болгодог. Google компани 2021 оны 7-р сард BIMI-ийг албан ёсоор дэмжсэнээс хойш энэ технологи улам бүр түгж байна[11].



4-р зураг. BIMI тохируулаагүй болон BIMI тохируулсан inbox харагдах байдал

BIMI-г хэрэгжүүлэхийн тулд дараах шаардлагуудыг хангах хэрэгтэй:

- DMARC бодлого: Байгууллага нь DMARC (Domain-based Message Authentication, Reporting & Conformance) протоколыг "quarantine" эсвэл "reject" бодлоготойгоор тохируулсан байх шаардлагатай.
- Логоны формат: Брэндийн лого нь SVG Tiny P/S форматаар, тэгш өнцөгт (square) хэлбэртэй байх ёстой.
- DNS TXT бичлэг: Домэйн нэрийн DNS тохиргоонд BIMI-г зааж өгөх TXT бичлэг нэмэх шаардлагатай. Энэ бичлэгт логоны байршлыг заасан URI-г оруулна.
- VMC (Verified Mark Certificate): Зарим и-мэйл үйлчилгээ үзүүлэгчид, тухайлбал Gmail, лого харуулахын тулд баталгаажсан тэмдгийн сертификат (VMC) шаарддаг.

BIMI бичлэг: BIMI-ийг домэйн нэр дээр идэвхжүүлэхийн тулд тухайн домэйний MX серверийн DNS TXT бичлэгт дараах өгөгдлийг нэмэх шаардлагатай:

v=BIMI1;l=<логоны холбоос>;a=<VMC холбоос>,

Энд: logo link нь брэндийн логоны холбоосыг заана харин vmc link нь баталгаажсан VMC-ийн холбоосыг заана. https протоколыг заавал ашиглах шаардлагатай.

Лого зураг: BIMI-д ашиглагдах брэндийн лого нь RFC 6170-д тодорхойлсон SVG файлын форматаар байх ёстой. Одоогоор SVG Tiny P/S нь интернэтийн стандарт болгохоор санал болгогдож байгаа бөгөөд дараах шаардлагуудыг агуулдаг:

- title tag заавал байх шаардлагатай (64 тэмдэгтээс бага байхыг зөвлөдөг). svg tag-д дараах шинж чанарууд заавал тохируулагдсан байх ёстой:
- *xmlns="http://www.w3.org/2000/svg"*
- *version="1.2"*
- *baseProfile="tiny-ps"*
- desc tag оруулахыг зөвлөж байна.
- Логоны файлын хэмжээ 32 KB-аас бага байхыг зөвлөдөг.

VMC (Verified Mark Certificate): VMC нь брэндийн логог баталгаажуулах зориулалттай дижитал гэрчилгээ юм. Одоогоор DigiCert болон Entrust байгууллагууд нь VMC-г олгох эрхтэй сертификат олгогч байгууллагууд (CAs) юм.

VMC авахын тулд байгууллага нь дараах алхмуудыг дагана:

1. Өөрийн брэндийн логог холбогдох гэрчилгээжүүлэгч байгууллагад бүртгүүлэх.
2. Байгууллагын үнэн зөвийг нотлох баримт бичгүүдийг бүрдүүлэх.
3. Гэрчилгээжүүлэгч байгууллагын шалгалт, видео баталгаажуулалтад хамрагдах.
4. Хэрэв бүх шаардлага хангасан бол VMC гэрчилгээ олгогдоно.

2024 оны байдлаар BIMI-г дэмжиж буй и-мэйлийн үйлчилгээ үзүүлэгчид:

BIMI-г дэмждэг үйлчилгээ үзүүлэгчид	BIMI-г хэрэгжүүлэхийг судалж буй үйлчилгээ үзүүлэгчид	BIMI-г дэмждэггүй үйлчилгээ үзүүлэгчид

CLOUDMARK	BT	
Fastmail	COMCAST	
Google	QUALITIA	
LA POSTE	GMX	
onet POCZTA		
yahoo!		
ZONE		

5-р зураг. BIMI-г дэмжиж буй и-мэйлийн үйлчилгээ үзүүлэгчид

Гэсэн хэдий ч бусад аюулгүй байдлын механизмуудтай адил BIMI нь өөрийн гэсэн сул талтай. Жишээлбэл, DMARC бодлого шаардлагатай учраас "quarantine" эсвэл "reject" бодлоготой байх ёстой тул зарим байгууллагууд одоогийн тохиргоогоо өөрчлөх шаардлагатай болно. Мөн VMC авах зардал өндөр бөгөөд одоогоор зөвхөн DigiCert, Entrust компаниуд олгодог.

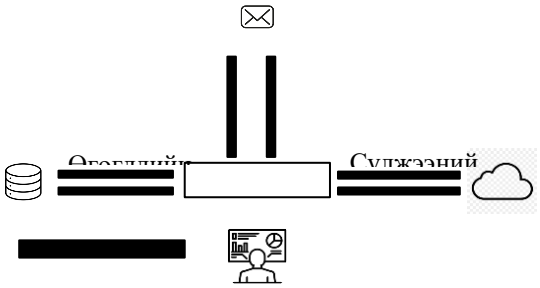
B. DMARCBox

И-мэйл spoofing халдлага нь олон жилийн турш и-мэйлийн аюулгүй байдлын гол сэдэв байсан. SMTP дээр spoofing халдлагын эсрэг ямар ч сэргийлэлт байхгүй тул SPF болон DKIM-г боловсруулсан. Аюулгүй байдлын механизмыг сайжруулж spoofing халдлагаас сэргийлэх зорилгоор SPF болон DKIM дээр DMARC-г бий болгосон[12].

Гэсэн хэдий ч илүү сайн сэргийлэлт механизмыг бий болгохын тулд илүү сайн илрүүлэлтийн арга хэрэгсэл хэрэгтэй. Халдлагад өртсөн и-мэйлүүдийг аль болох хурдан илрүүлж хариу үйлдэл үзүүлэхийн тулд сайн шинжилгээний хэрэгсэл хэрэгтэй. Одоогоор хамгийн алдартай арга бол спам шүүлтүүрийн логик (spam filter logic) юм. Арга техникүүдэд ангилал, төрөлжүүлэл, профайл хийх (машин сургалт), нарийвчлалтай шүүх зэрэг багтана.

Байгууллагын и-мэйлийг хуурамчаас ялгах боломжийг нэмэгдүүлдэг ч хэрэглээ нь хязгаарлагдмал байна. DMARCBox нь DMARC бодлогын хэрэгжилтийг сайжруулж, халдлагыг

DMARCBox нь дамжуулалтын үеэр халдлагад өртсөн и-мэйлүүдийг шинжилж илрүүлэх зорилгоор бүтээгдсэн. Энэ нь DMARC протоколыг ашиглан Reporting URIs for Aggregate Date (RUA) болон Reporting URIs for Failure (RUF) бүртгэлийг авах бөгөөд дараа нь и-мэйлүүдийн шинжилгээнд үндэслэн уншихад хялбар тайланг өгдөг. Энэ нь тусгай серверт эсвэл үүлэн орчинд хөгжүүлж болно. DMARCBox-ийн ерөнхий ажиллах зарчмыг Зураг 5-т харуулав.



6-р зураг. DMARCBox ажиллах зарчим

DMARC нь SPF болон DKIM дээр бүтээгдсэн тул DMARCBox нь и-мэйлүүдийг ангилахад SPF болон DKIM-ийн протоколын дэлгэрэнгүй мэдээллийг ашиглаж чадна. DMARCBox нь RUA болон RUF дээр үндэслэн долоон өөр ангилал санал болгодог бөгөөд эдгээр ангилалд үндэслэн нэмэлт хариу үйлдлийн протоколуудыг бий болгох боломжтой.

Спам хавтасны эмзэг тал нь и-мэйлүүдийг аль хэдийн хүргэгдсэний дараа шинжилдэг бөгөөд энэ нь хэрэглэгчийн спам хавтсыг хялбархан нээж, хуурамч и-мэйлд өртөх боломжийг ихээхэн нэмэгдүүлдэг. Хохиролтой и-мэйл илрүүлэх илүү сайн механизмыг бий болгохын тулд бид и-мэйлүүдийг дамжуулалтын үед шинжилж, тэдний шуудангийн хайрцагт очихоос өмнө хариу үйлдэл үзүүлэх хэрэгтэй.

ДҮГНЭЛТ

И-мэйл spoofing халдлагын эрсдэл өндөр хэвээр байгааг тогтоож, хамгаалалтын одоогийн арга хэмжээнүүдийн үр нөлөө болон сул талуудыг тодорхойллоо. SPF, DKIM, DMARC зэрэг баталгаажуулалтын аргууд нь халдлагыг тодорхой хэмжээнд хязгаарлах боловч бүрэн хамгаалалт хангахгүй байгааг онцолсон.

BIMI болон DMARCBox гэсэн нэмэлт хамгаалалтын шийдлүүдийн тухай судлан тэдгээрийг өргөн хүрээнд хэрэгжүүлэхэд техникийн болон бодлогын түвшинд тодорхой бэрхшээлүүд байгааг илрүүллээ. BIMI нь

илрүүлэх үр дүнг нэмэгдүүлж буй ч бүх байгууллагад нэвтрээгүй байна. Цаашид BIMI болон DMARCBox-ийн хэрэгжилтийг сайжруулах, олон

давхар хамгаалалтын механизмуудыг хослуулах шаардлагатай юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Email tooltester: Email Usage Statistics 2025. [Online] https://www.emailtooltester.com/en/blog/email-usage-statistics/. Accessed 2025-02-20.

[2] Sibi Chakkaravarthy, S., Devi Priya, V. S., Tarun Reddi, M. S. T. R., & Khan, M. K. A Comprehensive Examination of Email Spoofing: Issues and Prospects for Email Security.

[3] Ma, J., Chen, L., Xue, K., Luo, B., Huang, X., Ai, M., ... & Zhuang, Y. (2024). {FakeBehalf}: Imperceptible Email Spoofing Attacks against the Delegation Mechanism in Email Systems. In *33rd USENIX Security Symposium (USENIX Security 24)* (pp. 1243-1260).

[4] APWG. APWG:Report Phishing. [Online]. https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf. Accessed: 2025-02-20.

[5] FBI Phoenix: Phishing and Spoofing scams. [Online]. https://www.fbi.gov/video-repository/phoenix-tech-june2021.mp4/view Accessed: 2025-02-27

[6] Hu, H., & Wang, G. (2018). {End-to-End} measurements of email spoofing attacks. In *27th USENIX Security Symposium (USENIX Security 18)* (pp. 1095-1112).

[7] Chen, J., Paxson, V., & Jiang, J. (2020). Composition kills: A case study of email sender authentication. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 2183-2199).

[8] Chen, G., & Wanner, R. (2022). Secure Email Transmission Protocols--A New Architecture Design. *arXiv preprint arXiv:2208.00388*.

[9] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[10] Eason, G., Noble, B., & Sneddon, I. N. (1955). On certain integrals of Lipschitz-Hankel type involving products of Bessel functions. Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences, 247(935), 529-551.

[11] Yajima, M., Chiba, D., Yoneya, Y., & Mori, T. (2023, March). A first look at brand indicators for message identification (BIMI). In *International Conference on Passive and Active Network Measurement* (pp. 479-495). Cham: Springer Nature Switzerland.

[12] Chen, G., & Wanner, R. (2022). Secure Email Transmission Protocols--A New Architecture Design. *arXiv preprint arXiv:2208.00388*.

[13] Altulaihan, E., Alismail, A., Hafizur Rahman, M. M., & Ibrahim, A. A. (2023). Email security issues, tools, and techniques used in investigation. *Sustainability*, *15*(13), 10612.

[14] Shen, K., Wang, C., Guo, M., Zheng, X., Lu, C., Liu, B., ... & Yang, M. (2021). Weak links in authentication chains: A large-scale analysis of email sender spoofing attacks. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 3201-3217).

[15] Chhabra, G. S., & Bajwa, D. S. (2015). Review of e-mail system, security protocols and email forensics. *International Journal of Computer Science & Communication Networks*, *5*(3), 201-211

[16] Ashiq, M. I., Li, W., Fiebig, T., & Chung, T. (2023). You've Got Report: Measurement and Security Implications of {DMARC} Reporting. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4123-4137).

[17] Tatang, D., Zettl, F., & Holz, T. (2021, October). The evolution of dns-based email authentication: Measuring adoption and finding flaws. In *Proceedings of the 24th International Symposium on Research in Attacks, Intrusions and Defenses* (pp. 354-369).

[18] Maroofi, S., Korczynski, M., & Duda, A. (2020). From Defensive Registration to Subdomain Protection: Evaluation of Email Anti-Spoofing Schemes for High-Profile Domains. In *TMA* (pp. 1-9).

[19] Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing email detection using natural language processing techniques: a literature survey. *Procedia Computer Science*, *189*, 19-28.

[20] Gao, X., & Zhang, E. Z. (2023, September). Key Generation and Identity Verification using Quantum Teleportation. In *Proceedings of the 1st Workshop on Quantum Networks and Distributed Quantum Computing* (pp. 62-66).

[21] Hu, H., & Wang, G. (2018). Revisiting email spoofing attacks. *arXiv preprint arXiv:1801.00853*.

КАРГО ТЭЭВРИЙН БИЧГЭЭС МЭДЭЭЛЭЛ ГАРГАН АВАХ УХААЛАГ СИСТЕМ

Мөнхбаяр ТҮМЭН-АЮУШ[1], Чулуунжин МИЧИДГОО[1], Сүхбаатар БАТМӨНХ[1], Соном-Очир ӨЛЗИЙБАЯР[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: B210930048@must.edu.mn[1], ulziibayar@must.edu.mn[2]

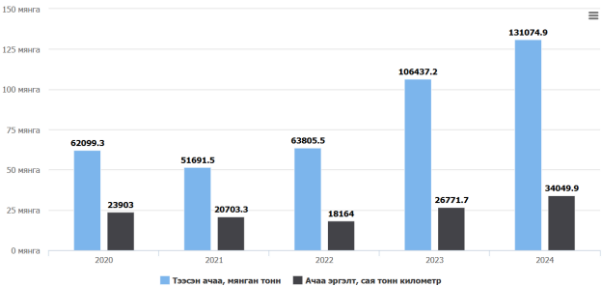
Хураангуй: **Монгол Улсад 60-80 гаруй карго үйлчилгээний байгууллага гадаадын улс орнуудаас бараа, бүтээгдэхүүн импортлон хэрэглэгчдэд хүргэж байна. Гэвч эдгээр үйлчилгээний явцад олон ажлыг гар аргаар гүйцэтгэж байгаагаас шалтгаалан хүн хүч, цаг хугацаа, санхүүгийн зардал нэмэгдэж, хэрэглэгчийн сэтгэл ханамжид сөрөг нөлөө үзүүлж байна. Энэхүү судалгаагаар карго үйлчилгээ эрхлэгчдэд зориулан объект таних моделийг ашиглан автоматжуулсан системийг хөгжүүлсэн бөгөөд уг систем нь барааны шошгоос хэрэглэгчийн дугаар, барааны код, бусад текст мэдээллийг өндөр нарийвчлалтай таних боломжтой юм. Судалгааны хүрээнд боловсруулсан систем нь шошго таних болон дугаар таних гэсэн хоёр үндсэн модультай. Шошго таних модульд анхны өгөгдөлд урьдчилсан боловсруулалт (preprocessing) хийж, дугаар таних модульд өгөгдөл нэмэгдүүлэх (data augmentation) аргыг ашиглан сургалтыг сайжруулсан. Үүний үр дүнд манай систем нь 97%-ийн нарийвчлалтайгаар дугаарыг таньж, олон төрлийн форматын бичилтийг ялгах чадвартай болсон. Систем нь аль ч улсын, ямар ч үйлдвэрийн барааны шошго дээр ажиллах боломжтой тул өргөн хэрэглээнд нэвтрүүлэх боломжтой юм. Энэхүү автоматжуулсан шийдэл нь карго үйлчилгээний менежментийг сайжруулах, хүний оролцоог багасгах, мэдээлэл боловсруулах үйл явцыг оновчтой болгох ач холбогдолтой. Логистикийн үйл ажиллагаанд гар ажиллагааг бууруулснаар алдаа багасаж, мэдээллийн найдвартай байдал нэмэгдэнэ. Судалгааны үр дүнгээс харахад боловсруулсан систем нь бодит нөхцөлд найдвартай, хялбар ажиллагаатай болох нь батлагдсан бөгөөд карго үйлчилгээний менежментийг улам хөгжүүлэх, өгөгдөлд суурилсан логистикийн шийдлийг нэвтрүүлэх чиглэлд цаашид ажиллахаар зорьж байна. Мөн энэхүү систем нь тээврийн зардлыг бууруулах, үйлчилгээний хурдыг нэмэгдүүлэх, хэрэглэгчийн мэдээллийг илүү найдвартай таних, хадгалах зэрэг олон давуу талтай. Урт хугацааны судалгаа, хөгжүүлэлтийн дараа системийг бодит орчинд туршиж, алдааны түвшин тодорхойлсон. Цаашид машин сургалтын аргыг ашиглан модулиудыг сайжруулж, бусад технологитой хослуулах замаар автоматжуулалтын түвшин нэмэгдүүлэх боломжтой. Энэхүү судалгаа нь карго үйлчилгээний салбарт технологийн дэвшлийг нэвтрүүлэх чухал алхам болж буйг харуулж байгаа бөгөөд системийн гүйцэтгэлийг улам сайжруулж, бодит орчинд илүү оновчтой ажиллах нөхцөлийг бүрдүүлэх шаардлагатай гэж үзэж байна.**

Түлхүүр үг —карго систем, шошго танилт, дугаар танилт, YOLOv8, OCR

I. УДИРТГАЛ

Карго үйлчилгээний систем гэдэг нь ачаа тээвэрлэлтийг үр ашигтай зохицуулах зорилготой ложистик, тээврийн удирдлагын систем юм. Энэ нь агаарын, далай, төмөр зам, авто зам гэх мэт өөр өөр тээврийн төрлөөр ачааг хянах, хадгалах, түгээх зэрэг төрөл бүрийн бүрэлдэхүүн хэсгүүдийг агуулдаг. Орчин үеийн дэлхийн нийлүүлэлтийн сүлжээнд ачаа тээврийн систем нь бараг үр ашигтай, найдвартай тээвэрлэх, түгээхэд чухал үүрэг гүйцэтгэдэг. Тус систем нь бизнес эрхлэгчид болон хэрэглэгчдэд тээвэрлэлтийг бодит хугацаанд хянах боломжийг олгож, саатал, бараагаа алдах, буруу хаяг, мэдээлэлтэй байх зэрэг менежменттэй холбоотой эрсдэлийг бууруулдаг. Ачааны хяналтын системүүд нь бар код, RFID (Radio Frequency Identification) эсвэл GPS-д суурилсан хяналтад тулгуурлан янз бүрийн цэгүүд дээр ачааг таньж, хянаж байдаг. Гэсэн хэдий ч эдгээр аргуудын ихэнх нь гар аргаар, хөндлөнгийн хүний ихээхэн хэмжээний оролцоо шаарддаг бөгөөд энэ нь үр ашиггүй байдал, алдаа, үйл ажиллагааны зардал нэмэгдэхэд хүргэдэг.

Одоогийн байдлаар Монгол Улсад ойролцоогоор 60-80 гаруй карго[15] үйлчилгээ үзүүлдэг бизнес эрхлэгч байгаа ба яг баттай тоо баримт үүнээс ч их байж магадгүй байна. Гэхдээ бид дараах тоо баримтаас харвал [1] хэр их бараа бүтээгдэхүүн импортоор орж ирдэг нь харагдаж байна. Энэ нь нөгөө талаараа их хэмжээний карго үйлчилгээ үзүүлэгч болон карго систем өндөр шаардлагатай болохыг харуулж байгаа юм.



1-р зураг. Ачаа тээврийн тоо баримт

Технологи хөгжихийн хэрээр ачаа тээврийн систем хөгжиж, машин сургалт болон дүрсийн боловсруулалтад суурилсан объект таних системийг хөгжүүлсээр байна. Ялангуяа объект таних модель нь зураг дээрх объектуудыг хурдан бөгөөд үнэн зөв таних чадвараараа автоматжуулсан хяналтад ихээхэн хэрэглээ өндөртэй болсон.

Манай карго үйлчилгээний систем нь гараар сканнердах, хэрэглэгчийн дугаар, барааны код, шаардлагатай дугаарыг хүний оролцоотой таних, системд оруулах явдлыг халж, нарийвчлалыг сайжруулж, процессыг хурдан боловсруулах замаар логистикийн менежментийг сайжруулах зорилготой юм. Систем нь барааны шошгоос танилт хийж, гаргаж авснаар ачааг таних үйлдлийг хялбарчилж, хүний алдааг багасгаж, ерөнхий үр ашгийг оновчтой болгож чадна.

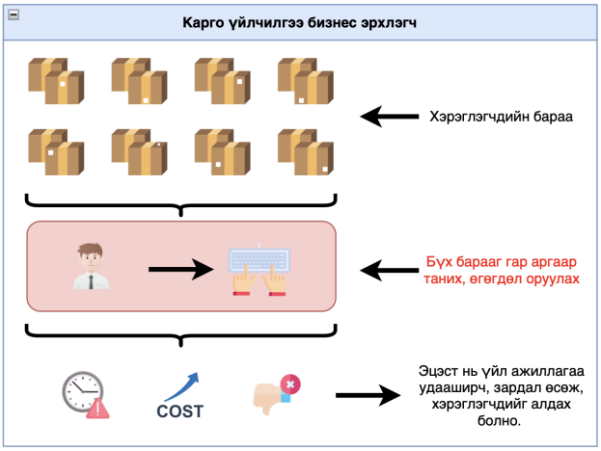
Энэхүү судалгаанд хэд хэдэн объект, текст таних моделийг туршиж өндөр нарийвчлалтай модельд суурилан ачаа тээврийн одоогийн системийн хэрэгжилт дээр нарийвчилсан дүн шинжилгээ хийж, үйл ажиллагаанд нэмэн ашиглаж болох боломж, сайжруулах шийдлүүдийг онцлон харуулсан болно.

Монгол улсад 60-аас 80 гаруй бие даасан карго үйлчилгээний газар нэгдсэн платформгүйгээр ажилладаг. Үүн дээр жижиглэн карго үйлчилгээ эрхэлдэг тоо баримт багтаагүй байгаа нь энэ тоо өсөх магадлалтай. Эдгээрийг нэгтгэх хэрэгцээ шаардлага байгаа ба хэрэглээнд нэвтрүүлэх боломж ч бүрэн байгаа гэж үзсэн.

2-р зураг. Одоогийн карго үйлчилгээний газар

Барааны шошго дээрх өгөгдлийг гараар шалгадаг бөгөөд энэ нь алдаа гарахад хүргэдэг [10]. Энэхүү судалгаанд барааны шошготой хэсгийг хурдан бөгөөд өндөр нарийвчлалтайгаар таних машин сургалт, дүрсийн боловсруулалтад суурилсан шийдлийг гүйцэтгэсэн. Энэхүү системийн эхний бөгөөд чухал үе шатуудын нэг бол барааны шошготой хэсгийг зөв тодорхойлох явдал юм. Энэ үе шатыг амжилттай гүйцэтгэх нь дараагийн процессуудыг амжилттай хэрэгжүүлэхэд чухал ач холбогдолтой.

Манай системийн гол зорилго нь хэрэглэгчийн захиалсан ачаа болон барааг ялгах, таних, хуваарилах явдал юм. Энэ хүрээнд дүрсийн боловсруулалтын технологийг ашиглан барааны шошгоос танилт хийж, дугаарыг автоматаар гарган, хүний оролцоог багасгаж, үйл явцыг хөнгөвчлөхийг зорьж байна.



3-р зураг. Одоогийн карго үйлчилгээний асуудал

Тус код нь үйлдвэрлэгч бүрээс хамааран өвөрмөц бөгөөд давтагдашгүй байдаг. Тиймээс зөв таних, ялгах нь хүний хөдөлмөр, цаг хугацаа ихээхэн шаарддаг. Ачаа тээврийн системүүд нь барааны шошгыг уншиж, тээвэрлэлтийг үр дүнтэй зохион байгуулахын тулд автомат таних технологиудыг ашигладаг. Эдгээр технологид RFID (Radio Frequency Identification), зураасан код (barcodes), QR код зэрэг нь өргөн ашиглагддаг. Судалгааны ажлын хүрээнд боловсруулж буй систем нь машин сургалт болон дүрс боловсруулалтын дэвшилтэт аргачлалуудыг агуулж, одоогийн байгаа системээс гар ажиллагааг халж илүү сайжруулах боломжтой.

II. СУДЛАГДСАН БАЙДАЛ

Манай системтэй төстэй одоогийн олон улсын техник технологийн шийдлийг судалж үзсэн. Үүнд техник хангамж болон программ хангамж дээр ялгаатай байдлаар шийдлийг багтаана судалсан. Үүнтэй холбоотой судалгаануудыг шинжилж, өөрсдийн системд нэвтрүүлэхээр тусгасан.

Ачаа барааны мэдээллийг хэд хэдэн аргаар шошго дээр тусгаж өгдөг. Үүнд :

Өгөгдлийг хадгалах, дамжуулах аргуудын нэг болох хэмжээст болон хоёр хэмжээст код нь ложистикийн хяналт, бараа материалын менежмент, барааны баталгаажуулалт зэрэг үйл явцыг хялбаршуулж, олон салбарт үр ашигтай шийдэл болж байна [5].

A. Судалгааны ажил

Өмнөх судалгааны ажлуудын нэг [13] болох "Multi-Directional Text Detection" нь янз бүрийн, олон талт чиглэлийн зургаас текстийг таньж, нарийвчлалыг сайжруулах зорилготой байсан.

- Sliding Vertex Box буюу хэвтээ эсвэл эргүүлсэн бол энэ нь текст таних дөрвөн өнцөгт хайрцгийг тодорхойлж, өнцгийн хил хязгаар болон оройн эрэмбийн алдааг багасгадаг.
- MD-Closs Loss Function нь CIOU (Complete IoU) дээр суурилсан бол алдагдлын функц нь олон чиглэлтэй текст таних нарийвчлалыг сайжруулдаг.
- Энэхүү судалгааны ажлаас манай баг нь далийсан, тэгш бус өгөгдлийг танихын тулд одоогийн моделийг хэрхэн сайжруулж болох санаа, аргачлаас санаа авсан.

4-р зураг. Судалгаа 2 тэгш бус өгөгдөл танилт

B. Судалгааны ажил

Энэхүү судалгаанд [14] автоматжуулсан контейнерын ID болон ISO кодыг танихын тулд гүн сургалтын аргыг ашиглан гар аргаар бичлэг хийх явцад гарах алдааг багасгах зорилготой байсан. Доор судалгааны ажлын онцлогийг үзүүлэв

- Контейнер таних, текст(ID болон ISO код) агуулсан текстийн хэсгийг задалдаг. Үүний дараа таньсан текст доторх тэмдэгтүүдийг олсон.
- Объект таних, ангилахад хамгийн сүүлийн үеийн мэдрэлийн сүлжээг ашигласан.
- Систем нь текст болон тэмдэгтийг танихад гарах алдааг багасгахын зэрэгцээ өндөр нарийвчлалтай болгосон.

Тус судалгаагаар RetinaNet буюу объект таних, үүнийг контейнер болон тэмдэгтүүдийг танихын тулд ашигласан. RetinaNet нь классын тэнцвэргүй байдлыг зохицуулахын тулд FPN болон фокусын алдагдлыг ашиглан хурд, нарийвчлалыг тэнцвэржүүлсэн байна.

Харин техник хангамжийг ашигласан шийдэл баркод дээр RFID ашигласан байна. Дээрх шийдлүүд нь сүүлийн үед дэлхийд ашиглагдаж буй арга бөгөөд программ хангамжид объект таних технологи, техник хангамжид баркод дээр RFID ашиглаж байна.

Одоогийн байгаа карго үйлчилгээний систем нь объект таних технологийг ашиглаж хийгдэж байгаа боловч Монгол улсад энэ байдал гар ажилгаагаар явагдаж байна. Мөн энэ объект таних технологийг ашиглаж хийгдэж байгаа шийдлийн судалгаа хомс байна.

1-Р ХҮСНЭГТ. СУДАЛГААНЫ АЖЛУУДЫН ХАРЬЦУУЛАЛТ

Судалгааны ажил	Модель	Үзүүлэлт
[A]	❖ YOL0v ❖ Models for Comparison (R2CNN, SegLink, PixeLink)	❖ Recall rate = 81.9% ❖ Precision = 86.2%
[B]	❖ RetinaNet ❖ Semantic Segmentation ❖ Custom CNN	❖ Текст таних алдаа хувь = 1% - ээс бага ❖ Custom CNN = 99% precision

III. ТӨСЛИЙН ХЭСЭГ

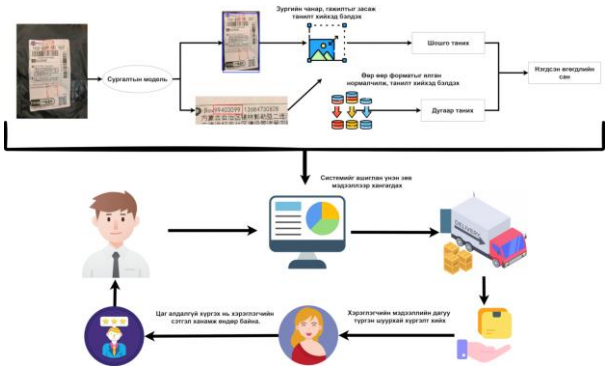
Төслийн эхний үе шатанд карго үйлчилгээний системийг сайжруулах зорилгоор шошго таних модуль, үүний дараа зорилтот дугаар буюу ачааны дугаар, каргоны дугаар, утасны дугаарыг таних модулийг хөгжүүллээ. Энэ систем нь ачаа

бараанаас шошгыг автоматаар таньж, зорилтот дугаарыг өндөр нарийвчлалтайгаар ялгаж, танилт хийнэ.

Төслийн дараагийн шатанд, дээрх хоёр танилтад хамгийн тохиромжтой модулиудыг сургаж, гүйцэтгэлийн хувиа төөрөгдлийн матрицыг ашиглан харьцуулалт хийсэн.

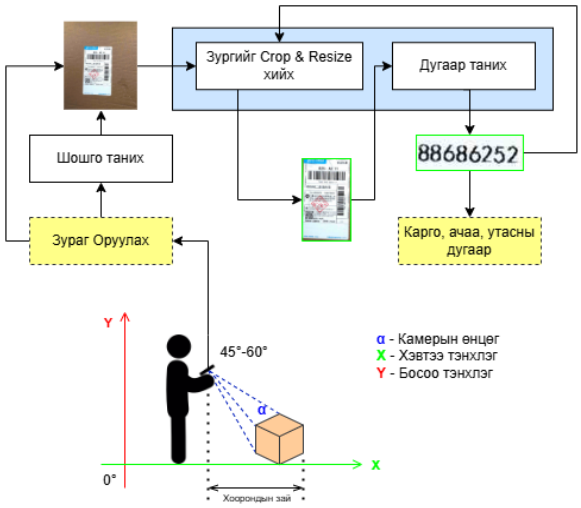
Дээрх гүйцэтгэлийн хувиа нэмэгдүүлэхийн тулд preprocessing, data augmentation ашиглан хэрхэн гүйцэтгэлийн хувь нэмэгдэж байгааг мөн харьцуулсан. Preprocessing хийснээр өгөгдлийг стандарт хэлбэртэй болгож, машин сургалтын модельд зориулсан хэрэгтэй мэдээллийг бэлдэх ба системийн гүйцэтгэлийн хувь нэмэгдсэн. Data augmentation хийснээр өгөгдлийн олон янз байдлыг нэмэгдүүлж, моделийн ерөнхий чадварыг сайжруулан, таних гүйцэтгэлийг нэмэгдүүлсэн.

Үүнээс хамгийн өндөр гүйцэтгэлтэй моделио цаашдын хөгжүүлэлтүүдээ ашигласан ба энэхүү төслийг цаашид машин сургалт, автоматжуулалтын түвшин нэмэгдүүлэх замаар үргэлжлүүлэн хөгжүүлэхээр төлөвлөж байна.



5-р зураг. Системийн ерөнхий ажиллагаа

Дээрх зурагт системийн ерөнхий бүтэц болон үйл ажиллагааг харууллаа. Эндээс үзвэл бизнес процесс болон ямар шат дамжлагаар хэнийг дамжин ажиллаж байгаа апплейкшн процессыг харууллаа.



6-р зураг. Процессуудын холбоо хамаарал

Дээрх үйл ажиллагааг дараалан дүрсэлсэн зураг нь нь модулиудын холбоо хамаарал, ашиглаж буй модель, оролт гаралтыг дүрслэн харуулсан. Үе шатаар нь ялган дэлгэрүүлбэл дараах байдлаар тайлбарлагдана.

1. Эхний үйл ажиллагаа нь ачаа барааны зургийг дарж системд оруулна.
2. Систем нь тухайн зургаас танилт хийхийн тулд систем модуль ажиллаж эхлэх ба эхэнд нь шошгыг танина.
3. Таньсан шошгыг тасалж хуваж аваад, дараагийн дугаар таних модуль ажиллана.
4. Системийн эцэст барааны шошгоос ID, хэрэглэгчийн дугаар, бусад шаардлагатай давтагдашгүй дугаарын мэдээлэлтэй болно.

Эдгээр үйл ажиллагааг хэрэгжүүлсний дараа бодит орчинд нэвтрүүлэх явцад гарсан давуу болон сул талуудыг тодорхойлсон. Үүний үр дүнд цаашдын хөгжүүлэлтийн үндэс суурь, чиглэлийг тодорхойлж, карго үйлчилгээ эрхлэгчид болон хэрэглэгчдийг илүү үр дүнтэй холбосон, хэрэглэгчдэд ээлтэй систем бий болгох зорилтыг гаргаж өгсөн.

2-Р ХҮСНЭГТ. ТӨСЛИЙН ДАВУУ БОЛОН СУЛ ТАЛ

Давуу тал	● Аль ч улсын, ямар ч үйлдвэрийн барааны шошго дээр ажиллах боломжтой тул өргөн хэрэглээтэй. ● Манай систем нь **97%**-ийн нарийвчлалтайгаар мэдээллийг таних чадвартай бөгөөд олон төрлийн форматын бичилтийг ялгах боломжтой. ● Ашиглахад хялбар ● Хүний оролцоог багасгаж, цаг хугацаа хэмнэх, ажлын бүтээмжийг нэмэгдүүлэх давуу талтай. ● Хэрэглэгчдийн хүлээлгийн хугацаа багасах тул үйлчилгээний чанар дээшилнэ. ● Өргөтгөх боломжтой.
Сул тал	● Нэвтрүүлэхэд зардал багагүй байх магадлалтай бөгөөд жижиг карго үйлчилгээ эрхлэгчдэд санхүүгийн дарамт учруулж болзошгүй. ● Шошго дээрх дугаарын тод байдал, хэвлэлийн чанар мэтчилэн зүйлсээс хамаардаг тул гэмтсэн эсвэл стандарт бус бичилттэй шошго дээр алдаа гарах магадлалтай.

IV. ШОШГО ТАНИХ МОДЕЛЬ

Бид энэхүү судалгаанд объект таних хэд хэдэн моделиудыг туршиж, судалгааны шалгуурт үндэслэн өөрсдийн шаардлагад хамгийн тохиромжтой моделийг сонгосон. Эдгээр моделийн ялгаа нь хурд, нарийвчлал, төвөгтэй байдлын харьцаа бөгөөд энэ нь хэрэглээний тусгай шаардлага болон тооцооллын хязгаарлалттай холбоотой байдаг.

Туршилт хийхдээ дараах моделиудыг ижил дата дээр шалгаж, хэд хэдэн үзүүлэлтэд тулгуурлан сонголт хийсэн. Нийт 640x640 хэмжээтэй 10000 ширхэг өгөгдөлтэй өгөгдлийн багц дээр тус бүрийг labeling хийж сургалтын дараах 3 хэсэгт хуваасан. Үүнд :

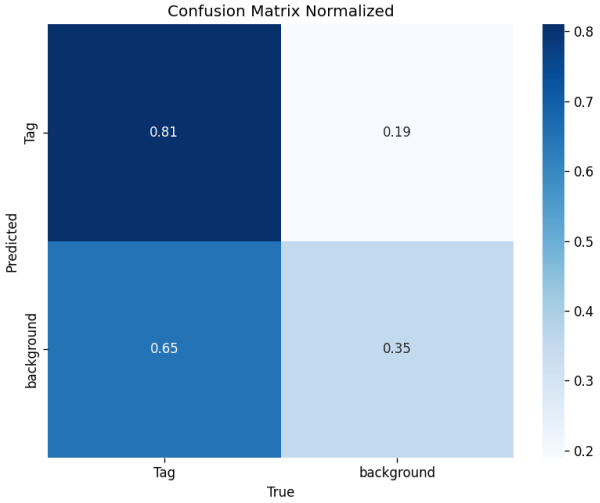
- Train - 70%
- Validation - 20%
- Test - 10%

3-Р ХҮСНЭГТ. ШОШГО ТАНИХ МОДУЛИЙН ӨГӨГДЛИЙН БАГЦ

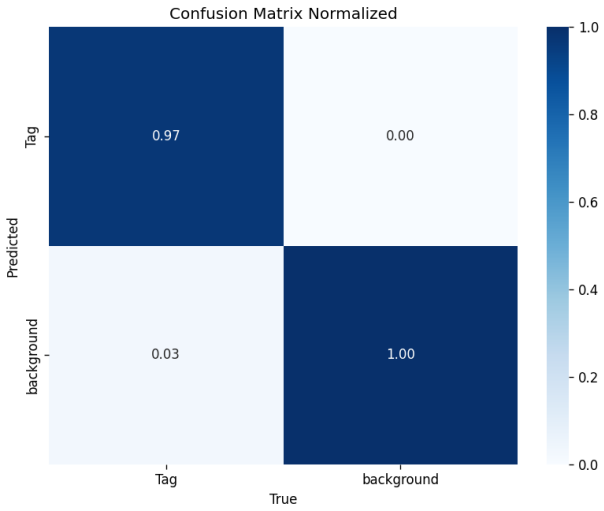
Dataset name	Label area
Source	Бодит орчноос цуглуулсан
Size	5000
Structure	● Images ● Labels

Эдгээр өгөгдлийн багцыг ашиглан объект таних өөр өөр модель дээр сургаж харьцуулан сонголтыг хийсэн. Preprocessing хийхдээ давхардал, алдаатай өгөгдлийг цэвэрлэж, өгөгдөл буюу шошгын зургуудаа стандарт хэмжээнд оруулан, танихад шаардлагатай гол элементүүдийг гарган авч өгөгдөл хуваарилсан болно.

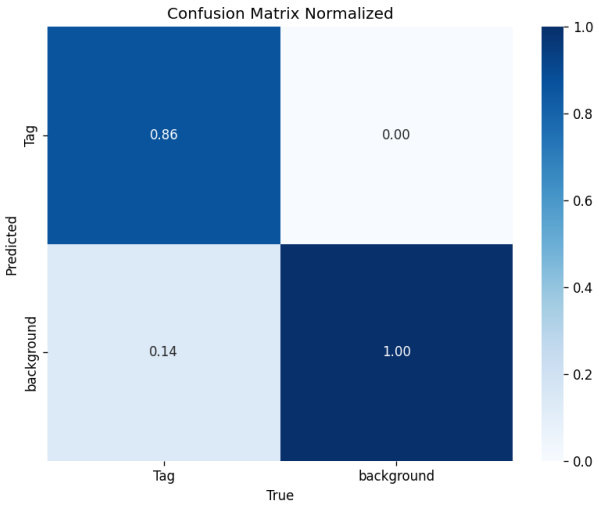
- **YOLOv8 -** YOLOv8 нь бодит цагийн танилт болон танилтын хурд өндөртэй, тиймээс видеоны болон камерын мэдээллийг шууд таних боломжтой. Энэ нь манай системийн гол давуу талыг гарган ирж байна.



7-р зураг. Модель сургасны дараа



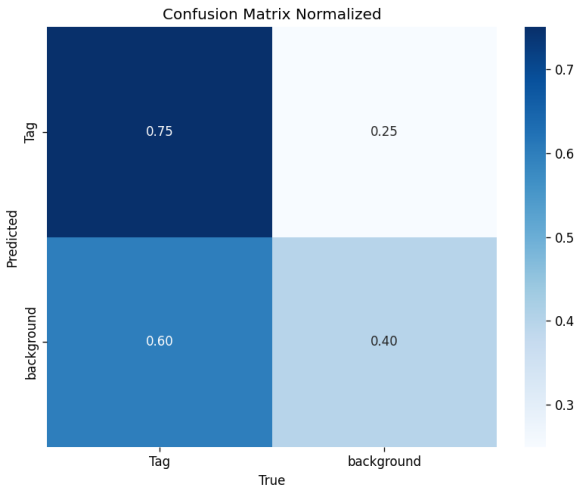
8-р зураг. Preprocessing хийсний дараа



10-р зураг. Preprocessing хийсний дараа

Бидний одоогийн серверийн нөөц болон карго үйлчилгээнд шаардлага хангахуйц үзүүлэлтэд нийцэж байсан. Мөн бодит цагийн болон хэрэгжүүлэхэд хялбар, mAP, бусад үзүүлэлт өндөр байсан нь энэ моделийг сонгох шалтгаан болсон.

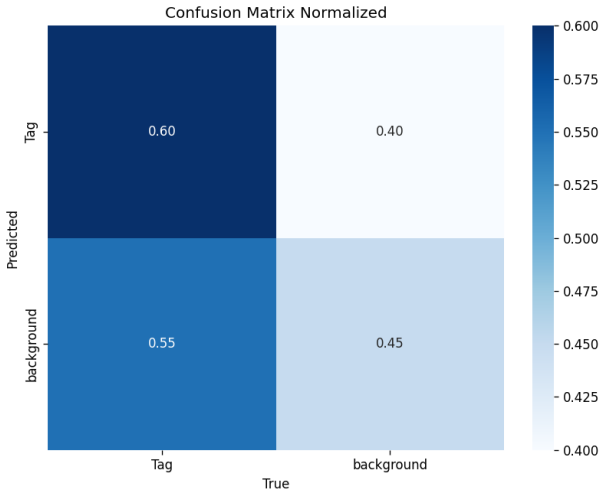
- **SSD (Single Shot MultiBox Detector)** - R-CNN-ээс хурдан ажилладаг ба бидний дараагийн сургаж туршсан модель нь дараах байдлаар үзүүлэлтүүд гарсан. Гэхдээ бусад модельтой харьцуулахад бага хүчин чадал дээр ажиллах боломжтой байдал нь сул тал болсон.



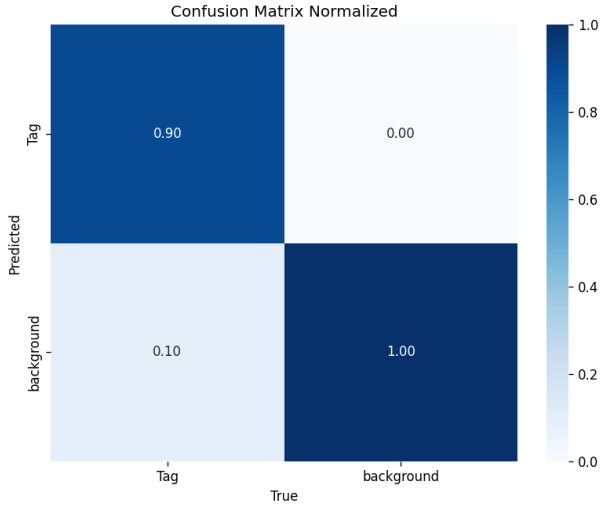
9-р зураг. Модель сургасны дараа

Төслийн эхний хэсэг болох шошго таних модулийг SSD модель дээр сургасан ба өмнөх болон дараах байдлаар төөрөгдлийн матриц гаргаж харьцуулалт хийж үзсэн. Үүнээс дүгнэн харахад моделийг сургаж нарийвчлал өссөн бидний хүссэн үр дүнд хараахан хүрээгүй байсаар байсан.

- **Faster R-CNN** - Тус модель нь объект таних хамгийн сайн, боломжтой загваруудын нэг юм. Энэ нь Region Proposal Network (RPN)-г нэвтрүүлснээр өмнөх хувилбаруудаа (R-CNN ба Fast R-CNN) сайжруулж, илүү хурдан болсон.



11-р зураг. Модель сургасны дараа



12-р зураг. Preprocessing хийсний дараа

R-CNN нь SSD болон YOLO зэрэг бусад объект таних загвартай харьцуулахад илүү өндөр mAP - тай байсан ч бусад үзүүлэлтүүдийг үзэхэд хангалтгүй байсан.

4-Р ХҮСНЭГТ. ШОШГО ТАНИХ МОДЕЛИЙН ХАРЬЦУУЛАЛТ

Модель	[1]	[2]	[3]
mAP	53%	50%	**58%**
Precision	**49%**	46%	47%
Recall	**95%**	86%	90%

Тодорхой шошгыг таних, илрүүлэх талаар одоо байгаа судалгааг судлахад Лаптев болон бусад судлаачид шошгод дүн шинжилгээ хийх зургийн сегментчиллийн янз бүрийн аргыг судалж үзсэн [7]. Тэд сегментчлэхдээ Unet, MobileNetV2, VGG16, YOLO алгоритмуудыг ашигласан ба сегментчилэхэд хамгийн тохиромжтой сүлжээ бол 96.92%-ийн нарийвчлалтай YOLO гэж мэдэгджээ.

Бид алдааны хувь, дундаж үзүүлэлтүүдийг нарийвчлан судалсны үндсэн дээр YOLO моделийг сонгож, түүнд тохирсон хэрэглээний нөхцөл болон өөрсдийн шаардлагыг харгалзан үзсэн.

V. ДУГААР ТАНИХ МОДЕЛЬ

Энэхүү хэсэгт бид ачаа бараа дээрх шошго хаяг таних моделийг туршиж, боловсруулж үр дүнгээс тохирох моделийг сонгох ажлыг хийсэн. Дараах моделиудад тус бүр ижил дата дээр туршиж үзсэн ба хэд хэдэн үзүүлэлт дээр тулгуурлан сонгосон.

5-Р ХҮСНЭГТ. ДУГААР ТАНИХ МОДУЛИЙН ӨГӨГДЛИЙН БАГЦ

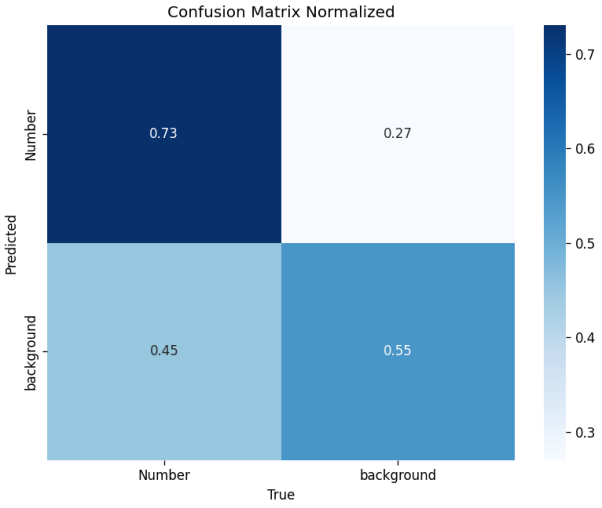
Dataset name	Number
Source	Бодит орчноос цуглуулсан
Size	5000
Structure	• Images • Labels

Data Augmentation хийж сургахад манай баг нь дараах үйл ажиллагааг хийсэн. Үүнд :

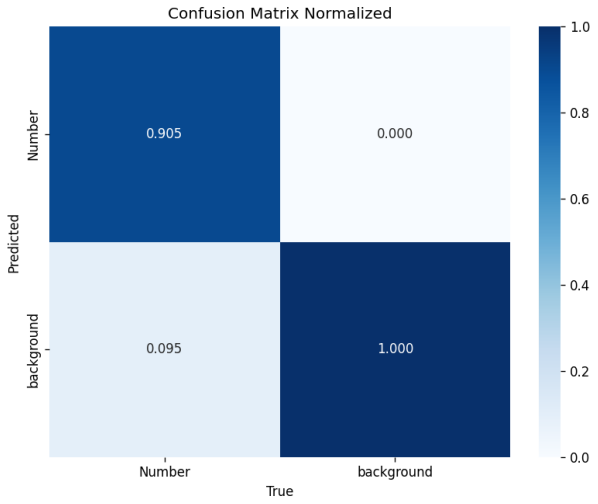
1. Blur - Сарнисан
2. Crop - Хуваасан
3. Noise added - Алдааг нэмэгдүүлэх
4. Rotate (Horizontal, Vertically) - Эргүүлсэн

Эдгээр өгөгдлийн багцыг ашиглан тэмдэгт таних өөр өөр модель дээр сургаж харьцуулан сонголтыг хийсэн.

- **Tesseract OCR** - Энэ нь нээлттэй эхийн (open source) тул чөлөөтэй ашиглах боломжтой мөн нейрон сүлжээ ашигласан тул бичгийн хэлбэр өөрчлөгдсөн ч таних чадвар сайтай байсан нь давуу тал болж байсан

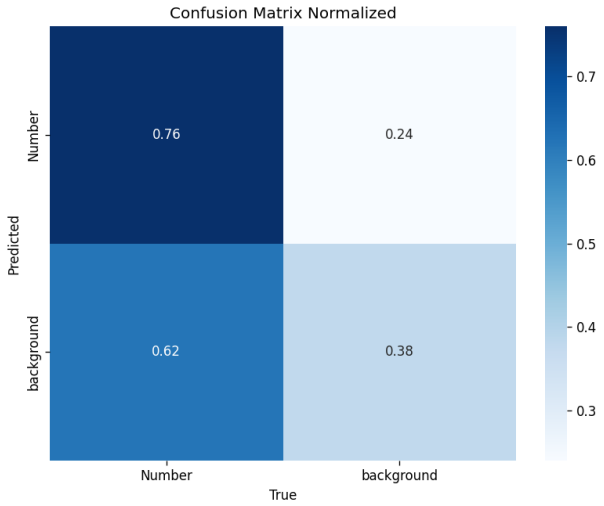


13-р зураг. Модель сургасны дараа

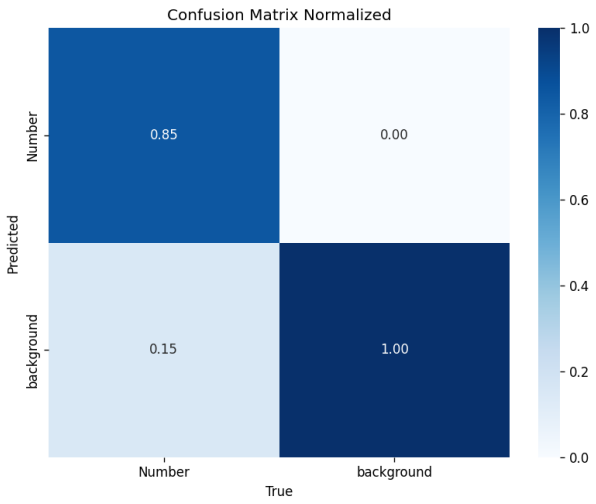


14-р зураг. Data Augmentation хийсний дараа

- **Easy OCR** - Тус модель нь хэрэглээний түвшин ашиглахад хялбар, нарийвчлал ч мөн сайн байсан. Гэхдээ бага хэмжээний өгөгдөл дээр сайн бол өгөгдлийн хэмжээ ихсэхэд алдааны хувь өссөн хандлагатай байх сул талтай байсан.



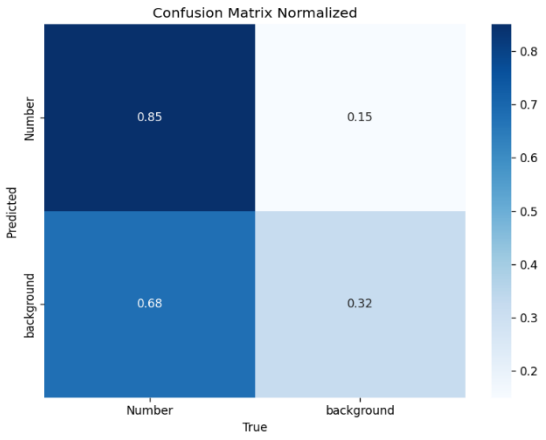
15-р зураг. Модель сургасны дараа



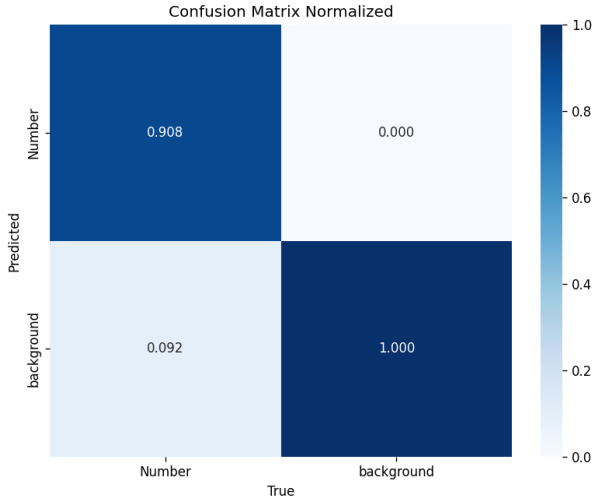
16-р зураг. Data Augmentation хийсний дараа

Дараах Easy OCR модель нь нөгөө хоёр модельтой харьцуулаад үзэхэд бага өгөгдөл дээр сайн ажилдаг энгийн хэрэглээд тохиромжтой гэж үзсэн нь манай систем дээр тохиромжгүй гэж дүгнэсэн.

- **Paddle OCR** - Эцсийн модель болох Paddle OCR нь илүү хурдан ажиллагаатай бөгөөд GPU-д тохиромжтой, нарийвчлал өндөртэй байсан. Гэхдээ хэрэгжүүлэлт нь нарийн төвөгтэй, өртөг өндөр байж болох бөгөөд маш их хэмжээний өгөгдөл дээр сайн ажилсан.



17-р зураг. Модель сургасны дараа



18-р зураг. Data Augmentation хийсний дараа

Paddle OCR модель нь GPU-тэй нөхцөлд тогтмол сайн ажиллах боломжтой ба энэ бидний одоогийн ашиглаж буй клөүд серверийн үзүүлэлтэй зохицохгүй байсан тул больсон.

6-Р ХҮСНЭГТ. ДУГААР ТАНИХ МОДЕЛИЙН ХАРЬЦУУЛАЛТ

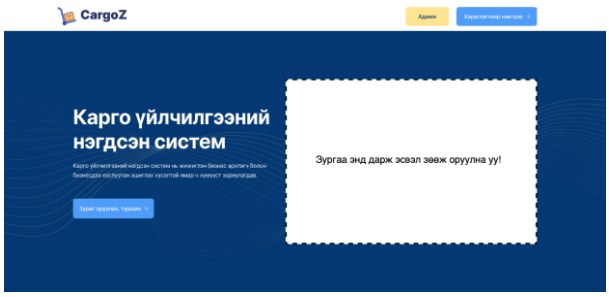
Модель	[1]	[2]	[3]
mAP	56%	50%	**63%**
Precision	**48%**	46%	48%
Recall	**92%**	85%	91%

Эцэст нь үзүүлэлтүүдийг судалсны үндсэн дээр дугаар таних модулийг Tesseract ашиглан хөгжүүлэхээр сонгосон.

VI. ХЭРЭГЖҮҮЛЭЛТ

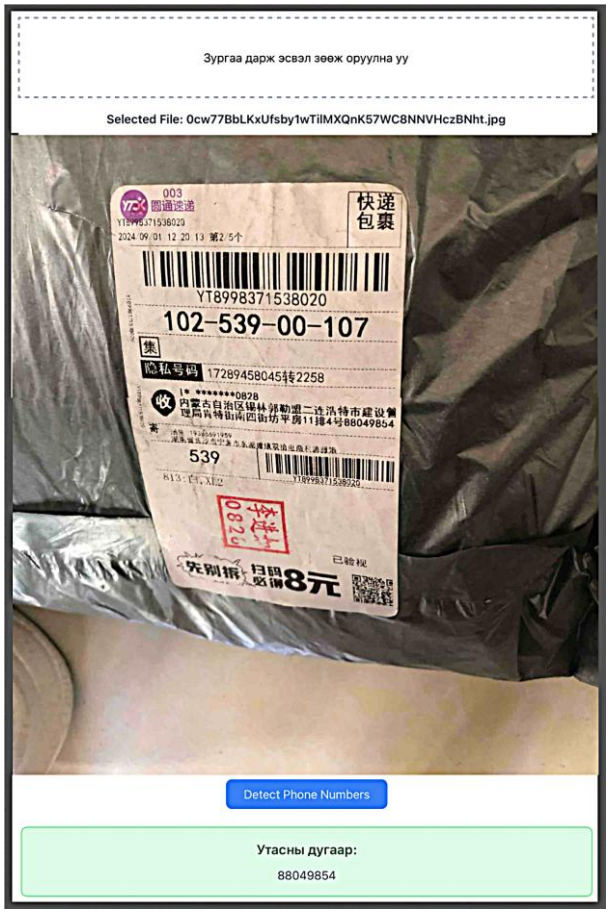
Карго үйлчилгээний систем нь ерөнхий дараах интерфейстэй байх бөгөөд хэрэглэгчдэд ойлгомжтой байлгах үүднээс хийсэн. Хэрэгжүүлэлтийн явцад бид энгийн, урвуу харсан, сарнисан, урагдсан гэх мэт асуудалтай шошго дээр туршилт хийсэн.

Харин хэрэгжүүлэлтийн үр дүнг дараагийн бүлэгт ангилал тус бүрд тест хийж тооцоолсон. Хэрэгжүүлэлтийн явцад дараах ангилалд 3000 гаруй удаа туршилт хийгдсэн ба гаралт болгоныг тэмдэглэж, хөгжүүлэх шаардлага өндөртэй хэсгийг танихад чиглүүлж өгсөн.



20-р зураг. Системийн нүүр хэсэг

Дараах байдлаар туршилтуудыг хийж манай системийн одоогийн ажиллагааны хувийг гаргаж ирсэн. Мөн цаашдын анхаарах зүйлсийг танихад тус болсон.



21-р зураг. Системийн ажиллагаа

VII. ТЕСТ

Туршилтын явцад хийгдсэн үйл явц, ажиллагааг нарийвчлан бодит үр дүнг гаргахын хувьд системийн тест болон программ хангамжийн тест хийж үзсэн.

A. Unit test - Нэгжийн тест

Программ хангамжийн нэгж эсвэл бүрэлдэхүүн хэсгүүдийг тусад нь туршиж үзэх нь программ хангамжийн туршилтын арга юм. Эдгээр нэгжүүд

нь кодын хамгийн жижиг хэсгүүд бөгөөд ихэвчлэн функцүүд бөгөөд хүлээгдэж буй гүйцэтгэлийг баталгаажуулдаг. [8]

1. Шошго таних модуль
2. Дугаар таних модуль

8-Р ХҮСНЭГТ. НЭГЖИЙН ТЕСТИЙН ҮР ДҮН

Test	Модуль	Тестийн тоо	Үнэн	Худал	%
[A]	[1]	250	232	18	**92%**
	[2]	250	238	12	96%

22-р зураг. Туршилтын ангилал

B. Integration test - Интеграцийн тест

Модулийн хоорондох интерфейсийг шалгах үйл явц юм. Энэ нэгдсэн нэгжүүдийн хоорондын харилцан үйлчлэлийн алдааг илрүүлэх явдал юм. Бүх модулиудыг нэгжээр шалгасны дараа нэгтгэх туршилтыг хийнэ. [9]

9-Р ХҮСНЭГТ. ИНТЕГРАЦИЙН ТЕСТИЙН ҮР ДҮН

Test	Модуль	Тестийн тоо	Үнэн	Худал	%
[B]	[1], [2]	500	476	24	**95%**

C. Performance test - Гүйцэтгэлийн тест

Системийн гүйцэтгэл, өргөтгөх чадварыг үнэлэхэд чиглэсэн программ хангамжийн туршилтын нэг төрөл юм. Гүйцэтгэлийн тест нь алдааг тодорхойлох, янз бүрийн ачаалал, нөхцөлд системийн гүйцэтгэлийг хэмжих, систем нь хүлээгдэж буй хэрэглэгчдийн тоо эсвэл гүйлгээг зохицуулахад чиглэгддэг.

Манай систем нь Монгол улсын үндэсний дата төвийн клөүд сервер дээр ажилсан. Доор серверийн үзүүлэлтийг багтаав.

10-Р ХҮСНЭГТ. СЕРВЕРИЙН ҮЗҮҮЛЭЛТ

Үзүүлэлт	Тохиргоо
Программчлалын хэл	Python
Үйлдлийн систем	Ubuntu 22.04 LTS
CPU	64vCPU (32core)
Memory	128 GB
Storage	1TB SSD
Firewall	all allowed
Epoch	all 200

Системийн гүйцэтгэлийн тестийг хийхийн тулд ерөнхий системийн үзүүлэлтүүдийг багтаав. Мөн нийт туршилтын үед системийн ачаалал нь ихдээ 5.3 сек, багадаа 3.4 сек хугацаанд ажилллаж байсан ба бидний одоогийн хөгжүүлэлтийн үед шаардлага хангасан ч илүү сайжруулах шалтгаан болсон.

VIII. ЦААШДЫН ХӨГЖҮҮЛЭЛТ

I. Программ хангамж

Цаашид модулиудаа сургах өгөгдлөө нэмэгдүүлэн, системийн гүйцэтгэлийг 99%-д хүргэнэ. Мөн карго үйлчилгээний бизнес эрхлэгчдэд зориулсан санхүүгийн тайлан гаргах функцийг нэмнэ.

II. Төхөөрөмж

Системийнхээ программ хангамжийг RFID төхөөрөмжтэй интеграци хийснээр алдаа гарах эрсдэлийг бууруулах, ажиллах хүчний зардлыг багасгах, бодит цагийн мэдээлэл дамжуулалт хийх боломжтой болно. Энэ нь карго үйлчилгээний найдвартай байдлыг нэмэгдүүлж, хэрэглэгчийн сэтгэл ханамжийг дээшлүүлэхэд чухал нөлөө үзүүлнэ.

22-р зураг. RFID төхөөрөмж

ДҮГНЭЛТ

Бид ачаа барааны шошгыг таньж, үүн дээрээ үндэслэн хэрэглэгчийн утасны дугаар, барааны код бусад мэдээллийг таних замаар карго үйлчилгээ процессыг автоматжуулахыг зорьсон. Судалгааны явцад туршилтын алдаа болон гүйцэтгэлийн үзүүлэлтүүдийг нарийвчлан судалж, харьцуулалт хийснээр цаашдын хөгжүүлэлтэд хэрэгжүүлэх шаардлагатай шинэ санаанууд тодорхойлогдсон. Шошго таних болон дугаар таних чадвар нь системийн бодит үр дүн болон найдвартай байдалд чухал нөлөө үзүүлж байгааг туршилтаар баталлаа. Мөн туршилтаар шошго таних зорилгоор YOLOv8 загварт суурилсан объект таних алгоритмыг ашиглаж, 3000 бодит туршилт хийсэн. Үүний үр дүнд шошго таних модуль 81%-ийн, дугаар таних модуль 73%-ийн нарийвчлалтай болохыг баталгаажуулсан. Энэхүү гүйцэтгэлийн хувийг нэмэгдүүлэхийн тулд preprocessing хийсний дараа модуль 1 - ийн гүйцэтгэл 97%, data augmentation хийсний дараа модуль 2-ын гүйцэтгэл 90% болж нэмэгдсэн. Эдгээр үр дүн нь судалгааны үр дүнгийн чанарыг дээшлүүлж, цаашдын хөгжүүлэлтийг бодитой болгоход чиглэсэн суурь нөхцөлийг бүрдүүлж өгч байна.

ТАЛАРХАЛ

Энэхүү төслийг хийж гүйцэтгэхэд туслалцаа үзүүлж, их зүйлийг зааж, чиглүүлж өгсөн удирдагч багш Доктор (Ph.D) С.Өлзийбаяр, зөвлөх багш нартаа баярлалаа.

НОМ ЗҮЙ

[1] Статистикийн мэдээллийн нэгдсэн сан Бүх төрлийн тээврийн ачаа эргэлт, тээврийн төрлөөр, сая тонн.км

[2] A Lightweight Barcode Detection Algorithm Based on Deep Learning, 2024 он, Jingchao Chen, Ning Dai, Xudong Hu, Yanhong Yuan

[3] MGL-YOLO: A Lightweight Barcode Target Detection Algorithm, 2024 он, Yuanhao Qu, Fengshou Zhang

[4] Enhancing automated vehicle identification by integrating YOLOv8 and OCR techniques for high-precision license plate detection and recognition, 2024 Jun, Hanae Moussaoi, Nabil El Akkad, Mohamed Benslimane, Walid El-Shafai, Abdullah Baihan, Chaminda Hewage, Rajkumar Singh Rathore

[5] Yan, L.Y.; Tan, G.W.H.; Loh, X.M.; Hew, J.J.; Ooi, K.B. QR code and mobile payment: The disruptive forces in retail. J. Retail. Consum. Serv. 2021.

[6] Development of a Price Tag Detection System on Mobile Devices using Deep Learning, 2022, Melek Turan, Musa Peker, Huseyin Ozkan, Cevat Balaban

[7] Neural network-based price tag data analysis. Future Internet, 2022, Laptev P., Litokin S., Davydenko S.

[8] Unit Testing - Software Testing - GeeksforGeeks

[9] Integration Testing - Software Engineering - GeeksforGeeks

[10] https://www.scmp.com/news/china/article/1694077/state-commerce-regulator-releases-damming-account-tabaocom-day-alibaba

[11] Joseph Redmon болон Anelia Angelova, RealTime Grasp Detection Using Convolutional Neural Networks (ICRA), 2015.

[12] Neural Network-Based Price Tag Data Analysis, 2022, Pavel Laptev, Sergey Litovkin, Anton Konev

[13] Multi-Directions Scene Text Detection Based on Improved YOLO, 2021, Liyun Xiao, Peng Zhou, Ke Xu

[14] Automatic Container Code Recognition using Deep Learning, 2021, Athira M.D, Lijo Jacob

[15] Монгол Улсад ХХК карго системийн тоо баримт ерөнхий 60-80 гаруй байдаг, Монсүх Карго ХХК захирал

ХИЙМЭЛ ОЮУН УХААНЫГ АШИГЛАН ЭРҮҮЛ МЭНДИЙН ШИНЖИЛГЭЭНИЙ ХАРИУНД АНАЛИЗ ХИЙХ

П.ЭРДЭНЭ-ҮҮЛ[1], Н.НОМИН-ЭРДЭНЭ[1], Г.ГАНЧИМЭГ[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын ухааны салбар
Холбоо барих зохиогчийн и-мэйл хаяг: erdenevvl67@gmail.com[1], ganaa@must.edu.mn[2]

***Хураангуй*: Орчин үед хиймэл оюун ухааны технологи нь эрүүл мэндийн салбарт маш хурдацтай нэвтэрч байгаа бөгөөд ялангуяа өвчтөний эрүүл мэндийн шинжилгээний хариуг дүгнэх, эрт үеийн өвчний илрүүлэлт, эмчилгээний төлөвлөгөө гаргах зэрэг чиглэлээр өргөн хэрэглэгдэж байна. Эрүүл мэндийн шинжилгээний хариуг дүгнэхэд эмч нар хугацаа их зарцуулдаг бөгөөд зарим тохиолдолд хүний алдаа гарах эрсдэлтэй байдаг. Энэ нь өвчтөнүүдийн оношилгоо хийлгэх хугацааг уртасгаж, эмчилгээний үр дүнд сөргөөр нөлөөлдөг. Мөн эмнэлгийн мэдээллийн системд хадгалагдаж буй өгөгдлүүдийг бүрэн ашиглаж чадахгүй байгаа нь эрүүл мэндийн салбарт тулгарч буй нэг асуудал юм. Иймд эрүүл мэндийн шинжилгээний хариуг хиймэл оюун ухааны аргаар шинжилж эмч нарт шуурхай, нарийвчилсан дүгнэлт санал болгох шаардлагатай байна. Энэ өгүүлэлд эрүүл мэндийн шинжилгээний хариуг боловсруулах хиймэл оюун ухааны загварууд болон хөгжүүлж буй системийн архитектур ба туршилтын үр дүнг танилцуулна.**

***Түлхүүр үг:** Эрүүл мэнд, шинжилгээ, хариу, загвар, сургалт, өгөгдөл*

I. УДИРТГАЛ

Хиймэл оюун ухаан (AI) нь эрүүл мэндийн салбарт шинжилгээний хариуг унших, дүн шинжилгээ хийх, оношлох, өвчний эрсдэлийг тодорхойлох зэрэг олон чиглэлээр ашиглагдаж байна [1]. Энэ нь оношилгооны үр дүнг сайжруулах, эмч нарын ажлыг хөнгөвчлөх, өвчний эрт илрүүлэлтийг нэмэгдүүлэх давуу талтай. Эмч нар өдөр бүр маш олон тооны шинжилгээний хариуг уншиж, тайлбарлах шаардлагатай болдог. Энэ нь цаг хугацаа их зарцуулдаг ба хүний анхаарал сарнисан үед алдаа гарах эрсдэлтэй байдаг [2]. Хиймэл оюун ухааны системүүд нь эдгээр өгөгдлийг автоматаар боловсруулж, хэвийн бус өөрчлөлтийг илрүүлэх, өвчний эрсдэлийг үнэлэх боломжийг олгодог [3-4]. *Жишээ нь*: IBM Watson Health нь лабораторийн шинжилгээний үр дүнг дүн шинжилгээ хийж, оношлох үйл явцыг сайжруулдаг. Google DeepMind компани AI ашиглан нүдний торлог бүрхүүлийн өвчнийг илрүүлдэг. Zebra Medical Vision нь рентген зураг дээрх эмгэг өөрчлөлтийг AI ашиглан автоматаар илрүүлдэг. Nuance компанийн AI платформ нь эмнэлгийн бичвэрийг боловсруулж, эмч нарт шийдвэр гаргахад тусалдаг. Deep Genomics компани AI ашиглан удамшлын өвчнийг оношлох шинэ аргачлалыг боловсруулсан.

Хиймэл оюун ухааныг эрүүл мэндийн шинжилгээнд дараах төрлүүдэд түгээмэл ашигладаг. *Үүнд [5-9]:*

1. Лабораторийн шинжилгээний хариуг дүн шинжилгээ хийх
   - ***Автомат дүн шинжилгээ***: AI нь цусны, шээсний, генетикийн шинжилгээ зэрэг лабораторийн хариуг хурдан боловсруулж, хэвийн болон хэвийн бус үзүүлэлтүүдийг тодорхойлж чадна.
   - ***Өгөгдлийн хазайлтыг илрүүлэх***: Машин сургалтын алгоритмууд нь өвчтөн бүрийн шинжилгээний өгөгдлийг түүхтэй нь харьцуулж, эмгэг өөрчлөлтийг эрт илрүүлэх боломжтой. *Жишээ нь*: Машин сургалтын регресс, шийдвэрийн мод, дэмжих вектор машин зэрэг алгоритмууд нь лабораторийн шинжилгээний хариуг ангилахад хэрэглэгддэг бол гүн сургалтын загварууд нь зураглалын шинжилгээнүүдэд *(рентген, КТ зэрэг)* үр дүнтэй ажилладаг. Convolutional нейрон сүлжээ *(CNN)* нь дүрсийн шинжилгээнд, Recurrent нейрон сүлжээ *(RNN)* нь цаг хугацааны цуваа өгөгдөлд хэрэглэгддэг.
2. Эмнэлгийн дүрслэлээс оношгаргах (Radiology & Imaging AI)
   - ***Рентген, MRI, CT зургийг шинжлэх***: AI нь дүрслэлийн өгөгдлөөс хавдар, ясны хугарал, судасны бөглөрөл зэрэг эмгэг өөрчлөлтүүдийг илрүүлэхэд тусалдаг.
   - ***Автомат оношилгоо***: Deep Learning загварууд нь эмч нарт туслан дүрснээс эмгэгийг илрүүлэх нарийвчлалыг сайжруулдаг ба автоматаар илрүүлдэг.
3. Байгалийн хэл боловсруулалт (NLP) ашиглан шинжилгээний тайлан унших
   - ***Эмнэлгийн тэмдэглэлээс мэдээлэл олборлох***: AI нь эмч нарын бичсэн тайлан, шинжилгээний

хариуг боловсруулж, оношилгоонд шаардлагатай өгөгдлийг гаргаж өгдөг.

- ***Автомат дүгнэлт хийх***: NLP загварууд эмчийн бичсэн тайлбарыг автоматаар ангилж, өвчтөний оношинд мэдээллийг нэгтгэн харуулна.

4. Генетикийн шинжилгээнд AI ашиглах

- ***Удамшлын өвчнийг оношлох***: Генетикийн өгөгдлийг AI ашиглан боловсруулж, удамшлын өвчний эрсдэл өндөртэй хүмүүсийг илрүүлэх.
- ***Генетик мэдээлэлд суурилсан эмчилгээ***: AI нь өвчтөний генетикийн өгөгдлийг ашиглан тохирсон эмчилгээ санал болгох боломжтой.

Хиймэл оюун ухааныг эрүүл мэндийн салбарт ашиглах нь дараах давуу талуудтай. *Үүнд [9-10]:*

- ***Хурдан, нарийвчлалтай***: Шинжилгээний үр дүнг богино хугацаанд гаргаж, алдааг багасгана.
- ***Эрт оношилгоо***: Эмнэлзүйн шинжилгээнээс өмнө өвчнийг илрүүлэх боломжтой.
- ***Эмч нарын ажлыг хөнгөвчлөх***: Том хэмжээний өгөгдлийг автоматаар боловсруулснаар эмч нарын ачаалал багасна.
- ***Хямд, хүртээмжтэй***: Хүний хүчин зүйлээс шалтгаалах алдаа, өртгийг бууруулна.

Түүнчлэн AI нь эрүүл мэндийн салбарт шинжилгээний хариуг унших, дүн шинжилгээ хийх, оношлох үйл явцыг хурдасгах, үр дүнг сайжруулах боломжтой хэдий ч хүний хяналт зайлшгүй шаардлагатай бөгөөд өгөгдлийн аюулгүй байдал, ёс зүйн асуудлуудыг сайтар анхаарах хэрэгтэй.*Үүнд [11-13]:*

- ***Өгөгдлийн аюулгүй байдал***: Эмнэлгийн мэдээллийг хамгаалах шаардлагатай.
- ***AI хариуцлагын асуудал***: Буруу оношгаргах эрсдэлтэй.
- ***Хүний хяналт шаардлагатай***: AI зөв ашиглахын тулд эмч нарын оролцоо чухал.

II. ЭРҮҮЛ МЭНДИЙН ШИНЖИЛГЭЭНИЙ ХАРИУ БОЛОВСРУУЛАЛТ

Эрүүл мэндийн шинжилгээний хариунд анализ хийхэд ашигладаг хиймэл оюун ухааны (AI) загварууд нь эмнэлзүйн оношилгоо, эмчилгээний төлөвлөлт, өвчний урьдчилан сэргийлэлт зэрэг олон чиглэлд хувь нэмэр оруулж байна [9-12]. AI загварууд нь эрүүл мэндийн салбарт өгөгдөлд суурилсан шийдвэр гаргалтыг дэмжиж, өвчтөний тусламж үйлчилгээг сайжруулахад чиглэгдсэн [13]. Гэсэн хэдий ч, тэдгээрийг хэрэгжүүлэхдээ өгөгдлийн чанар, ёс зүйн асуудал, эмч нарын оролцоо зэрэг хүчин зүйлсийг анхаарах шаардлагатай. Тус судалгааны ажлаар эрүүл мэндийн шинжилгээний цаасан хариуг унших боломжтой программ хөгжүүлж туршилт хийхийг зорьсон. Хиймэл оюун ухаанаар боловсруулах хэсэг нь цусны, биохимийн шинжилгээ, рентген зураг зэрэг янз бүрийн төрлийн өгөгдлийг боловсруулж, тайлбарлах процессыг багтаана.

Лабораторийн шинжилгээнүүдийн хэмжилтүүд нь тодорхой хэм хэмжээтэй харьцуулах замаар үнэлж болох тоон өгөгдлүүд байдаг. Харин зураглалын шинжилгээнүүд нь илүү нарийн дүрс таних алгоритмуудыг шаарддаг. Хиймэл оюун ухаан дараах үндсэн үйлдлүүдийг гүйцэтгэнэ. *Үүнд:*

- *Өгөгдлийн цуглуулалт ба боловсруулалт*
- *Хэвийн бус өөрчлөлтийн илрүүлэлт*
- *Эрсдэлийн үнэлгээ ба оношилгоо*
- *Эмчилгээний зөвлөмж*
- *Өвчний хяналт*

Эрүүл мэндийн шинжилгээний хариуг боловсруулахын тулд өгөгдлийг эмнэлгийн мэдээллийн системээс олборлож, цэвэрлэж, нэгтгэх шаардлагатай болсон. Мөн зургаас өгөгдлийг уншихдаа дутуу өгөгдлийг засах, гажуудлыг шүүх, өгөгдлийн бүтцийг стандартчилах зэрэг үйлдлүүд хийгдэнэ. Түүнчлэн хиймэл оюун ухаан ашиглан эрүүл мэндийн шинжилгээний хариуг унших системийг 1 дүгээр хүснэгтэд үзүүлсэн хүн хүч болон мөнгөн зардлаар хөгжүүлбэл тухайн эмнэлэг эсвэл байгууллага нь гар аргаар шинжилгээний хариуг боловсруулж дүгнэснээс эдийн засгийн хувьд илүү ашигтай байх тооцооллыг үзүүлсэн.

1-Р ХҮСНЭГТ. ЭДИЙН ЗАСГИЙН ҮНДЭСЛЭЛ

№	Төслийн багийнхан	Цалин (₮, сая)	Бусад зардал (₮, сая)
1	Хөгжүүлэгч 1	2.4	0.8
2	Хөгжүүлэгч 2	2.4	0.8
3	Өгөгдлийн шинжээч	2.5	0.5
4	Эрүүл мэндийн мэргэжилтэн	2.0	0.4
5	Төслийн менежер	1.8	0.5
Нийт		11.1	3.0

Лабораторийн шинжилгээний хариуг шууд хиймэл оюунаар (AI) уншуулж өвчнийг оношлох нь эдийн

засгийн хувьд олон давуу талтай, гэхдээ эрсдэлүүд ч бас бий [17-19]. *Үүнд:*

Эдийн засгийн ашиг тус:

1. **Хөдөлмөрийн зардал хэмнэнэ** – Эмч, лаборантын цагийг хэмнэж, хүний нөөцийн зардлыг бууруулна.
2. **Шинжилгээний хариу гаргах хурд нэмэгдэнэ** – AI 24/7 ажиллаж, олон хүний шинжилгээг хурдан боловсруулах боломжтой.
3. **Оношилгооны нарийвчлал нэмэгдэнэ** – AI том хэмжээний өгөгдөл дээр суралцаж, хүний алдаа гаргах магадлалыг багасгана.
4. **Эмнэлгийн ачааллыг бууруулна** – Өвчтөн бүр эмч дээр очих шаардлагагүй болж, зөвхөн онцгой тохиолдолд л эмчийн оролцоо шаардлагатай болно.
5. **Хөдөө, алслагдсан бүсийн хүртээмж сайжирна** – Тусгай эмч дутагдалтай газруудад хиймэл оюунаар оношилгоо хийх нь эрүүл мэндийн үйлчилгээний хүртээмжийг нэмэгдүүлнэ.

Эдийн засгийн боломжит эрсдэлүүд:

1. **Анхны хөрөнгө оруулалт өндөр** – AI системийг хөгжүүлэх, алгоритм сургах, дата боловсруулалт хийх нь өндөр зардал шаарддаг.
2. **Хүний баталгаажуулалт зайлшгүй шаардлагатай** – AI онош буруу тавьсан тохиолдолд хариуцлагын асуудал үүсэж болзошгүй.
3. **Хууль, зохицуулалтын асуудал** – Эрүүл мэндийн салбарт AI ашиглах нь эрх зүйн орчныг бүрдүүлэх шаардлагатай болно.
4. **Шинэ ажлын байр бий болох ч, зарим ажлын байр алдагдана** – Лаборант, шинжилгээний эмч нарын ажлын шаардлага буурч, харин AI хөгжүүлэгч, дата шинжээчдийн хэрэгцээ өснө.
5. **Өвчний хүнд, ховор тохиолдлуудад AI хангалттай сайн ажиллахгүй байж болно** – Зарим өвчний нарийн оношилгоонд AI бүрэн хангалттай биш байж болно.

Эдийн засгийн эрсдэлүүд байгаа хэдий ч эдийн засгийн үр өгөөж нь илүү юм. *Жишээ нь [17]:* АНУ-д хийсэн судалгаагаар AI ашиглан лабораторийн оношилгооны процессыг автоматжуулснаар эмнэлгүүд жилд 10-30%-ийн үйл ажиллагааны зардал хэмнэх боломжтой гэж үзсэн.

Хятад, Энэтхэгт AI суурилсан оношилгоо хямд, хүртээмжтэй болсноор орлого багатай иргэдэд эрүүл мэндийн үйлчилгээний хүртээмж сайжирсан.

Иймд хиймэл оюунаар лабораторийн шинжилгээний хариуг уншуулж, онош тавих системийг зөв нэвтрүүлбэл эдийн засгийн хувьд ашигтай, хэмнэлттэй, шуурхай, хүртээмжтэй. Гэхдээ хүний оролцоо зайлшгүй хэрэгтэй, хяналт шаардлагатай. Тиймээс хиймэл оюуныг эмч нарт туслах хэрэгсэл болгон ашиглавал хамгийн үр өгөөжтэй юм.

III. СИСТЕМИЙН ХӨГЖҮҮЛЭЛТ БА ТУРШИЛТЫН ХЭСЭГ

Эрүүл мэндийн шинжилгээний лабораторийн хариуг дүгнэх хиймэл оюун ухааны системийг дараах технологиудыг ашиглан хөгжүүлсэн. *Үүнд:*

- *Frontend: JavaScript, React.js, Next.js*
- *Backend: Python, Flask, Django*
- *Өгөгдлийн сан: PostgreSQL*
- *Машин сургалт: TensorFlow, PyTorch, Scikit-learn*
- *API: RESTful API, GraphQL*
- *Аюулгүй байдал: OAuth 2.0, JWT, HTTPS*

Судалгааны арга зүй дараах хэсгүүдтэй. *Үүнд:*

Өгөгдлийн сан: Өвчтөний мэдээлэл, шинжилгээний хариу, эмчилгээний түүх зэргийг хадгалах.

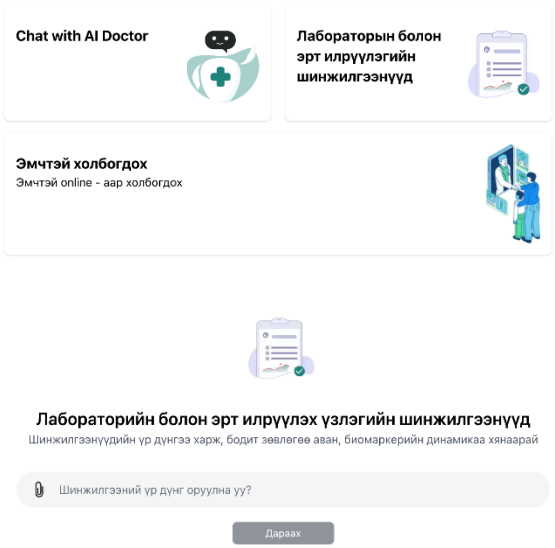
Өгөгдөл боловсруулах хэсэг: Өгөгдлийг цэвэрлэх, нэгтгэх, хувиргах.

ХОУ загвар: Шинжилгээний хариуг боловсруулж, дүгнэлт гаргах.

Хэрэглэгчийн интерфейс: Эмч, өвчтөнүүдэд мэдээллийг ойлгомжтой хэлбэрээр харуулах.

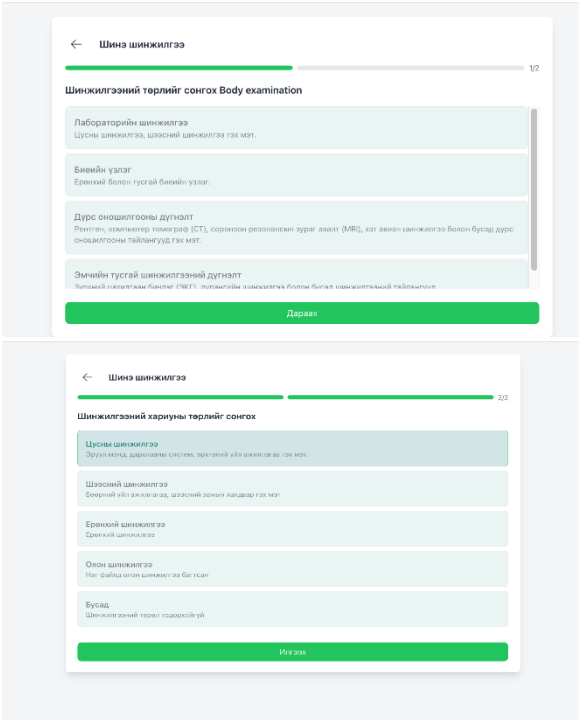
Аюулгүй байдлын давхарга: Өвчтөний мэдээллийн нууцлалыг хангах.

Системийн хэрэглэгчийн интерфейсийн харагдах байдлыг 1 ба 2 дугаар зургуудад үзүүлсэн. Интерфейс нь хэрэглэгчид шинжилгээний хариуг ойлгомжтой уншиж, хэвийн бус өөрчлөлтийг болзошгүй учир шалтгаан болон авах хувийн арга хэмжээ эмчид яаралтай хандвал зохих эсэхийг хялбархан олж мэдэх боломжийг олгоно.



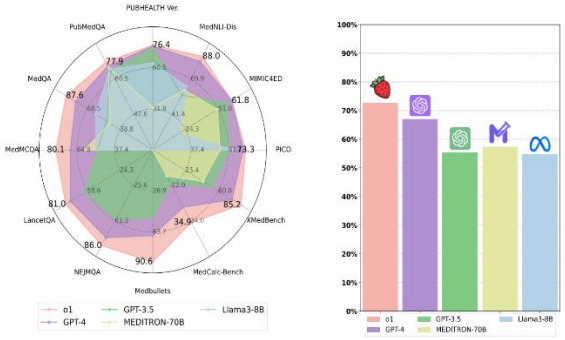
1-р зураг. Хөгжүүлж буй программын харагдах хэсэг I

Тус хөгжүүлж буй системд эрүүл мэндийн шинжилгээний хариуг оруулахдаа зураг, текст хэлбэрээр оруулах боломжтой ба чатбот хэсгээс өвдөж буй байдлын шинж тэмдгүүдээ хүүрнэх байдлаар бичээд зөвлөгөө авч болно.



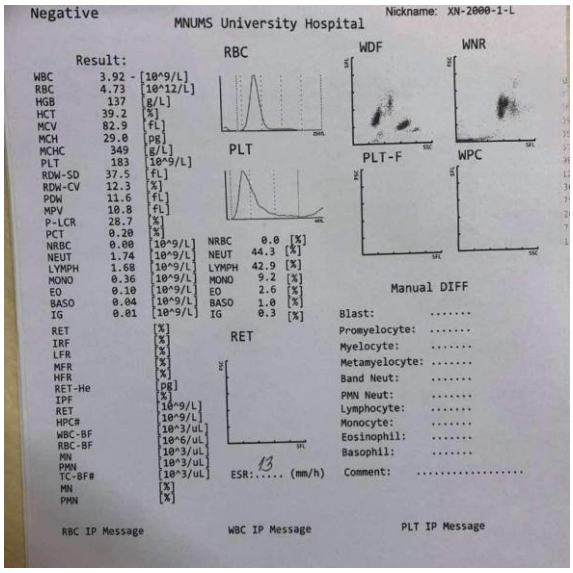
2-р зураг. Хөгжүүлж буй программын харагдах хэсэг II

Бидний судалгаандаа ашиглаж буй хиймэл оюуны o1 загвар нь 2024 оны 9 дүгээр сард танилцуулагдсан бөгөөд өмнөх загваруудаас ялгаатай нь хариултаа өгөхөөс өмнө илүү их хугацаа зарцуулж, дотоддоо олон боломжит хувилбарыг үнэлдэг ба o1 загвар нь илүү урт дотоод бодлын гинжин хэлхээ үүсгэж, хариултаа сайжруулдаг [14].



3-р зураг. o1 болон бусад 4 хүчирхэг LLM загварын 12 эмнэлгийн мэдээллийн баазын дата дээр үзүүлсэн ерөнхий үр дүн [15]

3 дугаар зургаас харахад o1 загвар илүү өндөр нарийвчлалыг үзүүлсэн нь нээлттэй эхийн бусад загваруудаас илүү давуу талтай байгаа нь харагдаж байна [15-16]. Судлаачид o1 загварын эмнэлгийн салбарт, тэр дундаа лабораторийн шинжилгээний үр дүнг тайлбарлах чадварыг үнэлсэн ба o1 загвар нь эмнэлгийн ойлголт, учир шалтгааныг тодорхойлох, олон хэл дээр ажиллах чадвартай болохыг харуулсан [15-16]. Мөн o1 нь 19 эмнэлгийн мэдээллийн багцад 74.3% буюу хамгийн өндөр дундаж нарийвчлалыг гаргаж байгааг судлаачид тогтоосон байна [15]. Иймд тус судалгааны ажилдаа хиймэл оюуны o1 загварыг сонгон ашигласан.



4-р зураг. Туршилтын шинжилгээний хариу [1]

Эрүүл мэндийн шинжилгээний хариуг автоматаар боловсруулах систем нь өвчтөний цуглуулсан мэдээлэлд үндэслэн өвчний эрсдэлийг үнэлэх, өөрчлөлтийг хянах, эмчилгээний үр нөлөөг дүгнэх зэрэг олон чадамжтай. 4 дүгээр зурагт үзүүлсэн лабораторийн шинжилгээний хариуг боловсруулж буй системийн туршилтын үр дүнг 5 дугаар зурагт үзүүлэв.

1. **WBC (Цагаан эсийн тоо) : 3.92 x 10^9/L**
   - Хэвийн хэмжээ: 4.0-11.0 x 10^9/L
   - Дүгнэлт: Доогуур. Энэ нь дархлаа сул, халдвар болон бусад асуудалтай холбоотой байж болно.
2. **RBC (Улаан эсийн тоо) : 4.73 x 10^12/L**
   - Хэвийн хэмжээ: 3.8-5.4 x 10^12/L
   - Дүгнэлт: Хэвийн.
3. **HGB (Гемоглобин) : 137 g/L**
   - Хэвийн хэмжээ: 120-160 g/L
   - Дүгнэлт: Хэвийн.
4. **HCT (Гематокрит) : 39.0%**
   - Хэвийн хэмжээ: 36-46%
   - Дүгнэлт: Хэвийн.
5. **MCV (Дундаж эсийн хэмжээ) : 82.9 fL**
   - Хэвийн хэмжээ: 80-100 fL
   - Дүгнэлт: Хэвийн.
6. **MCH (Дундаж эсийн гемоглобин) : 29.0 pg**
   - Хэвийн хэмжээ: 27-32 pg
   - Дүгнэлт: Хэвийн.
7. **MCHC (Дундаж эсийн гемоглобин концентраци) : 349 g/L**
   - Хэвийн хэмжээ: 320-360 g/L
   - Дүгнэлт: Хэвийн.
8. **PLT (Тромбоцитын тоо) : 185 x 10^9/L**
   - Хэвийн хэмжээ: 150-450 x 10^9/L
   - Дүгнэлт: Хэвийн.
9. **RDW-CV (Эсийн хэмжээний тархалт) : 37.5%**
   - Хэвийн хэмжээ: 11.5-14.5%
   - Дүгнэлт: Өндөр. Энэ нь улаан эсийн хэмжээнд өөрчлөлт байж болохыг харуулж буй тул нарийн оношилгоо шаардлагатай.
10. **LYMPH (Лимфоцит) : 42.9%**
    - Хэвийн хэмжээ: 20-40%
    - Дүгнэлт: Өндөр. Энэ нь вирусийн халдвар эсвэл дархлаа тогтолцоо идэвхжсэн үед ажиглагдана.
11. **NEUT (Неутрофил) : 44.3%**
    - Хэвийн хэмжээ: 40-70%
    - Дүгнэлт: Хэвийн.

Нийт дүгнэлт:

Лабораторийн шинжилгээний үр дүнг үнэлэхэд ихэнх үзүүлэлтүүд референс хязгаарт байна. Гэсэн хэдий ч WBC-ийн түвшин бууралттай, RDW-ийн үзүүлэлт илүүдэлтэй байгаа нь цус тэлжилтийн процессын алдагдал болон/эсвэл дархлааны тогтолцооны үйл ажиллагааны өөрчлөлтийг илтгэж болзошгүй юм. Энэхүү үр дүнд үндэслэн дараах арга хэмжээг авахыг зөвлөж байна: (1) давтан шинжилгээг 7-14 хоногийн дотор хийлгэх; (2) гематологийн нэмэлт үзүүлэлтүүдийг тодорхойлох шинжилгээ (ялтсын тоо, ретикулоцитийн түвшин, сийвэнгийн төмрийн хэмжээ, ферритин гэх мэт); (3) шаардлагатай гэж үзвэл дархлааны системийн үзүүлэлтүүдийг тодорхойлох нарийвчилсан шинжилгээ хийлгэх. Та эмнэлзүйн хяналтад байж шаардлагатай бөгөөд эдгээр үзүүлэлтүүдийн динамик өөрчлөлтийг тогтмол хянах нь зүйтэй.

5-р зураг. Эмнэлгийн шинжилгээний хариуг тайлбарласан туршилтын хэсэг

Бидний боловсруулж буй систем нь нэг шинжилгээний хариуг оруулаад дүгнэлт гаргахад ойролцоогоор 10 секундээс 1 минут зарцуулна. Шинжилгээний хариу график дүрслэлтэй болон олон төрлийн шинжилгээний бичиглэлтэй үед 1 минут орчим зарцуулж байгаа бол ганц төрлийн эсвэл цөөн хэмжигдэхүүнтэй шинжилгээний хариуг 10-15 секундийн хооронд хурдан боловсруулж байсан. Туршилтын үр дүнг цаашид сайжруулан үргэлжлүүлэн хийж байгаа болно.

ДҮГНЭЛТ

Хиймэл оюун ухааныг эрүүл мэндийн шинжилгээний хариуг боловсруулахад ашиглах нь эмч нарын ажлын ачааллыг бууруулж, алдаа гарах эрсдэлийг багасгах, оношилгооны хурдыг нэмэгдүүлэх зэрэг олон давуу талтай. Энэхүү судалгааны ажлаар эрүүл мэндийн шинжилгээний хариуг боловсруулах хиймэл оюун ухааны системийн архитектурыг танилцуулж, түүнийг бүтээхэд шаардагдах хүний нөөц болон санхүүгийн зардлыг тооцоолон үзүүлсэн. Уламжлалт гар аргаар шинжилгээний хариуг дүгнэхийг хиймэл оюун ухааны системээр автоматжуулснаар эмнэлгийн үйл ажиллагаанд үр өгөөж нэмэгдэж, эмч нар өвчтөний оношийг бага хугацаанд тодорхойлоход чухал ач холбогдолтой юм.

НОМ ЗҮЙ

[1] A. Esteva, A. Kuprel, R. A. Novoa, J. Ko, S. M. Swetter, H. M. Blau, and S. Thrun, "Dermatologist-level classification of skin cancer with deep neural networks," Nature, vol. 542, no. 7639, pp. 115–118, 2017.

[2] V. Gulshan, L. Peng, M. Coram, M. C. Stumpe, D. Wu, A. Narayanaswamy, et al., "Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs," JAMA, vol. 316, no. 22, pp. 2402–2410, 2016.

[3] D. S. Kermany, M. Goldbaum, W. Cai, C. C. Valentim, H. Liang, S. L. Baxter, et al., "Identifying medical diagnoses and treatable diseases by image-based deep learning," Cell, vol. 172, no. 5, pp. 1122–1131, 2018.

[4] J. De Fauw, J. R. Ledsam, B. Romera-Paredes, S. Nikolov, N. Tomasev, S. Blackwell, et al., "Clinically applicable deep learning for diagnosis and referral in retinal disease," Nature Medicine, vol. 24, no. 9, pp. 1342–1350, 2018.

[5] B. Shickel, P. J. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis," IEEE Journal of Biomedical and Health Informatics, vol. 22, no. 5, pp. 1589–1604, 2018.

[6] Z. Obermeyer and E. J. Emanuel, "Predicting the future — big data, machine learning, and clinical medicine," The New England Journal of Medicine, vol. 375, no. 13, pp. 1216–1219, 2016.

[7] C. Xiao, E. Choi, and J. Sun, "Opportunities and challenges in developing deep learning models using electronic health records data: a systematic review," Journal of the American Medical Informatics Association, vol. 25, no. 10, pp. 1419–1428, 2018.

[8] A. Rajkomar, E. Oren, K. Chen, A. M. Dai, N. Hajaj, M. Hardt, et al., "Scalable and accurate deep learning with electronic health records," NPJ Digital Medicine, vol. 1, no. 1, p. 18, 2018.

[9] Valentin Li´evin, Christoffer Egeberg Hother, Andreas Geert Motzfeldt, and Ole Winther. Can large language models reason about medical questions? Patterns, 2024.

[10] Yunxiang Li, Zihan Li, Kai Zhang, Ruilong Dan, Steve Jiang, and You Zhang. Chatdoctor: A medical chat model fine-tuned on a large language model meta-ai (llama) using medical domain knowledge.Cureus, 15(6), 2023.

[11] Tessa Han, Aounon Kumar, Chirag Agarwal, and Himabindu Lakkaraju. Towards safe large language models for medicine. In ICML 2024 Workshop on Models of Human Feedback for AI Alignment, 2024.

[12] Albert Q Jiang, Alexandre Sablayrolles, Arthur Mensch, Chris Bamford, Devendra Singh Chaplot, Diego de las Casas, Florian Bressand, Gianna Lengyel, Guillaume Lample, Lucile Saulnier, et al. Mistral 7b. arXiv preprint arXiv:2310.06825, 2023.

[13] Di Jin, Eileen Pan, Nassim Oufattole, Wei-Hung Weng, Hanyi Fang, and Peter Szolovits. What disease does this patient have? a large-scale open domain question answering dataset from medical exams. Applied Sciences, 2021.

[14] OpenAI. Openai o1 system card. https://openai.com/index/openai-o1-system-card/, September 2024.

[15] Y Xie, J Wu, H Tu, S Yang, B Zhao, Y Zong, Q Jin, C Xie, Y Zhou, A Preliminary Study of o1 in Medicine: Are We Closer to an AI Doctor? arXiv preprint arXiv:2409.15277, 2024•arxiv.org

[16] Xidong Wang, Nuo Chen, Junyin Chen, Yan Hu, Yidong Wang, Xiangbo Wu, Anningzhe Gao, Xiang Wan, Haizhou Li, and Benyou Wang. Apollo: Lightweight multilingual medical llms towards democratizing medical ai to 6b people. arXiv preprint arXiv:2403.03640, 2024.

[17] Жулиен Флоркин, “AI-ийн Ашиг Тус: Өөрчлөлт, Сорилт, Боломжууд”, https://julienflorkin.com/mn

[18] Хиймэл оюун ухааны засаглалын тогтолцооны загварчлал тохимол, https://www.crc.gov.mn/storage

[19] Бодлого боловсруулагчдад зориулсан гарын авлага: Хиймэл оюун ухаан, том хэлний загвар болон бусад зүйлс зэрэг хурдацтай хөгжиж буй технологиудыг үнэлэх, https://mn.council.science/publications/ai-policy/

ГЭРИЙН АВТОМАТЖУУЛАЛТЫГ ДУУ ХООЛОЙГООР УДИРДАХ

А.ДАВААСҮРЭН[1], С.БАТДАЛАЙ[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Холбооны салбар
Холбоо барих зохиогчийн и-мэйл: davasuren146@gmail.com[1], batdalai@must.edu.mn[2]

Хураангуй: **Орчин үеийн ухаалаг гэрийн технологи нь хэрэглэгчийн тав тухыг нэмэгдүүлж, энерги хэмнэлттэй байдлыг сайжруулж байна. Энэ судалгаанд ESP8266 WROOM-32 микроконтроллер, WS2812B LED гэрэл ашиглан хүссэн өнгөөр асаах, BME680 мэдрэгч ашиглан өрөөний агаарын чанарыг хянаж, Chimege SST (Speech-to-Text), TTS (Text-to-Speech) API ашиглан хэрэглэгчтэй дуу хоолойгоор харилцах ухаалаг системийг хөгжүүлж буй судалгааны ажлын үр дүнг танилцууллаа. Энэ систем нь Монгол Улсад ухаалаг технологийн хөгжлийг дэмжих, хэрэглэгчдэд эх хэл дээрээ дуу хоолойн удирдлагатай орчин бүрдүүлэх боломжийг олгоно.**

Түлхүүр үг: Ухаалаг гэр, дуу хоолойн удирдлага, агаарын чанар, IoT, Chimege API, ESP8266 WROOM-32, BME680, WS2812B LED

I. УДИРТГАЛ

Сүүлийн жилүүдэд интернэтэд холбогдсон ухаалаг төхөөрөмжүүд (IoT) эрчимтэй хөгжиж, хүний өдөр тутмын амьдралд нэвтэрч байна. Дэлхийн томоохон технологийн компаниуд Amazon Alexa, Google Assistant, Apple Siri зэрэг дуу хоолойн туслахуудыг хөгжүүлснээр хэрэглэгчид гэр ахуйн цахилгаан хэрэгсэл, аюулгүй байдлын систем болон бусад төхөөрөмжүүдийг дуу хоолойгоор удирдах боломжтой болжээ.

Монгол Улсад энэхүү технологийн хөгжүүлэлт харьцангуй удаан байгаа ч Chimege API-ийн дэвшилтэт шийдлүүд гарч ирснээр монгол хэл дээрх дуу хоолойн удирдлагатай систем хөгжүүлэх боломж бүрдэж байна. Энэхүү судалгаагаар ухаалаг гэрийн технологийг монгол хэлээр дэмжих, өрөөний агаарын чанарыг хянах, хэрэглэгчтэй дуу хоолойн интерфейсээр харилцах боломжтой системийг хөгжүүлж буй ажлыг танилцуулна.

1-Р ХҮСНЭГТ. ОЛОН УЛСАД ХЭРЭГЛЭГДДЭГ СИСТЕМҮҮД [1]

д/д	Нэр
1	Amazon Alexa
2	Apple siri
3	Google assistant
4	Huawei technologies
5	Baidu DuerOS
6	Tencent AI Lab

Өөр улсын бүтээгдэхүүний судалгаа:
Дэлхийн дуу хоолойн удирдлагатай системийн хөгжүүлэлт

- Amazon Alexa, Google Assistant, Apple Siri зэрэг технологийн шийдлүүд нь хэрэглэгчийн дуу хоолойг таньж, даалгавар биелүүлдэг. Гэвч эдгээр системүүд нь Монгол хэл дээрх дэмжлэг хангалттүй байгаа.
- Baidu DuerOS, Tencent AI Lab зэрэг Хятадын системүүд нь ази хэлнүүдийг илүү сайн ойлгодог боловч Монгол хэл дээр мөн адил хязгаарлагдмал байна.

IoT ба ухаалаг гэрийн шийдлүүд

- **ESP8266, ESP32, Raspberry Pi** зэрэг микроконтроллерүүдийг ашиглан ухаалаг гэрийн төслүүд өргөн хөгжиж байна.
- **BME680 мэдрэгч** нь температур, чийгшил, даралт, VOC (Organic Compound) гэх мэт агаарт агуулагдах хорт бодисыг хэмжих боломжтой.
- **WS2812B LED** нь өнгийг динамикаар өөрчлөх, хэрэглэгчтэй интерактив харилцах боломжийг олгодог.

1-р зураг. Amazon Alexa харагдах байдал [2]

2-р зураг. Google assistant харагдах байдал [3]

Дуу хоолойн удирдлагын ашигтай байдал:

- Дуу хоолойгоор удирддаг ухаалаг гэрийн систем хөгжүүлэх
- Монгол хэл дээр хэрэглэгчтэй харилцах боломж бүрдүүлэх
- Агаарын чанарын мэдээллийг дуу хоолойгоор дамжуулан мэдээлэх - BME680 мэдрэгчийн тусламжтай өрөөний агаарыг хянаж, бохирдлын түвшнийг хэрэглэгчдэд мэдэгдэх боломжтой.
- Дуу хоолойн удирдлага нь харааны болон хөдөлгөөний бэрхшээлтэй хүмүүст төхөөрөмжүүдийг хялбар удирдах боломж олгоно.
- Ийм төрлийн систем нь технологийн шинэчлэлийг хэрэглэгчдийн өдөр тутмын амьдралд нэгтгэн, бидний сэтгэхүйн болон хэрэглээний хэв маягийг өөрчлөх ач холбогдолтой. Энэ нь шинэ технологийг өргөн хүрээнд танилцуулах, хэрэглэгчдэд илүү өндөр түвшний үйлчилгээ үзүүлэх боломжийг олгоно.

Системийн бүтэц ба хөгжүүлэлт

Техник хангамжийн бүтэц

- ESP8266 WROOM-32 – Удирдлагын үндсэн микроконтроллер
- BME680 мэдрэгч – Температур, чийгшил, VOC хэмжих
- WS2812B LED – Гэрэлтүүлэг болон агаарын чанарыг өнгөөр илэрхийлэх
- Чанга яригч, микрофон – Дуу хоолойгоор мэдээлэл дамжуулах

Программ хангамжийн бүтэц

- **Chimege SST API** – Дуу хоолойг текст болгон хөрвүүлэх
- **Chimege TTS API** – Текстийг дуу хоолойгоор унших
- **Arduino IDE, Micropython,** – Код бичих, төхөөрөмжүүдийг програмчлах

Системийн шаардлага

A. Функциональ шаардлага (Functional Requirements)

1.1 Дуу хоолойгоор LED удирдах

Хэрэглэгч "улаан ас!", "ногоон ас!", "цэнхэр ас!", "гэрэл унтраа!" гэх мэт тушаал өгч LED-г удирдана.

ESP32-WROOM32 нь Chimege STT API-аас ирсэн текстийг таньж, WS2812B LED-г тохирох өнгөөр асаана.

1.2 Агаарын чанарын мэдээлэл авах

- Хэрэглэгч "агаарын чанар?" гэж хэлэхэд ESP32 нь:
  - BME680 мэдрэгчээс температур, чийгшил, хорт утааны түвшин авах
  - Эдгээр мэдээллийг Chimege TTS API ашиглан дуу хоолойгоор уншуулах

1.3 Дуу хоолойн гаралт (Voice Feedback)

- ESP32 нь агаарын чанарын мэдээллийг Chimege TTS API-рүү илгээж, чанга яригч руу буцааж дуу хоолойгоор өгнө.
- Жишээ: "Температур 22°C, чийгшил 40%, хорт утаа бага байна."

1.4 Wi-Fi холболт

- ESP32 нь Wi-Fi сүлжээнд холбогдож, Chimege API-рүү хандаж тушаал хүлээн авна.

B. ТЕХНИК ХАНГАМЖИЙН ШААРДЛАГА (Hardware Requirements)

Бүрэлдэхүүн хэсэг	**тайлбар**
ESP32	Wi-Fi-д холбогддог микроконтроллер
WS2812B LED Strip (1+ LED)	Өнгө солигддог LED
BME680 мэдрэгч	Температур, чийгшил, Хорт утаа хэмжих (CO_2, NH_3)
5V 2A Power Adapter	ESP32, LED-д хүчдэл өгөх
Чанга яригч, өсгөгчийн хамт	Эргэн хариу өгөх
Микрофон	Яриаг оруулах

C. ПРОГРАММ ХАНГАМЖИЙН ШААРДЛАГА (Software Requirements)

Программ	**Тайлбар**
Arduino IDE / PlatformIO	Код бичих, ESP32 програмчлах
ESP32WiFi, WebServer, Adafruit_NeoPixel, BME680 сангууд	ESP32 дээр хэрэглэх
Chimege API (STT + TTS)	Дуу хоолойг боловсруулах
WebSocket / HTTP API	Микроконироллероос тушаал авах

Гүйцэтгэлийн шаардлага (Performance Requirements)

- ESP32 нь Wi-Fi сүлжээнд автоматаар холбогдож байх ёстой.
- Chimege API-д тушаал илгээх хурд 4 сек-ээс бага байх.
- WS2812B LED нь тушаал өгснөөс хойш 1с дотор асах ёстой.
- Агаарын чанарын мэдээлэл 5 сек-ийн дотор боловсруулагдаж, хариу өгөх ёстой.

Хэрэглээний шаардлага (Usability Requirements)

- Дуу хоолойн тушаалууд ойлгомжтой, хялбар байх ёстой.
- Микрофоноос дуу хоолойгоор команд өгөхөд нэмэлт төхөөрөмж шаардахгүй.
- Гэрлийн өнгийг өөрчлөх, унтраах нь хурдан, хялбар байх ёстой.

Хамгаалалтын шаардлага (Security Requirements)

- Wi-Fi холболтод зөвхөн итгэмжлэгдсэн төхөөрөмж нэвтрэх ёстой.
- ESP32 нь зөвхөн тодорхой IP хаягаас Chimege API-тэй холбогдох ёстой.
- Тушаалууд зөвхөн тухайн хэрэглэгчийн төхөөрөмжөөс л хүлээн авах ёстой.

DATASHEET

1. Ерөнхий мэдээлэл

- Бүтээгдэхүүний нэр: Дуу хоолой удирдлагатай агаарын чанар, гэрэлтүүлгийн систем
- Загвар: ESP32-VC02
- Үндсэн микроконтроллер: ESP32-WROOM-32
- Холболт: Wi-Fi
- Гол функцүүд:
  - Дуу хоолойгоор LED гэрэл удирдах
  - Агаарын чанарыг хэмжих
  - Дуу хоолойн хариуг чанга яригчаар сонсох
  - Чимэгээ API ашиглан STT/TTS хийх

- **Техникийн үзүүлэлтүүд**

  - **Тэжээлийн хангамж**

- Ажиллах хүчдэл: 220v AC
- Эрчим хүчний зарцуулалт: Дунджаар 250мА – **500мА**

  - **ESP32-WROOM-32 Модуль**

- CPU: Dual-core Xtensa LX6 240MHz
- RAM: 520KB SRAM + 4MB Flash
- Интерфейсүүд: I2C, I2S, PWM, GPIO, UART, SPI
- Wi-Fi: **802.11 b/g/n (2.4GHz)**

  - **Мэдрэгч (BME680)**

- Температур хэмжих хүрээ: **-40°C – 85°C**
- Чийгшил: **0% – 100% RH**
- Агаарын чанар: **VOC (Дэгдэмхий органик нэгдлүүд)**
- Холболт: **I2C (SCL: GPIO22, SDA: GPIO21)**

  - **Дуу хоолойн оролт (INMP441 I2S микрофон)**

- Дуу хүлээн авах хүрээ: **60Hz – 15kHz**
- Холболт: **I2S (WS: GPIO15, SCK: GPIO14, SD: GPIO32)**

  - **2.5. Дуу гаралт (MAX98357 + Speaker)**

- Дижитал оролт: **I2S (LRC: GPIO25, BCLK: GPIO26, DIN: GPIO22)**
- Ачааллын эсэргүүцэл: **4Ω – 8Ω**
- Гаралтын чадал: **3W (4Ω, 5V оролттой үед)**

  - **2.6. Гэрэлтүүлэг (WS2812B RGB LED Strip)**

- Өнгө: **16.8 сая өнгө (RGB)**
- Холболт: **GPIO4**
- Тэжээл: **5V DC**

- **Программ хангамж ба API**

- **Хөгжүүлэлтийн орчин:** Arduino IDE, PlatformIO
- **Дуу хоолой боловсруулах:** Chimege API
- **Firmware:** OTA (Over-the-Air) шинэчлэлт дэмжинэ

4. Хэрэглээний боломжууд

- Ухаалаг гэрийн автоматжуулалт
- Гэрэлтүүлгийн дуу хоолой удирдлага
- Агаарын чанарын хяналт
- AI туслах хөгжүүлэлт

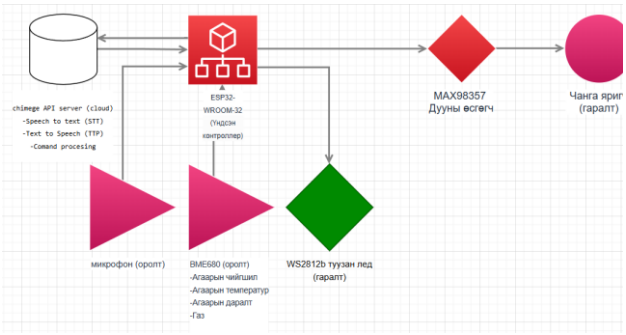
5. Физик үзүүлэлтүүд

- **Хэмжээ:** D: 60мм x h:30мм

6. Ашиглалтын нөхцөл

- Ажиллах температур: **-10°C – 60°C**
- Чийгшил: **10% – 90% RH**

Блок диаграм



4-р Зураг. Блок диаграм

📌 **Mic (Voice In):**
→ Chimege STT API ашиглан команд илгээх.

📌 **ESP32-WROOM32:**
→ Тушаал хүлээн авч **RGB LED-г удирдах, агаарын чанарын мэдээлэл авах.**

📌 **WS2812B RGB LED:**
→ "улаан", "ногоон" гэх тушаалаар өнгөө өөрчлөх.

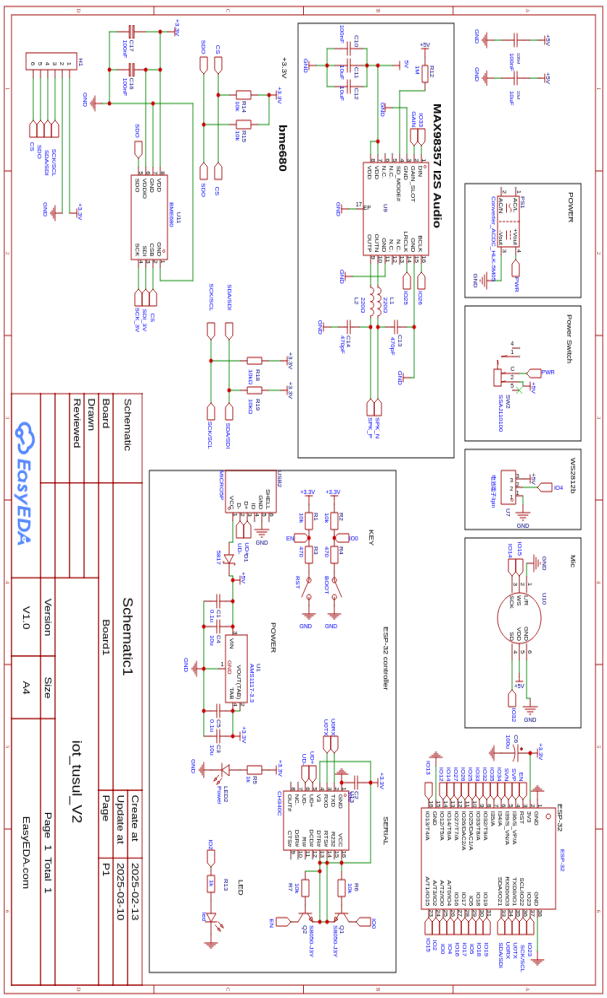
📌 **Агаарын чанарын мэдрэгч BME680:**
→ Температур, чийгшил, хорт утааны мэдээлэл дамжуулах.

📌 **Чанга яригч (Voice Out):**
→ Chimege TTS API-аас ирсэн текстийг гар утас дуу хоолойгоор унших.

Холболтын схем

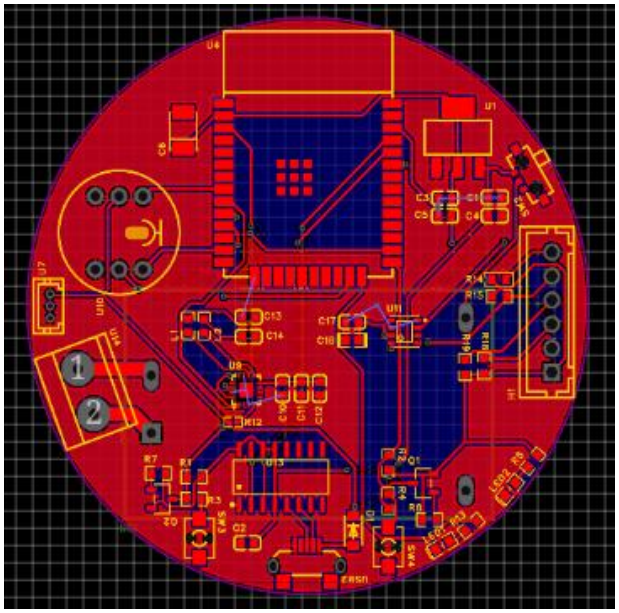
Төхөөрөмж	**Esp32 pin**
INMP441 Mic(SCK)	GPIO14
INMP441 Mic(WS)	GPIO15
BME680 (SCL)	GPIO22
BME680 (SDA)	GPIO21
INMP441 Mic(SD)	GPIO32
MAX98357(LRC)	GPIO25
MAX98357(BCLK)	GPIO26
MAX98357(DIN)	GPIO33
WS2812B LED	GPIO4

Схем зураг

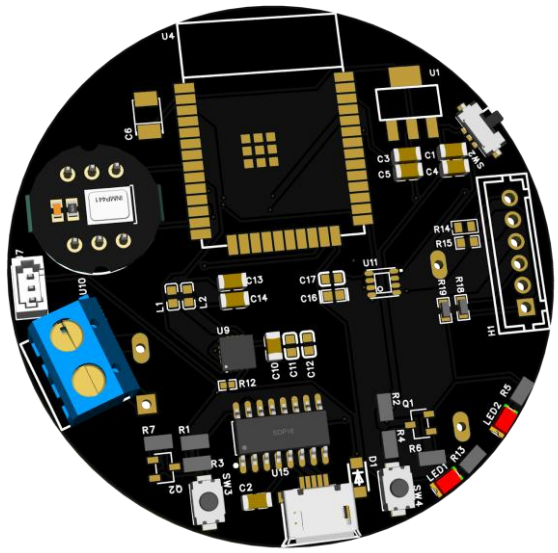


5-р зураг. Схем зураг

PCB зураг



6-зураг. PCB зураг



7-р зураг. PCB зураг 3D харагдах байдал

2-Р ХҮСНЭГТ. САНХҮҮГИЙН ТААМАГЛАЛ

д/д	Эд анги	Тоо ширхэг	Нэг бүрийн үнэ ₮	Нийт үнэ ₮
1	ESP8266 WROOM-32	1	45000	45000
	WS2812B Led	8	10000	10000
	bme680 sensor	1	50000	50000
	Чанга яригч	1	25000	25000
	Микрофон	1	15000	15000
	PCB хавтан	1	10000	10000
	3D хэвлэгээ	1	25000	25000
	Бусад туслах элементүүд	1	10000	10000
5	**Нийт**			**190,000₮**

Системийн ерөнхий урсгал

1. Систем асаагдах үед:
   1.1. Wi-Fi-д холбогдох
   1.2. Chimege API-д холбогдох
   1.3. BME680 мэдрэгчийг тохируулах
   1.4. WS2812B LED-ийг анхны төлөвт оруулах

2. Хэрэглэгчийн дуу хоолойг хүлээн авах:
   2.1. Микрофоноор хэрэглэгчийн хэлсэн үгийг бичиж авах
   2.2. Дуу хоолойг Chimege SST API руу илгээж, текст болгон хөрвүүлэх
   2.3. Текстийг боловсруулах

3. Командыг таних:
   3.1. “Агаарын чанар ямар байна?” гэх мэт команд илгээгдсэн эсэхийг шалгах
   3.2. Хэрэв агаарын чанарыг шалгах команд өгсөн бол:
      3.2.1. BME680 мэдрэгчээс мэдээлэл унших
      3.2.2. Температур, чийгшил, VOC зэрэг өгөгдлийг боловсруулж текст үүсгэх
      3.2.3. Chimege TTS API ашиглан дуу хоолойгоор мэдээлэл уншуулах
      3.2.4. LED-ийг агаарын чанарын түвшний дагуу өнгөөр гэрэлтүүлэх
   3.3. Бусад командын хариуг боловсруулах

4. Систем хүлээлтийн төлөвт шилжих:
   4.1. Дараагийн дуу хоолойг хүлээх
   4.2. Дахин шинэ команд орж ирэхийг сонсох

Алгоритмын шаталсан дэлгэрэнгүй дүрслэл

(1) Системийн эхлүүлэх процесс

Эхлүүлэх функц:
Wi-Fi-д холбогдоно
Chimege API-д холбогдоно
BME680 мэдрэгчийг тохируулна
WS2812B LED-ийн анхны төлөвийг тогтооно
Системийг хүлээлтийн төлөвт шилжүүлнэ

(2) Дуу хоолойн оролт авах

Дуу хоолойг бичиж авах функц:
Микрофоноор дууг хүлээн авна
Дууг аудио файл болгон хадгална
Аудио файлыг Chimege SST API руу илгээнэ
Буцаж ирсэн текстийг хүлээн авч боловсруулна

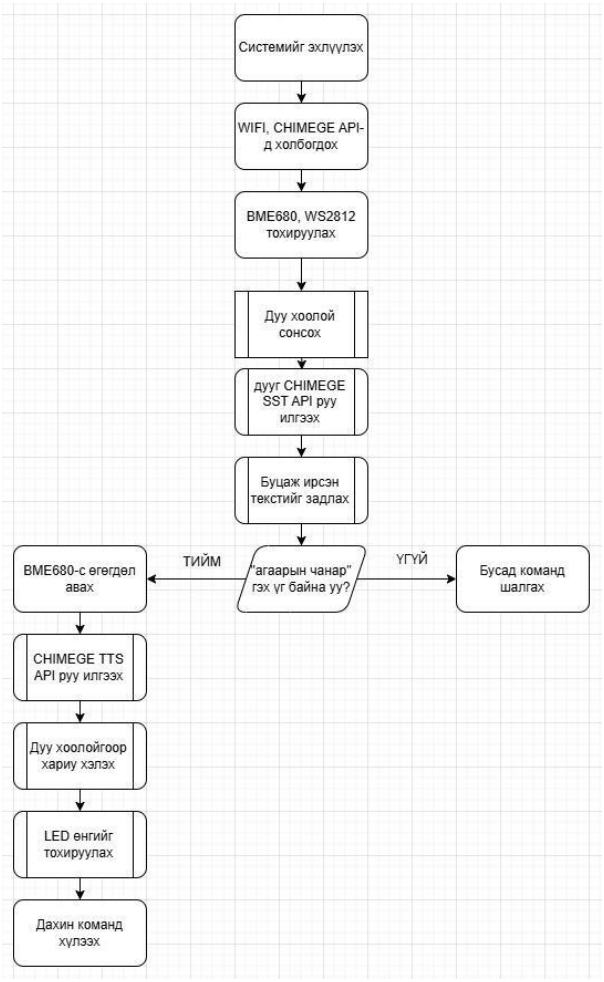
(3) Командыг таних ба боловсруулалт хийх

Команд боловсруулах функц:
"Агаарын чанар" гэх түлхүүр үг байгаа эсэхийг шалгана
Хэрэв байгаа бол:
BME680 мэдрэгчээс температур, чийгшил, VOC-г уншина
Агаарын чанарын тайлбар үүсгэнэ (Жишээ: "Өрөөний агаарын температур 23°C, чийгшил 45%, агаарын чанар хэвийн байна.")

Chimege TTS API-д текстийг илгээн дуу хоолой болгон хөрвүүлнэ
Чанга яригчаар мэдээллийг дамжуулна
LED өнгийг өгсөн утгын хэмжээнд тохируулан өөрчилнө
Бусад командуудыг шалгана (жишээ нь, гэрэл асаах, унтраах гэх мэт)

(4) LED өнгийг тохируулах
LED өнгийг тохируулах функц:
Агаарын чанарын үзүүлэлтүүдийг шалгана
Хэрэв VOC түвшин бага байвал:
LED-ийг ногоон өнгөөр асуулна
Хэрэв VOC түвшин дунд зэрэг бол:
LED-ийг шар өнгөөр асуулна
Хэрэв VOC түвшин өндөр байвал:
LED-ийг улаан өнгөөр асуулна

(5) Дахин команд хүлээх
Команд хүлээх функц:
Дахин шинэ дуу хоолойг хүлээх төлөв рүү шилжинэ
Дуу хоолойг хүлээж авсны дараа 2-р алхмаас давтаж эхэлнэ



8-р зураг. Үндсэн программын алгоритм

ДҮГНЭЛТ

Энэхүү судалгаагаар дуу хоолойгоор удирддаг, агаарын чанарыг хянадаг ухаалаг гэрийн системийг хөгжүүлж, Монгол Улсад ашиглах боломжийг судаллаа. Chimege API-ийг ашигласнаар системийг монгол хэл дээр хөгжүүлэх боломж бүрдэх бөгөөд энэ нь технологийн хөгжлийг дэмжих, агаарын бохирдлыг хянах, хөгжлийн бэрхшээлтэй иргэдэд туслах зэрэг олон давуу талтай.

Цаашид энэхүү судалгааг өргөжүүлж, нэмэлт төхөөрөмжүүд интеграци хийх, хэрэглэгчийн туршлагыг сайжруулах, зах зээлд нэвтрүүлэх судалгаа хийх шаардлагатай.

НОМ ЗҮЙ

1. IoT болон Микроконтроллер

- Bahga, A., & Madisetti, V. (2015). *Internet of Things: A Hands-On Approach*. VPT.
- Monk, S. (2017). *Programming Arduino: Getting Started with Sketches*. McGraw-Hill Education.
- McEwen, A., & Cassimally, H. (2013). *Designing the Internet of Things*. John Wiley & Sons.

2. Дуу хоолойн боловсруулалт ба AI

- Jurafsky, D., & Martin, J. H. (2021). *Speech and Language Processing*. Pearson.
- O'Shaughnessy, D. (2010). *Speech Communications: Human and Machine*. IEEE Press.
- Deng, L., & Li, X. (2013). *Machine Learning Paradigms for Speech Recognition: An Overview*. IEEE/ACM Transactions on Audio, Speech, and Language Processing.

3. Агаарын чанар ба мэдрэгчүүд

- Snyder, E. G., et al. (2013). *The Changing Paradigm of Air Pollution Monitoring*. Environmental Science & Technology.
- Wilson, J. G., et al. (2005). *Modelling Air Quality for Exposure Assessments*. Environmental Modelling & Software.
- Texas Instruments. (2020). *Understanding VOC Sensors for Air Quality Monitoring*. Application Note.

4. ESP32, WS2812B, BME680 Ашиглалт

- Espressif Systems. (2023). *ESP32-WROOM-32 Datasheet*. [Online] Available at: https://www.espressif.com/en/products/socs/esp32
- Bosch Sensortec. (2020). *BME680 Environmental Sensor Datasheet*. [Online] Available at: https://www.bosch-sensortec.com
- Adafruit Industries. (2022). *WS2812B Intelligent LEDs*. [Online] Available at: https://www.adafruit.com

МОНГОЛ ХЭЛ ДЭЭРХ ТЕКСТИЙГ ОНОВЧТОЙ ХУРААНГУЙЛАХ АРГЫН СУДАЛГАА

Бөхбатын АМАРТҮВШИН[1], Нямын ГАНТӨМӨР[1], Бямбадоржийн ЗОЛЗАЯА[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээлэл технологийн салбар
Холбоо барих зохиогчийн и-мэйл: B231910004@must.edu.mn[1], b.zolzaya@must.edu.mn[2]

Хураангуй: **Сүүлийн жилүүдэд цахим орчинд маш их хэмжээний текстэд мэдээлэл хуримтлагдаж, эдгээр мэдээллээс үнэ цэнтэй, голлох агуулгыг шуурхай оновчтой гарган авах хэрэгцээ нэмэгдэж байна. Текст хэлбэрийн мэдээлэлд буй гол санааг эх хэлний боловсруулалтын аргын тусламжтайгаар хураангуйлах нь цаг хугацааг тодорхой хэмжээгээр хэмнэх, ажлын бүтээмжийг нэмэгдүүлэх юм. Текст хураангуйллыг хэрэгжүүлэхэд хоёр төрлийн арга байх бөгөөд хийсвэр текст хураангуйлал (Abstractive text summarization), экстрактив текст хураангуйлал (Extractive text summarization) аргуудаар хэрэгжүүлдэг. Энэ удаад бид экстрактив текст хураангуйллын аргыг монгол хэл дээр хэрэгжүүлсэн ба экстрактив текст хураангуйллыг хэрэгжүүлэхэд тооцооллын нөөц, өгөгдлийн нөөц бага шаарддаг, хураангуйлалд эх текстийн өгүүлбэрийг сонгох ба ямар нэгэн хийсвэрлэл байхгүй нь зарим тохиолдолд зохимжтой жишээлбэл: нийтлэл, шинжлэх ухааны өгүүлэл. Бид экстрактив текст хураангуйллыг хэрэгжүүлэхдээ граф дээр суурилсан TextRank, LexRank, статистик дээр суурилсан TF-IDF алгоритмуудыг ашиглан нэмэлт урьдчилсан боловсруулалтын (preprocessing) phrase болон дараах боловсруулалтын (postprocessing) sentence positioin сайжруулалтуудыг нэмэн хэрэгжүүлэв. Туршилтын үр дүнд тухайн phrase болон sentence position нэмэлт сайжруулалтын давхаргатай үед энгийн үеэс илүү сайн үзүүлэлт гаргасан. Энэхүү судалгаа нь текстийн голлох агуулгыг үр ашигтайгаар гаргаж, текст мэдээлэлтэй харьцдаг текст мэдээлэлтэй ажилладаг бүх хүний цаг хугацааг хэмнэх зорилготой.**

Түлхүүр үг: ***LexRank, TextRank, TF-IDF, mBert, rouge-score, sentence position, phrase***

I. УДИРТГАЛ

Орчин үеийн мэдээллийн эрин зуунд асар их хэмжээний текст мэдээлэл өдөр бүр үүсэж, хуримтлагдсаар байна. Энэ их мэдээллийн урсгалаас хэрэглэгчдэд богино хугацаанд гол санаа, үндсэн агуулгыг нь хүргэх шаардлага өсөн нэмэгдэж байна. Текст хураангуйлал нь энэ асуудлыг шийдвэрлэх үр дүнтэй арга замын нэг юм. Үүнийг хийсвэр (abstractive) болон экстрактив (extractive) гэсэн хоёр аргаар хэрэгжүүлэх боломжтой. Монгол хэл дээрх өгөгдлийн хомс байдал, мөн хийсвэр хураангуйллын хувьд өмнө нь сургагдсан загваруудыг нутагшуулах, техник хангамжийн хязгаарлагдмал байдал зэрэг нь тодорхой хүндрэлтэй тул бид судалгаандаа экстрактив хураангуйллыг түлхүү ашиглаж, Монгол хэл дээр текст хураангуйллыг үр ашигтай хэрэгжүүлэх боломжийг судалсан.

Нэгт экстрактив хураангуйлах арга нь эх бичвэрийн агуулгыг өөрчлөхгүйгээр, эх текстээсээ шууд өгүүлбэрүүдийг сонгож хураангуйлдаг ба ямар нэгэн хийсвэрлэл, товчлол агуулдаггүй тул хэрэглэгчдэд эх мэдээллийг найдвартай хүргэдэг. Жишээлбэл албаны баримт бичиг, эрдэм шинжилгээний өгүүлэл гэх мэт албан ёсны найруулгатай текстүүдийн гол санаа, өгүүлбэр, үгийг өөрчлөхгүй өөрийн байгаагаар нь хураангуйг гаргадгаараа давуу тал болж байна.

Хоёрт энэхүү арга нь хийсвэр хураангуйлах (abstractive text summarization) аргатай харьцуулбал тооцооллын бага нөөц шаардах ба энгийн хялбар хэрэглээнд хэрэглэхэд илүү тохиромжтой байдлаараа давуу талтай. Гэсэн хэдий ч, экстрактив хураангуйллын үр дүнгийн чанар нь ашигласан алгоритм, оновчлолын аргачлалаас хамаарч өөр өөр байж болно. Иймд, бид судалгаандаа Монгол хэлний онцлогт тохирсон экстрактив хураангуйллын аргыг боловсруулж, үр дүнг тодорхойлохыг зорьсон бөгөөд улмаар хэрэглэгчдэд хэрэгтэй мэдээллийг оновчтой, үр дүнтэй хүргэхэд чиглэгдэж байна.

Энэхүү судалгааны ажил нь дараах гол асуудлуудыг авч үзнэ:

1. Экстрактив хураангуйллын аргачлал, алгоритмуудын харьцуулалт
2. Монгол хэлэнд тохирох оновчтой аргыг сонгон турших, үр дүнг үнэлэх
3. Тухайн домэйнд тохирсон аргуудыг тодорхойлох

Ингэснээр бид Монгол хэл дээрх мэдээллийн боловсруулалтын судалгаанд хувь нэмэр оруулахын зэрэгцээ экстрактив хураангуйллын практик хэрэглээг сайжруулах боломжтой болно.

II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Монгол хэл дээрх текст хураангуйллын зорилго нь их хэмжээний текст өгөгдлөөс гол утга санааг алдагдуулалгүйгээр товч, тодорхой байдлаар хураангуйлан гаргаж авах явдал юм. Текст хураангуйллын олон төрлийн арга байдаг бөгөөд [1]-д хамгийн түгээмэл хэрэглэгддэг TF-IDF,

TextRank, LexRank, мөн урьдчилсан сургагдсан загваруудыг ашиглах талаар өгүүлсэн.
Мөн [2]-д өгөгдлийн урьдчилан боловсруулах аргачлал, түүнээс гол утга агуулсан өгүүлбэрүүдийг сонгох тухай судалгаа хийгдсэн. Харин [3]-[5] судалгааны ажлуудад Монгол хэлтэй ижил бага хэмжээний өгөгдлийн сантай хэлнүүдэд дээрх аргууд хэрхэн үр дүнтэй хэрэгжсэнийг нарийвчлан судалсан. Ихэнх текст хураангуйллын судалгаа нь Англи болон бусад олон хэрэглэгчтэй хэл дээр хийгдсэн байдаг боловч бага хэрэглэгчтэй хэлнүүд дээр үр дүнтэй хэрэгжсэн нь Монгол хэлэнд ч амжилттай ашиглах боломжтойг харуулж байна.

Эдгээр судалгааны ажлуудыг үндэслэн, бид Монгол хэлний мэдээний өгөгдлийг ашиглан текст хураангуйллын аргуудыг харьцуулан судалж, аль арга нь хамгийн үр дүнтэй болохыг тодорхойлох зорилготой байна.

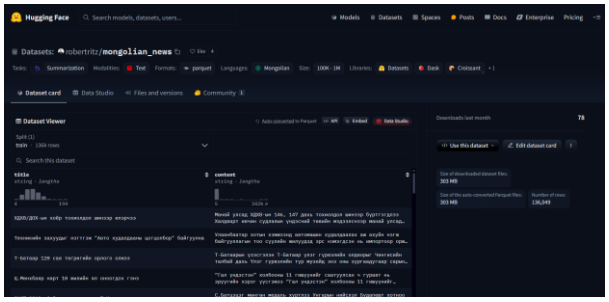
III. АШИГЛАСАН АРГА

3.1 Тестийн өгөгдлийн багц

Бид судалгааны ажлынхаа үр дүнг хэмжихдээ rouge-score хэмжүүрээр хэмжсэн ба өөрсдийн хэрэгжүүлсэн аргуудын гүйцэтгэлийг үнэлэх зорилгоор мэдээ, эрдэм шинжилгээний өгүүлэл, цахим орчны пост өгөгдлийн багц тус бүрийг үүсгэсэн.

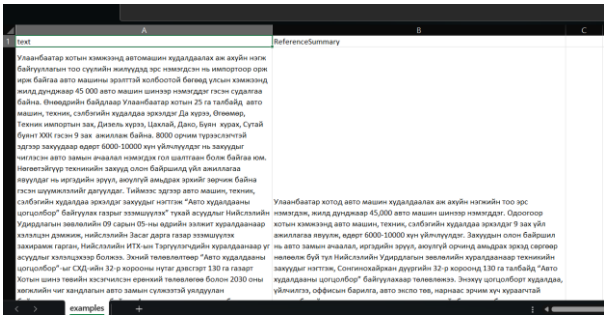
3.1.1 Мэдээний өгөгдлийн багц

Мэдээний агуулгатай өгөгдлийн багцыг бэлтгэхдээ hugging face дээрх монгол хэл дээрх мэдээний Өгөгдлийн багцаас санамсаргүйгээр 10 жишээ авсан.



1 – р зураг. Hugging Face дээрх мэдээний өгөгдлийн багц

HuggingFace дээрх өгөгдлийн багц нь content, title гэсэн атрибутуудтай бөгөөд бид content атрибутын утгуудыг авч тестийн өгөгдлийн багцын оролтын текст болгон ашигласан.

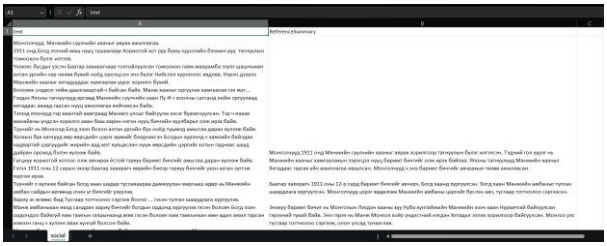


2 – р зураг. Мэдээний өгөгдлийн багц

Дараах зурагт бидний бэлдсэн мэдээний өгөгдлийн багцын харагдах байдлыг харуулав.

3.1.2 Цахим орчны өгөгдлийн багц

Цахим орчны өгөгдлийн багцыг бэлтгэхдээ бид X, Facebook платформуудыг ашиглан пост нийтлэлийг оролтын текст болгон ашигласан.



3 – р зураг. Цахим орчны өгөгдлийн багц

3.1.3 Эрдэм шинжилгээний өгүүллийн өгөгдлийн багц

Эрдэм шинжилгээний өгөгдлийн багцыг бэлдэхдээ ШУТИС Мэдээлэл холбоо технологийн сургуулийн эрдэм шинжилгээний эмхэтгэлээс эрдэм шинжилгээний өгүүллүүдийг оролтын текст болгон ашигласан.

4 – р зураг. Эрдэм шинжилгээний өгүүллийн өгөгдлийн багц

Rouge score үнэлгээний арга нь тухайн текстийн лавлагаа (reference) хураангуйг хэрэгжилтийн загварын гаргасан хураангуйтай харьцуулж үнэлгээ хийнэ. Өгөгдлийн багц бүр дээр лавлагаа хураангуйг бэлтгэхдээ хэлний мэргэжилтнээр тухайн текстийн хураангуйг тодорхойлбол илүү сайн хураангуй гарах боловч цаг хугацаа болон, санхүүгийн нөөц шаардана.

Тиймээс бид лавлагаа хураангуйг бэлтгэхдээ хиймэл оюун ухааныг ашигласан. CHAT GPT LLM нь Монгол хэл дээрх гүйцэтгэл нь сүүлийн үед маш сайжирсан бөгөөд туршилтаар өөрсдийн тодорхойлсон хураангуй болон CHAT GPT – ийн тодорхойлсон хураангуйг харьцуулахад CHAT GPT нь лавлагаа хураангуйг илүү сайн тодорхойлсон. Ингэснээрээ бидэнд тодорхой хэмжээний цаг хугацаа хэмнэхэд тусалсан.

1 – Р ХҮСНЭГТ. ӨГӨГДЛИЙН БАГЦЫН ХЭМЖЭЭС

Өгөгдлийн багцын нэр	Баганын тоо	Мөрийн тоо
News	2	10
Paper	2	10
Social	2	10

Дээрх хүснэгтэд бидний бэлтгэсэн нийт тестийн өгөгдлийн багцын хэмжээснүүдийг харуулж байна.

3.2 Өгөгдлийн урьдчилсан боловсруулалт

Текст өгөгдлийг хураангуйлах үйл явцыг үр дүнтэй гүйцэтгэхийн тулд өгөгдлийг эхлээд урьдчилан боловсруулж, стандартчилах шаардлагатай. Өгөгдлийн урьдчилсан боловсруулалт нь анхны түүхий өгөгдлийг ашиглахад тохиромжтой, боловсруулсан хэлбэрт хувиргах үйл явц юм. Энэ нь өгөгдлийн чанарыг сайжруулж, боловсруулалтын нарийвчлалыг нэмэгдүүлэх ач холбогдолтой.

Уг үйл явц нь дараах үндсэн үе шатуудыг агуулна:

- Нормалчлах (Normalization) - Энэ нь текстийг стандарт хэлбэрт оруулж, боловсруулахад хялбар болгох үйл явц юм. Үүнд том жижиг үсгийн ялгааг арилгаж жижиг тэмдэгт рүү хувиргах, илүүдэл хоосон зай, цэг тэмдэгтүүдийг стандартчилах зэрэг алхмууд багтана.
- Токенжуулалт (Tokenization) - Текстийг үг, өгүүлбэр зэрэг жижиг хэсгүүдэд хуваах процесс. Энэ өгөгдлийг цааш боловсруулахад хялбар болгодог.
- Зогсоц үгийг хасах - “ба”, “болон”, “юм” гэх мэт утга агуулгын хувьд ач холбогдол багатай үгсийг хасах. Энэ нь өгөгдлийг оновчтой боловсруулалтад тусалдаг. Монгол хэлэнд зогсоц үгийн сан одоогоор байхгүй тул бид өөрсдийн судалгаанд хэрэглэх зорилгоор бага хэмжээний зогсоц үгийн сан үүсгэн хэрэглэсэн болно.

Эдгээр алхмуудыг хэрэгжүүлснээр өгөгдлийн хураангуйлах процесс илүү үр дүнтэй явагдаж, боловсруулсан мэдээлэл илүү чанартай, оновчтой болж, цаашдын боловсруулалт, анализ хийхэд тохиромжтой болно.

3.3 Өгүүлбэрийн ач холбогдлыг тооцоолох алгоритмууд

3.3.1 TF-IDF (Term frequency - Inverse document frequency)

TF-IDF нь эх хэлний боловсруулалтад ашигладаг статистик хэмжүүр бөгөөд тодорхой баримт бичиг дэх үгсийн ач холбогдлыг үнэлэхэд хэрэглэдэг. Энэхүү хэмжүүр нь тухайн бичиг баримт дахь давтамж болон нийт баримт бичгийн сан дахь ховор эсэхийг харгалзан үгийн ач холбогдлыг тодорхойлдог.

TF-IDF нь дараах томьёогоор илэрхийлэгдэнэ:
TF-IDF(t, d, D) = TF(t, d) x IDF(t, D).
TF(t, d) нь тухайн t үгийн d баримт бичиг доторх давтамж бөгөөд дараах томьёогоор илэрхийлэгдэнэ:

$$TF(t,d) = \frac{f_{t,d}}{\sum_{t'}^{d} f_{t',d}}$$

Энд $TF(t,d)$ нь тухайн t үгийн d баримт бичиг дэх давтамжийг илэрхийлнэ.

IDF(t, D) нь тухайн үг нийт баримт бичгийн санд хэр ховор байгааг хэмжих үзүүлэлт бөгөөд дараах томьёогоор тодорхойлогдоно:

$$TF(t,d) = log\left(\frac{|D|}{1 + |\{d \in D : t \in d\}|}\right)$$

Энд:

- $|D|$ нь нийт баримт бичгийн тоо.
- $|\{d \in D : t \in D\}|$ нь тухайн үг орсон баримт бичгийн тоо.

TF-IDF алгоритм нь олон болон бага давтамжтай үгсийг тодорхойлох замаар текстийн онцлог шинж, утга санааг илэрхийлсэн үг болон өгүүлбэрүүдийг илрүүлэхэд ашигладаг.

3.3.2 TextRank

TextRank алгоритм нь граф суурьтай үнэлгээний алгоритм бөгөөд эх хэлний боловсруулалтад текстийн хураангуй үүсгэх, түлхүүр үг тодорхойлох, өгүүлбэрийн ач холбогдлыг үнэлэх зэрэгт ашигладаг. Энэ алгоритм нь Google-ийн PageRank алгоритм дээр суурилж бүтээгдсэн бөгөөд текст дэх өгүүлбэрүүдийг граф байдлаар дүрслэн, тэдгээрийн хоорондын холбоог үнэлж, хамгийн чухал өгүүлбэрүүдийг тодорхойлох зарчмаар явагддаг.

TextRank алгоритмын үндсэн үе шатууд:

1. Граф үүсгэх - Текстийн өгүүлбэрүүдийг зангилаа (node) болгон тодорхойлж, тэдгээрийн

хоорондын холбоог ирмэг (edge) хэлбэрээр илэрхийлнэ.

2. Өгүүлбэр хоорондын ижил төстэй байдлыг тооцоолох - Өгүүлбэрүүдийн утгын ойролцоо байдлыг хэмжиж, ижил төстэй өгүүлбэрүүдийг харилцан холбох замаар граф үүсгэнэ.
3. PageRank алгоритмыг хэрэгжүүлэх - Граф дээр PageRank алгоритмыг ашиглаж, өгүүлбэрүүдийн ач холбогдлын оноог тооцоолно.
4. Өгүүлбэрүүдийг сонгох - Текстийн хураангуйд оруулах өгүүлбэрүүдийн хамгийн өндөр оноотой өгүүлбэрүүдээс сонгож, гарган авна.

Ингэснээр текст өгөгдлөөс өндөр оноо бүхий гол өгүүлбэрүүдийг ялгаж хураангуйг үүсгэдэг.

3.3.3 LexRank

LexRank нь граф суурьтай эх хэлний боловсруулалтад ашигладаг алгоритм юм. Энэ нь өгүүлбэрүүдийн харилцан хамаарлыг графын тусламжтайгаар үнэлж, хамгийн чухал өгүүлбэрүүдийг тодорхойлох замаар текстийн хураангуй үүсгэдэг. LexRank нь PageRank алгоритмтай төстэй бөгөөд өгүүлбэрүүдийг зангилаа (node) болгон авч, тэдгээрийн хоорондох холбоог ирмэг (edge) хэлбэрээр дүрсэлдэг.

Энэхүү алгоритмын үндсэн зарчим нь өгүүлбэрүүдийн ижил төстэй байдлыг тооцоолж, тэдгээрийн хоорондын холбогдлыг тодорхойлох явдал юм. Өгүүлбэр хоорондын ижил төстэй байдал нь косинусын ижил төстэй байдлын хэмжүүр (cosine similarity) ашиглан тооцоологддог.

LexRank алгоритм нь дараах үндсэн үе шатуудтай:

1. Өгүүлбэр хоорондын ижил төстэй байдлыг тооцоолох

$$sim(S_i, S_j) = \frac{V_i \cdot V_j}{\left||V_i| \times |V_j|\right|}$$

S - өгүүлбэрүүд, V - өгүүлбэрүүдийн вектор илэрхийлэл

2. Граф бүтээх

- Өгүүлбэрүүдийг зангилаа болгон авч, ижил төстэй байдлын босго утгаас өндөр тохиолдолд хооронд нь холбож, жинг (weight) тооцоолно.
- Холбоосны жинг дараах томьёогоор тодорхойлдог.

$$\omega_{ij} = \begin{cases} sim(S_i, S_j), \text{ хэрэв } sim(S_i, S_j) > r \\ 0, \text{ бусад тохиолдолд} \end{cases}$$

Энд r нь босго утга.

3. PageRank-ийн зарчмаар оноог тооцоолох

$$PR(S_i) = (1 + d) + d \sum_{S_k}^{adj(S_i)} \frac{\omega_{ij \times PR(S_j)}}{\sum_{S_k}^{adj(S_j)} \omega_{jk}}$$

4. Өгүүлбэрүүдийг сонгох

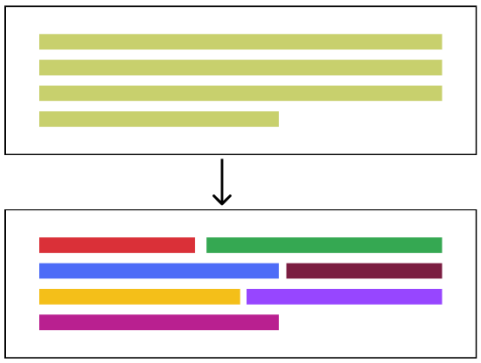
- PageRank онооны дагуу өгүүлбэрүүдийг эрэмбэлж, хамгийн өндөр оноотой өгүүлбэрүүдийг хураангуйд оруулна

3.4 Нэмэлт сайжруулалт

3.4.1 **Phrase** урьдчилсан боловсруулалтын (*preprocessing*) сайжруулалтын давхарга

Бидний нэмэлтээр хэрэгжүүлсэн phrase сайжруулалтын давхарга нь 3.2-т заасан урьдчилсан боловсруулалтын алхмууд хэрэгжсэн текст өгөгдөлд боловсруулалт хийх буюу таслалаар холбогдсон нийлмэл өгүүлбэрүүдийг тус бүрд нь дахин өгүүлбэрүүдэд хуваах үүрэгтэй.

Ингэснээр нийлмэл өгүүлбэрт буй текстийн агуулгад нөлөө ихтэй гишүүн өгүүлбэрийг илүү нарийвчлалтайгаар ялган авах давуу талтай.

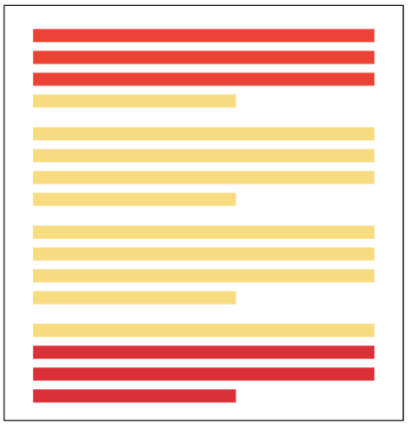


5 – р зураг. Phrase давхаргын хэрэгжилтийн жишээ

3.4.2 **Sentence position** дараах боловсруулалтын (*postprocessing*) сайжруулалтын давхарга

Өгүүлбэрийн ач холбогдлыг тооцоолох алгоритмын гаралтад нэмэлтээр оруулж буй сайжруулалтын давхарга болох sentence position нь [6] – д дурдсаны дагуу ихэнх текстэд өгөгдлийн хувьд жишээлбэл: эрдэм шинжилгээний өгүүлэл, мэдээ, нийтлэлүүдийн цөм утга санааг агуулах өгүүлбэрүүд нь нийт текстийн эхлэл болон төгсөл хэсэгт байршдаг гэсэн үндэслэл дээр үндэслэн өгүүлбэрийн байршлыг (sentence position) онцолж, дараах боловсруулалтын (postprocessing) сайжруулалтын давхаргыг хэрэгжүүлсэн.

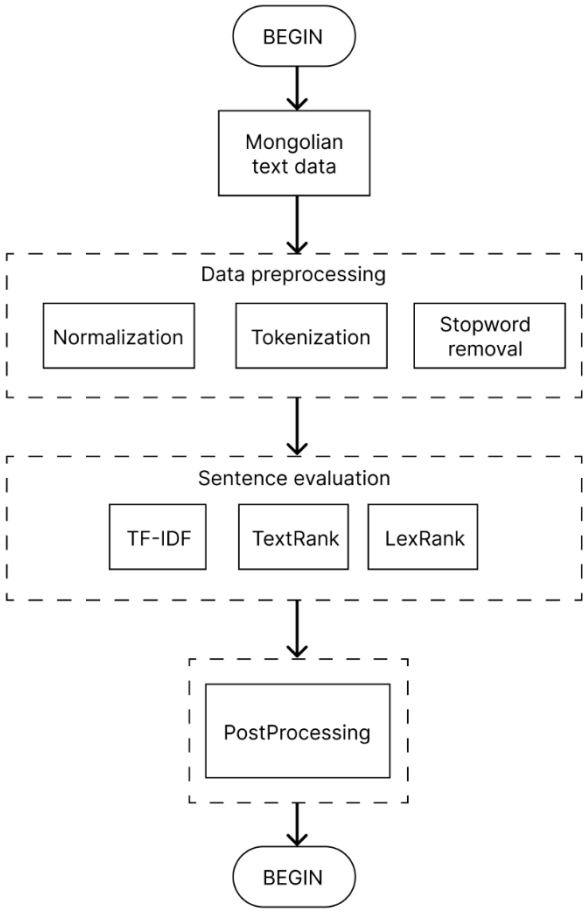
Sentence position нь хэрэгжихдээ оролтын текстийн эхний болон сүүлийн 20% - д, нийт өгүүлбэрийг ямар нэгэн үнэлгээний алгоритм үнэлсний дараа нэмэлт оноо өгөх зарчмаар хэрэгжинэ.
Жишээлбэл: загвар луу нийт 10 өгүүлбэртэй текст өгөгдөл оруулахад эхний болон, сүүлийн 2 өгүүлбэр дээр нэмэлт оноо өгөх юм.



6 – р зураг. Sentence position давхаргын хэрэгжилтийн жишээ

3.5 Хэрэгжүүлсэн загваруудын бүрэлдэхүүн хэсгүүд

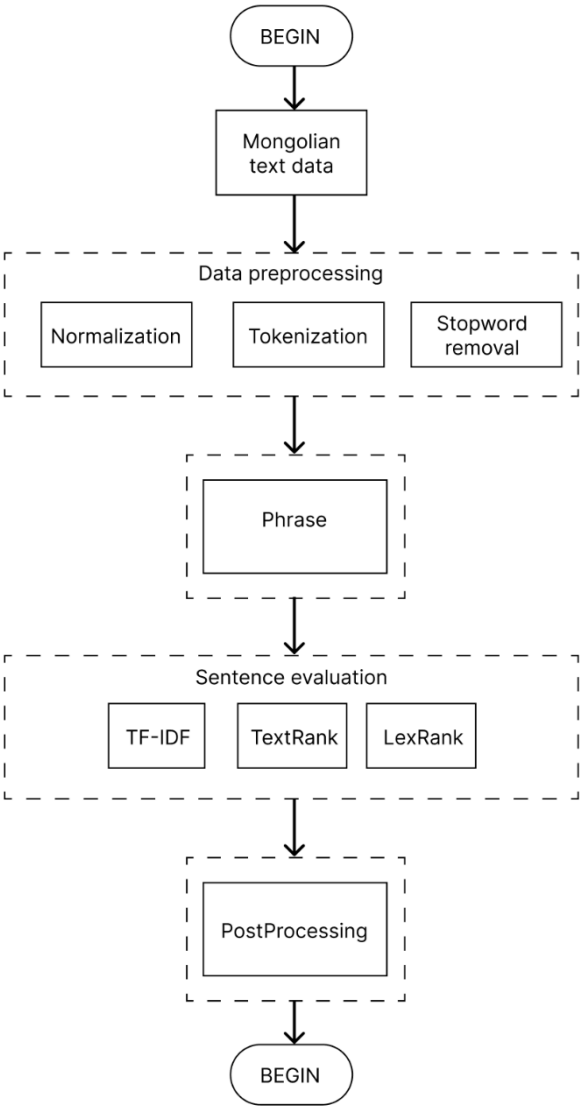
Энэхүү судалгааны ажлын хүрээнд бид TF-IDF, TextRank, LexRank алгоритмуудыг өөрөөр нь болон өөрсдийн нэмэлт сайжруулалтын давхарга нэмэн хэрэгжүүллээ.



7- р зураг. Нэмэлт давхаргүй хэрэгжилтийн бүрэлдэхүүн хэсгүүд

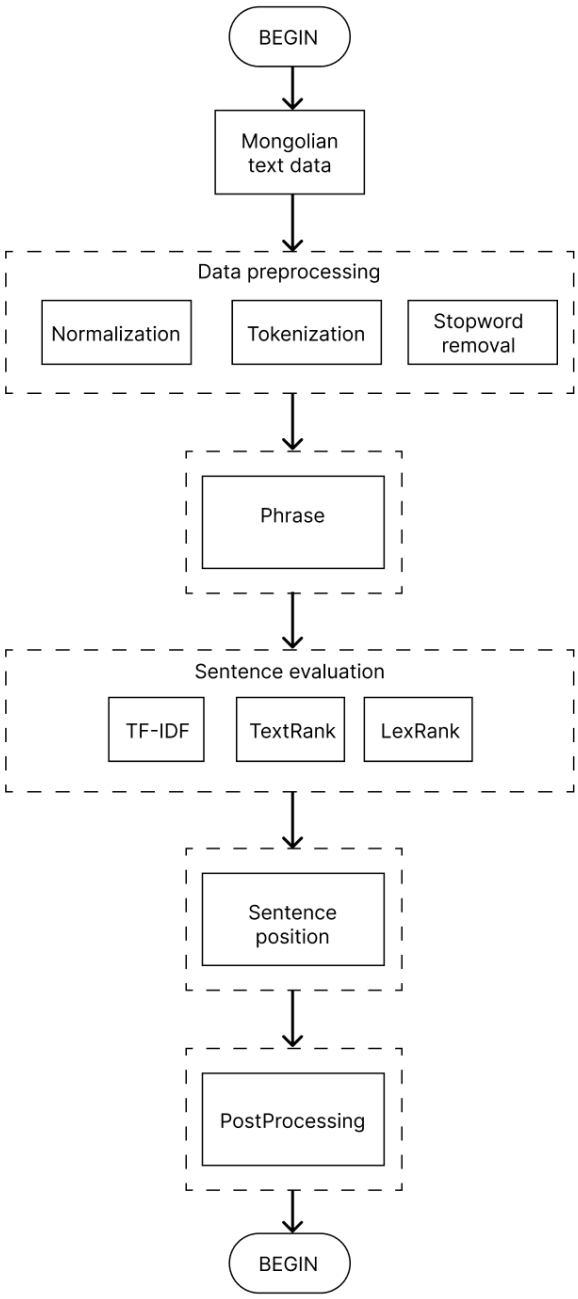
Дараах зурагт хэрэгжүүлж буй загварууд нь ямар нэгэн нэмэлт сайжруулалтын давхаргүй хэрэгжүүлэх үеийн загварын бүрэлдэхүүн хэсгүүдийг харуулж байх бөгөөд энд TF-IDF, LexRank, TextRank алгоритм тус бүр дээр тус тус нэг хэрэгжилт байна.

Эдгээр нэмэлт сайжруулалтын давхаргүй загваруудыг үндсэн загвар гэж үзэх бөгөөд, үндсэн загвартай өөрсдийн нэмж оруулж буй сайжруулалтын давхаргатай загваруудыг гүйцэтгэл болон үзүүлэлтээр нь харьцуулах зорилготой ашиглах юм.



8 – р зураг. Phrase нэмэлт сайжруулалтын давхаргатай хэрэгжилтийн бүрэлдэхүүн хэсгүүд

Дээрх зурагт өмнөх хэрэгжүүлсэн загвар дээр phrase нэмэлт сайжруулалтын давхарга оруулан хэрэгжүүлэх үеийн загварын бүрэлдэхүүн хэсгүүдийг харуулж байна. Мөн алгоритм тус бүр дээр тус тус нэг загвар хэрэгжинэ.



9 – р зураг. Phrase болон Sentence position сайжруулалтын давхаргатай хэрэгжилтийн бүрэлдэхүүн хэсгүүд

Энэхүү зурагт үндсэн загвар дээр phrase болон sentence position сайжруулалтын давхаргуудыг нэмж оруулсан үеийн загварын бүрэлдэхүүн хэсгүүдийг харуулж байна. Мөн адил алгоритм тус бүр дээр тус тус нэг загвар хэрэгжинэ.

3.6 Үнэлгээний аргачлал

ROUGE score (Recall-Oriented Understudy for Gisting Evaluation) нь текст хураангуй болон машин орчуулга зэрэг автомат үнэлгээний системүүдийг шалгахад өргөн хэрэглэгддэг үнэлгээний хэмжүүр юм. Энэ хэмжүүр нь лавлах хураангуй болон алгоритмын хураангуй хоорондох ижил төстэй байдлыг хэмжиж үнэлдэг.

ROUGE score тооцоолохдоо ихэвчлэн recall (буцаалт), precision (нарийвчлал) болон F1-score гэсэн үзүүлэлтүүдийг ашигладаг.

- Recall нь лавлах хураангуйн хэдэн хувь нь алгоритмын үүсгэсэн хураангуйд багтсан эсэхийг илэрхийлнэ.
- Precision нь лавлах хураангуйн доторх мэдээллээс алгоритмын хураангуйтай хэр зэрэг таарч буйг хэмжинэ.
- F1-score нь recall болон precision-ийн дундаж утгыг харуулдаг.

Rouge score нь дараах төрлүүдтэй байна:

1. Rouge-1 нь нэг үгийн (unigram) давхцалыг хэмждэг үзүүлэлт юм.
2. Rouge-2 нь хоёр үгийн дараалал (bigram) 2 үгийн давхцалыг хэмждэг үзүүлэлт юм.
3. Rouge-L нь Longest common subsequence (LCS) буюу хураангуйн хамгийн урт нийтлэг дарааллыг тодорхойлох замаар үнэлгээ хийдэг.

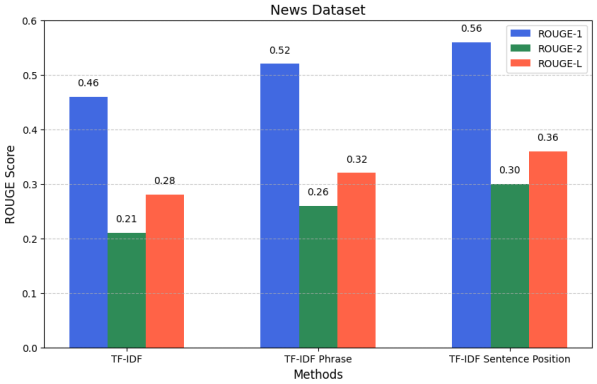
IV. ҮР ДҮН

Бид экстрактив текст хураангуйллын хүрээнд TF-IDF, TextRank, LexRank алгоритмуудыг өөрсдийн тодорхойлсон нэмэлт сайжруулалтын давхаргаар баяжуулж хэрэгжүүллээ.

2 – Р ХҮСНЭГТ. ХЭРЭГЖҮҮЛСЭН АРГУУД

TF-IDF			
		Давхарга 1	Давхарга 2
1	TF-IDF		
2	TF-IDF	Phrase	
3	TF-IDF	Phrase	Sentence
TextRank			
		Давхарга 1	Давхарга 2
1	TextRank		
2	TextRank	Phrase	
3	TextRank	Phrase	Sentence
LexRank			
		Давхарга 1	Давхарга 2
1	LexRank		
2	LexRank	Phrase	
3	LexRank	Phrase	sentence

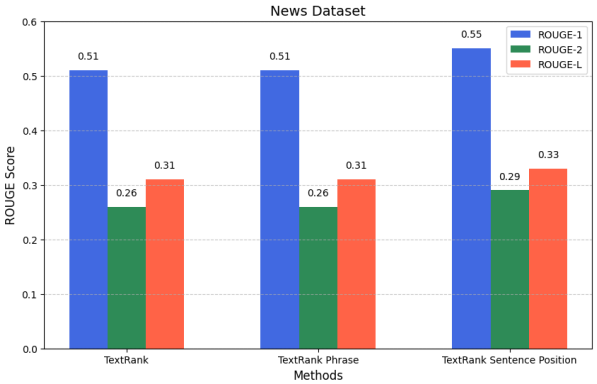
4.1 Мэдээний өгөгдлийн багц дээрх загваруудын үр дүнгүүд



10 – р зураг. Мэдээний өгөгдлийн багц дээрх TF-IDF загваруудын үр дүнгүүд

10 – р зурагт үзүүлснээр мэдээний өгөгдлийн багц дээр TF-IDF sentence position загвар нь хамгийн үр дүнтэй буюу rouge score 0.56 байна.

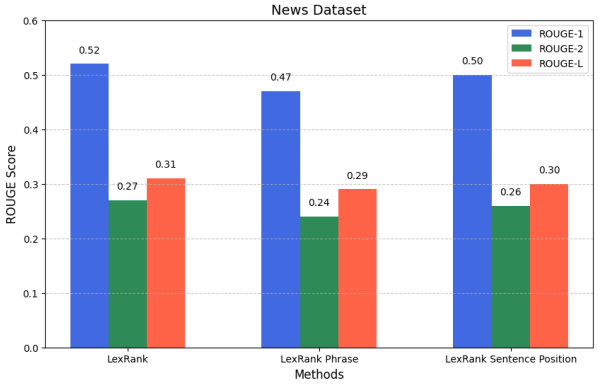
Мөн TF_IDF алгоритм дээр сайжруулалтын давхарга нэмэх бүрд rouge score нь өссөн харагдаж байна. Энэ нь өгүүлбэрийн байршил болон нийлмэл өгүүлбэрт буй гишүүн өгүүлбэрүүдийг тус бүрд өгүүлбэр болгон авсан нь хураангуй илүү нарийвчлалтай болж байгааг илэрхийлж байна.



11 – р зураг. Мэдээний өгөгдлийн багц дээрх TextRank загваруудын үр дүнгүүд

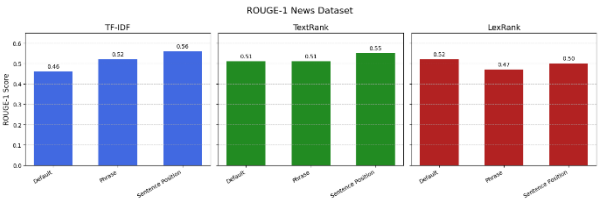
11 – р зурагт үзүүлснээр мэдээний өгөгдлийн багц дээр TexRank алгоритм давхарга нэмэх бүрд үзүүлэлт бууураагүй байна.

Мөн TextRank sentence position арга хамгийн өндөр буюу rouge score нь 0.55 байна.



12 – р зураг. Мэдээний өгөгдлийн багц дээрх LexRank загваруудын үр дүнгүүд

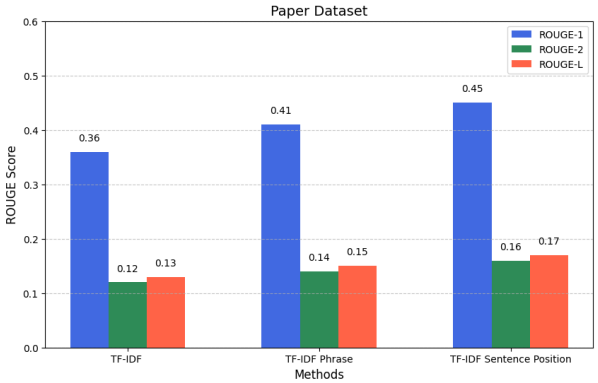
12 – р зураг харуулснаар LexRank алгоритм дээр phrase сайжруулах давхарга нэмсэн тохиолдолд үзүүлэлт буурсан боловч sentence position давхарга нэмэлтээр орсон үед өссөн байна. Гэвч 2 нэмэлт давхарга нь үндсэн (default) LexRank – тай харьцангуй бага үзүүлэлт үзүүлсэн байна.



13 – р зураг. Мэдээний өгөгдлийн багц дээрх нийт загваруудын үр дүнгүүд

13 – р зураг харуулснаар мэдээний өгөгдлийн багц дээр нийт хэрэгжүүлсэн загваруудыг харьцуулж гаргасан бөгөөд загвар тус бүр дээр sentence position сайжруулалтын давхарга нэмсэн үед тодорхой хэмжээнд үзүүлэлт өссөн үзэгдэл ажиглагдаж байна.

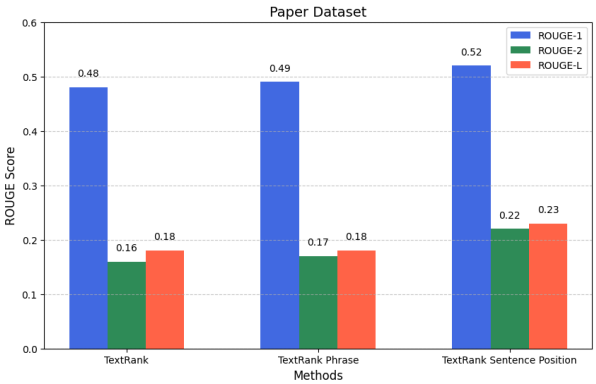
4.2 Эрдэм шинжилгээний өгөгдлийн багц дээрх загваруудын үр дүнгүүд



14 – р зураг. Эрдэм шинжилгээний өгөгдлийн багц дээрх TF-IDF загваруудын үр дүн

14 – р зураг харуулснаар эрдэм шинжилгээний өгөгдлийн багц дээр TF-IDF sentence position нь хамгийн өндөр үзүүлэлтийг үзүүлсэн байна.

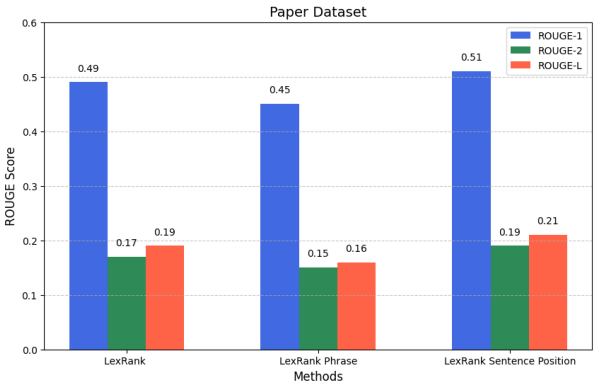
Өмнөх мэдээний өгөгдлийн багцын үр дүнгийн шинж чанартай адилаар үндсэн алгоритм дээр сайжруулалтын давхарга нэмэх бүрд үзүүлэлт нь ахисан байна.



15 – р зураг. Эрдэм шинжилгээний өгөгдлийн багц дээрх TextRank загваруудын үр дүнгүүд

15 – р зураг үзүүлснээр TextRank sentence position эрдэм шинжилгээний өгөгдлийн багц дээр хамгийн өндөр үзүүлэлт буюу rouge score нь 0.52 байна.

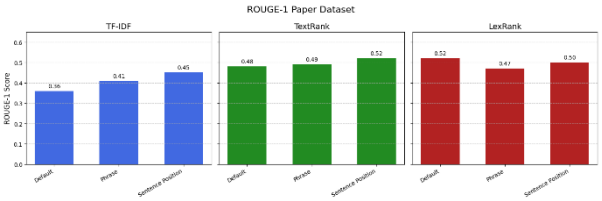
Мэдээний өгөгдлийн багц дээрх үр дүнтэй адил алгоритм дээр сайжруулалтын давхарга нэмэх бүрд өссөн байна.



16 – р зураг. Эрдэм шинжилгээний өгөгдлийн багц дээрх LexRank загваруудын үр дүнгүүд

16 – р зураг харуулснаар эрдэм шинжилгээний өгүүллийн өгөгдлийн багц дээр LexRank sentence position нь хамгийн өндөр үзүүлэлт буюу rouge score нь 0.51 байна.

Үзүүлэлтийн шинж чанарыг хувьд phrase сайжруулалтын давхарга нэмсэн үед үндсэн алгоритмын үр дүнгээс үзүүлэлт нь буурсан боловч sentence position сайжруулалтын давхарга орсон тохиолдолд өссөн байна.

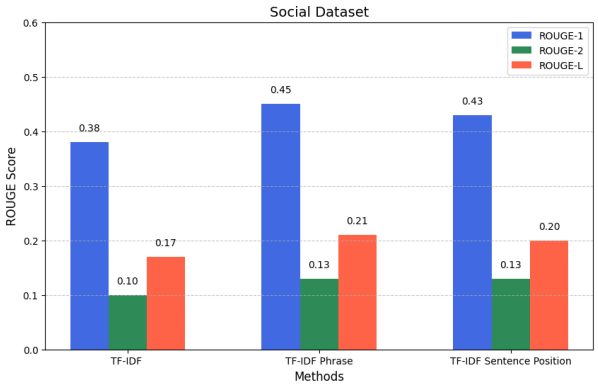


17 – р зураг. Эрдэм шинжилгээний өгөгдлийн багц дээрх нийт загваруудын үр дүнгүүд

17 – р зурагт үзүүлснээр эрдэм шинжилгээний өгөгдлийн багц дээр нийт хэрэгжүүлсэн загваруудын үзүүлэлтүүдийг харьцуулж гаргасан.

Мэдээний өгөгдлийн багц дээр үр дүнтэй ижил TF-IDF, TextRank суурьтай загваруудад сайжруулалтын давхарга нэмэх тохиолдол бүрд үзүүлэлт өссөн бол LexRank суурьтай загваруудад phrase сайжруулалтын давхарга нэмсэн тохиолдолд үндсэн загварын үзүүлэлтээс буурж, sentnce position сайжруулалтын давхарга нэмэхэд эргээд үзүүлэлт өссөн ижил шинж чанар ажиглагдаж байна.

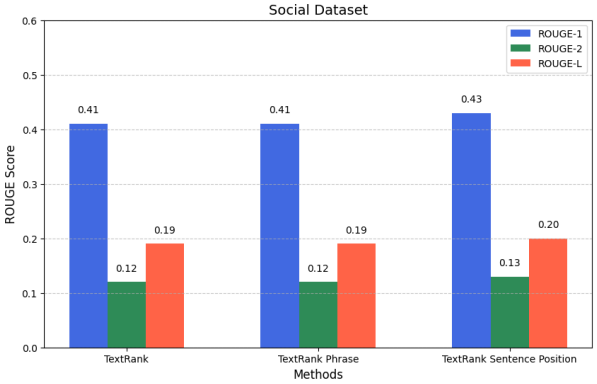
4.3 Цахим орчны өгөгдлийн багц дээрх загваруудын үр дүнгүүд



18 – р зураг. Цахим орчны өгөгдлийн багц дээрх TF-IDF загваруудын үр дүнгүүд

18 – р зурагт үзүүлснээр цахим орчны текст өгөгдлийн багц дээр TF-IDF phrase загвар хамгийн өндөр үзүүлэлтийг үзүүлсэн буюу rouge score нь 0.45 байна.

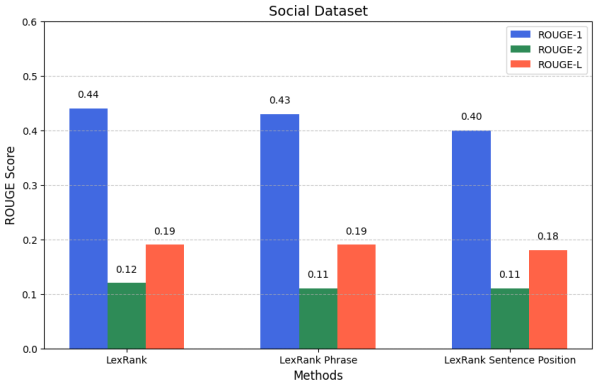
Загваруудын үзүүлэлтийн шинж чанарын хувьд phrase сайжруулалтын давхарга дээр өсөж sentence position сайжруулалтын давхарга нэмсэн үед буурч байна. Мөн өмнөх өгөгдлийн багцуудаас өөр шинж чанартай байна.



19 – р зураг. Цахим орчны өгөгдлийн багц дээрх TextRank загваруудын үр дүнгүүд

19 – р зурагт харуулснаар цахим орчны өгөгдлийн багц дээр TextRank sentence position нь хамгийн өндөр үзүүлэлтийг үзүүлсэн байна.

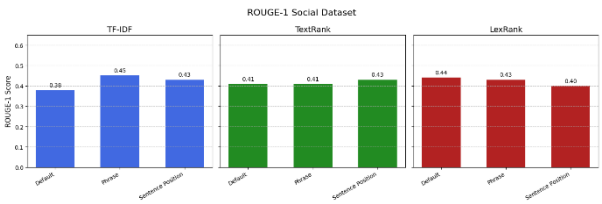
Харин загваруудын үзүүлэлтийн шинж чанаруудын хувьд sentence position сайжруулалтын давхарга нэмсэн тохиолдолд өсөж бусад тохиолдолд хэвийн байгаа бөгөөд мэдээний өгөгдлийн багц дээрх гаргасан үзүүлэлттэй ижил шинж чанартай байна.



20 – р зураг. Цахим орчны өгөгдлийн багц дээрх LexRank загваруудын үр дүнгүүд

20 – р зурагт үзүүлснээр цахим орчны өгөгдлийн багц дээр LexRank (default) нь хамгийн өндөр үзүүлэлт үзүүлсэн байна.

Энэ удаад өмнөх үзэгдлүүдээс эсрэг үзэгдэл гарсан бөгөөд сайжруулалтын давхарга нэмсэн тохиолдол бүрд үзүүлэлт буурсан эсрэг үзэгдэл гарсан байна.



21 – р зураг. Цахим орчны өгөгдлийн багц дээрх нийт загваруудын үр дүнгүүд

21 – р зурагт харуулснаар цахим орчны өгөгдлийн багц дээрх нийт хэрэгжүүлсэн загваруудын үзүүлэлтийг харьцуулав.

Үзүүлэлтийн шинж чанарын хувьд өмнөх 2 өгөгдлийн багц дээр гарсан үзэгдлээс өөр үзэгдэл гарсан байна. Жишээлбэл: LexRank алгоритм дээр сайжруулалтын давхарга нэмэх бүрд үзүүлэлт буурсан байна. Харин бусад алгоритмын хувьд sentence position сайжруулалтын давхарга нэмэгдсэн үед өсөлт үндсэн (default) загварын үзүүлэлтээс өссөн үзэгдэл нь хэвээрээ байна.

Цахим орчны өгөгдлийн багц дээр үзүүлэлт буурж байгаа шалтгаан нь цахим орчин дахь нийтлэл нь эрдэм шинжилгээний өгүүлэл болон мэдээтэй адил цэгцтэй, албан ёсны найруулгатай биш учир цахим орчны өгөгдлийн багц дээр үзүүлэлт буурсан гэж үзэж байна.

ДҮГНЭЛТ

Монгол хэлний цахим хэрэглээ нэмэгдэж, мэдээллийн урсгал хурдацтай өсөхийн хэрээр текст хураангуйллын аргуудыг хөгжүүлэх хэрэгцээ улам бүр нэмэгдэж байна. Их хэмжээний мэдээллийг богино хугацаанд боловсруулах шаардлага академик судалгаа, хэвлэл мэдээлэл, цахим орчин, бизнесийн салбар зэрэг олон чиглэлд тулгарч буй гол асуудлуудын нэг болоод байна. Бусад орны олон хэрэглэгчтэй хэл дээр үр ашигтай ажилладаг олон төрлийн текст хураангуйллын алгоритмууд боловсруулагдсан ч Монгол хэлний хувьд үг зүй, өгүүлбэр зүй, бүтэц зэргээс шалтгаалан эдгээр аргуудыг шууд хэрэглэх боломж хязгаарлагдмал байдаг. Иймд Монгол хэлэнд тохирсон, оновчтой хураангуйллын аргуудыг боловсруулах нь чухал ач холбогдолтой юм.

Энэхүү судалгааны ажлын хүрээнд Монгол хэл дээрх экстрактив текст хураангуйллын хэрэгжүүлэлтийг гүйцэтгэлээ. Судалгааны явцад граф өгөгдлийн бүтэц дээр суурилсан TextRank, LexRank алгоритмууд болон статистик аргачлалд тулгуурласан Term Frequency (TF), Inverse Document Frequency (IDF) аргуудыг ашиглан өөрсдийн тодорхойлсон phrase, sentence position сайжруулалтын давхаргуудыг оруулж 9 өөр загварыг хэрэгжүүлсэн болно. Хэрэгжүүлсэн загвараа үнэлж харьцуулахдаа 10 жишээтэй 3 өөр өгөгдлийн багцыг үүсгэж нийт 270 туршилт хийв.

Судалгааны үр дүнг **ROUGE Score** ашиглан үнэлж, нийт хэрэгжүүлсэн 9 загварын дундаж үзүүлэлтийг гаргалаа. Үр дүнгээс харахад:

- Мэдээний хураангуйлалд TF-IDF sentence poistion загвар нь хамгийн өндөр үр дүнг үзүүлэв.
- Цахим орчны текстийн хувьд TF-IDF phrase загвар нь хамгийн өндөр үр дүнг үзүүлэв.
- Эрдэм шинжилгээний өгүүллийн хураангуйлалд TextRank sentence position загвар нь хамгийн өндөр үр дүнг үзүүлэв.

Энэхүү судалгаа нь Монгол хэл дээрх текст хураангуйллын аргуудын үр дүнг харьцуулан судалж, текстийн төрөл бүрд хамгийн тохиромжтой аргачлалыг тодорхойлоход чиглэсэн болно. Цаашлаад нарийвчилсан судалгаа, боловсруулалт хийхэд чухал суурь болох боломжтойг харуулж байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Shimpikar, Sheetal, and Sharvari Govilkar. "A survey of text summarization techniques for Indian regional languages." *International Journal of Computer Applications* 165, no. 11 (2017): 29-33.

[2] Gupta, Vishal, and Gurpreet Singh Lehal. "Automatic Punjabi text extractive summarization system." In *Proceedings of COLING 2012: Demonstration Papers*, pp. 191-198. 2012.

[3] Han, Yongshun, Qintu Si, and Siriguleng Wang. "Mongolian Automatic Text Summarization Method Based on Pre-trained Model and Improved TextRank." *Advances in Computer and Communication* 5, no. 2 (2024).

[4] Wijayanti, Rini, Masayu Leylia Khodra, Kridanto Surendro, and Dwi H. Widyantoro. "Learning bilingual word embedding for automatic text summarization in low resource language." *Journal of King Saud University-Computer and Information Sciences* 35, no. 4 (2023): 224-235.

[5] Munaf, Mubashir, Hammad Afzal, Khawir Mahmood, and Naima Iltaf. "Low resource summarization using pre-trained language models." *ACM Transactions on Asian and Low-Resource Language Information Processing* 23, no. 10 (2024): 1-19.

[6] https://web.archive.org/web/20160304045652/http://faculty2.ric.edu/rfeldstein/202_spring_08_files/4.par_ex_4_topic_sentence.pdf

ОРЧИН ҮЕИЙН ВИДЕО КОНТЕНТОД MAXON CINEMA 4D ПРОГРАММЫН ХӨДӨЛГӨӨНТ ГРАФИКИЙН ХЭРЭГЛЭЭ

Золхуягын НАРАНГАРАВ, Ламжавын ЭРДЭНЭБАЯР

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн сургууль, Холбооны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: narkazol37@gmail.com

Хураангуй: **Сүүлийн жилүүдэд дижитал технологи, мультимедиа чиглэлээрх хөгжил хурдацтай нэмэгдэж, видео контентын хэрэглээ огцом өссөн нь график дизайн, хөдөлгөөнт дүрслэлийн технологид шинэ шаардлагыг бий болгож байна. Орчин үед видео контент зөвхөн энгийн дүрс, текстээс гадна 3D хөдөлгөөнт график, VFX эффект, интерактив агуулга бүхий өндөр түвшний бүтээл болон хөгжиж байгаа нэгэн тод жишээ нь Maxon Cinema 4D программ бөгөөд хялбар интерфейс, хүчирхэг хөдөлгөөнт графикийн хэрэгслүүд, динамик гэрэлтүүлэг, физик суурьтай хөдөлгөөн зэрэг олон давуу талтай. Энэхүү судалгааны ажлаар орчин үеийн видео контент бүтээхэд Cinema 4D программын хэрэглээ ямар ач холбогдолтойг судалж, түүний хэрэглээний боломжуудыг тодорхойлох зорилготой. Мөн тус программын тусламжтай хөдөлгөөнт графикийн бүтээлч боломжийг өргөжүүлэх, контент бүтээгчдэд тулгардаг бэрхшээлүүдийг судлахын зэрэгцээ хэрэглээнд нэвтрүүлэх арга замыг тодорхойлсон болно. Түүнчлэн, бодит жишээнүүдэд тулгуурлан Cinema 4D ашиглан бүтээсэн хөдөлгөөнт график контентуудын үр нөлөөг судлах, хэрэглэгчийн хүлээн авах байдлыг үнэлж, цаашдын хөгжүүлэлтийн чиг хандлагыг тодорхойлох болно. Энэ нь зөвхөн контент бүтээгчдэд төдийгүй маркетинг, боловсрол, эрүүл мэндийн салбарт ч чухал ач холбогдолтой юм.**

Түлхүүр үг: ***хөдөлгөөнт график, видео контент, 3D загвар, программ хангамж, динамик симуляци***

I. УДИРТГАЛ

Орчин үеийн дижитал контент үйлдвэрлэл хурдацтай хөгжиж, сошиал медиа, кино үйлдвэрлэл, маркетингийн салбаруудад өргөнөөр хэрэглэгдэж байна. Видео контентын чанар, үзүүлэх нөлөөллийг нэмэгдүүлэх гол хэрэгслүүдийн нэг нь хөдөлгөөнт график буюу motion graphics бөгөөд энэ нь аливаа мэдээллийг сонирхолтой, ойлгомжтой, бүтээлч байдлаар дамжуулах чухал арга хэрэгсэл болж байна. Maxon Cinema 4D программ нь 3D хөдөлгөөнт график бүтээхэд өргөн хэрэглэгддэг мэргэжлийн программ хангамж бөгөөд 3D загварчлал, текстуринг, хөдөлгөөнт эффект, динамик хөдөлгөөн, гэрэлтүүлэг зэрэг олон төрлийн функцээрээ график дизайнерууд, аниматорууд, кино бүтээгчдийн дунд өндөр үнэлгээтэй байдаг.

Хөдөлгөөнт графикийн техник, технологи хурдацтай хөгжихийн хэрээр контент бүтээгчид илүү нарийн, өндөр чанартай, үзэгчдийг татахуйц дүрслэлүүдийг боловсруулах хэрэгцээтэй тулгарч байна. Ялангуяа 3D хөдөлгөөнт график нь уламжлалт 2D графикаас илүү бодит мэдрэмж төрүүлдэг ба үүний нэгэн тод жишээ нь өдгөө кино үйлдвэрлэл гэх том зах зээлийн салшгүй нэгэн том хэсэг болсон байгаагаас харах боломжтой.

Энэхүү судалгаагаар Maxon Cinema 4D-ийн хөдөлгөөнт графикийн гол давуу талуудыг тодорхойлох, видео контент бүтээх явц дахь хэрэглээний онцлогуудыг шинжлэх, бодит кейс судалгаан дээр үндэслэн энэхүү программыг үр дүнтэй ашиглах арга зүйг боловсруулах зорилготой. Үүний тулд Maxon Cinema 4D-ийн хөдөлгөөнт графикийн хэрэгсэл, боломжууд хэрхэн видео контентод хэрэглэгддэг, видео бүтээлийн чанарт хэрхэн нөлөөлдөг, мөн энэхүү программыг ашиглан сошиал медиа, маркетингийн контент, кино үйлдвэрлэлд хэрхэн шинэчлэл хийх боломжтой талаар судална.

Судалгааны ажлын таамаглал:

Энэхүү судалгааны сэдэв нь видео контентын динамик байдал, сонирхол татах чадвар, мэргэжлийн түвшинд хэрхэн нэмэгдүүлж байгааг судалж дүгнэлт хийнэ. Таамаглал нь тус программын уян хатан боломжууд нь контент бүтээгчдэд бүтээлч илэрхийлэл, интерактив байдал, бодит мэдрэмжийг нэмэгдүүлэх замаар хэрэглэгчдийн анхаарлыг илүү үр дүнтэй татах нөхцөл бүрдүүлнэ гэж үзэж байна.

Cinema 4D программын орчин дахь бүтээлийн үйл явц:

- Судалгааны зорилгыг тодорхойлох Видео контентод тохиромжтой хөдөлгөөнт графикийн элементүүдийг сонгох
- Программын үндсэн хэрэгслүүдийг судлах 3D загварчлал, текстуринг, гэрэлтүүлгийн тохиргоог боловсруулах

- Динамик хөдөлгөөн, эффект, анимацийн тохиргоог хийх
- Видео контентод зориулсан нэмэлт хөдөлгөөнт график элементүүдийг загварчлах
- Real time rendering болон post-production тохиргоог хийх
- Бэлэн болсон хөдөлгөөнт графикийг видео контентод интеграцлах
- Туршин засварлах, оновчлох, хэрэглэгчийн хариу үйлдлийг үнэлэх

II. ОНОЛЫН ТОДОРХОЙЛОЛТ

A. Кино үйлдвэрлэл дэх хөдөлгөөнт графикийн ач холбогдол:

Хөдөлгөөнт график нь орчин үеийн кино үйлдвэрлэлийн салшгүй нэгэн хэсэг болж, дүрслэлийн уран сайхны илэрхийллээс эхлээд өгүүлэмжийг өргөжүүлэхэд чухал үүрэг гүйцэтгэж байна. Энэ нь ялангуяа нээлтийн кредит, тусгай эффект, тайлбар бичлэг, виртуал орчин үүсгэх зэрэгт өргөнөөр ашиглагддаг.

B. Maxon Cinema 4D-ийг контент үйлдвэрлэлд ашиглах нь:

Maxon Cinema 4D нь 3D хөдөлгөөнт график, тусгай эффект, визуал эффект (VFX) бүтээхэд хамгийн өргөн хэрэглэгддэг программ хангамжуудын нэг юм. Энэхүү программ нь дараах давуу талуудыг контент үйлдвэрлэлд олгодог.

- Нээлтийн кредит ба текстийн анимаци: Киноны эхлэл болон төгсгөл хэсэгт гардаг график текстүүдийг илүү динамик, сонирхолтой байдлаар илэрхийлэхэд Cinema 4D-ийн MoGraph системийг ашигладаг. Энэ нь текстийг 3D орчинд хөдөлгөөнд оруулж, төрөл бүрийн эффектийг нэмж, кинематик дүрслэл үүсгэх боломжийг олгодог.
- Визуал эффект (VFX) ба тусгай эффект (SFX):
- Кинонд бодит болон компьютер график хослуулан дүрслэлүүдийг бүтээхдээ Cinema 4D-г ашигладаг. Жишээлбэл, дэлбэрэлт, усны долгион, гал, утаа зэрэг физик суурьтай эффектүүдийг бодит мэтээр дүрслэхэд тус программын Dynamics ба Particle System хэрэгслүүд чухал үүрэгтэй.
- 3D орчин ба виртуал продакшн:
- Орчин үеийн кинонд бодит байршилд зураг авалт хийхийн оронд виртуал орчинд бүрэн зохиомол ертөнц үүсгэж, дүрүүдийг байршуулан киногоо бүтээх нь түгээмэл болсон. Cinema 4D нь Redshift Render engine болон бусад рендеринг системүүдтэй нийлж, бодит мэт гэрэлтүүлэг, сүүдэр үүсгэн, өндөр чанартай дүрслэл боловсруулах боломжийг олгодог.
- Анимейшн ба персонажийн хөдөлгөөн Кинонд ашиглагдах 3D персонаж болон объектуудыг хөдөлгөөнд оруулахдаа Cinema 4D-ийн Character Animation Toolset-ийг ашиглаж, дүрийн хөдөлгөөнийг нарийн тохируулах боломжтой. Энэ нь ялангуяа VFX-тэй хослуулан ажиллахад тохиромжтой.
- Интеграцийн боломж Cinema 4D нь After Effects, Houdini, Unreal Engine зэрэг бусад программ хангамжуудтай уялдан ажиллах чадвартай тул киноны post-production-д хэрэглэгддэг бусад программтай хялбар холбогдох давуу талтай.

C. Хөдөлгөөнт графикийн онол - Саул Басс ба Жон Уитнигийн хандлага

- Саул Басс ба хөдөлгөөнт графикийн өгүүлэмжийн үүрэг Саул Басс нь киноны титр дизайныг урлагийн түвшинд хүргэсэн анхдагч уран бүтээлчдийн нэг бөгөөд түүний хөдөлгөөнт графикт хандах арга барил нь өгүүлэмжийг дүрслэх шинэ арга замыг нээсэн. Тэрээр “Хөдөлгөөнт график нь киноны өгүүлэмжийн нэг хэсэг байх ёстой.” гэсэн зарчмыг баримталж, киноны ерөнхий уур амьсгал, сэдлийг эхнээс нь тодорхойлохын тулд график хэлбэрийг динамик хөдөлгөөнтэй уялдуулсан. Түүний бүтээлүүдэд:
  - График хэлбэрийн минималист хэв маяг: Энгийн дүрсүүдийг хөдөлгөөнөөр баяжуулан киноны сэдэв, уур амьсгалыг илэрхийлдэг.
  - Динамик хөдөлгөөн, ритм: Тайвшруулах эсвэл хурцадмал байдлыг хөдөлгөөний хурд, чиглэлээр илэрхийлдэг.
  - Киноны өгүүлэмжтэй нэгдсэн хөдөлгөөнт график: зөвхөн гүү зүйн зориулалттай биш, харни өгүүлэмжийн эхлэл, өнгө аясыг тодорхойлдог.

Түүний алдартай бүтээлүүдээс “Psycho” (1960), “Vertigo” (1958), “North by Northwest” (1959) зэрэг кинонуудын титр дизайн нь хөдөлгөөнт графикийн шинэ стандартыг тогтоож, киноны эхлэлээс л үзэгчдэд тухайн киноны сэтгэлзүйн уур амьсгалыг мэдрүүлж чадсан байдаг.

- Жон Уитни ба компьютер графикийн хөгжүүлэлт Жон Уитни нь хөдөлгөөнт графикт компьютерын алгоритм ашиглах боломжийг судалж, математик тооцоолол дээр суурилсан анхны компьютер графикчдын нэг

юм. Тэрээр хөдөлгөөнт графикийн онолд дараах шинэчлэлүүдийг оруулсан.

- Гар аргаар бус, алгоритм дээр суурилсан хөдөлгөөнт дүрслэл: Дижитал техник ашиглан илүү нарийн, динамик хөдөлгөөн үүсэх боломжийг судалсан.
- Фрактал хөдөлгөөн ба геометрийн давтамж: Компьютерын тооцооллыг ашиглан, дүрсийн харилцан хамаарал, давтагдалтай хөдөлгөөнүүдийг бий болгосон.
- Кино, телевизийн салбарт дижитал графикийн хэрэглээ: 1960-аад оноос эхлэн компьютер графикийг киноны титр, тусгай эффектэд ашиглах боломжийг судалсан.

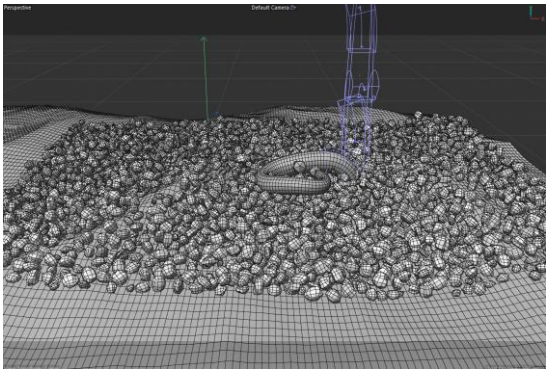
Жон Уитнигийн технологийн дэвшил нь орчин үеийн компьютер график, хөдөлгөөнт дүрслэлийн үндэс суурийг тавьж, өнөөдөр Cinema 4D, After Effects зэрэг программуудын хөгжлийн суурь болсон.

III. ТУРШИЛТ БА СУДАЛГАА

"Cinema 4D-д ашиглан усан доорх бодит орчны хөдөлгөөнт график ба динамик симуляци бүтээх"

А. Усан доорх орчны динамик симуляцийн судалгаа Усан доорх орчныг бодитой дүрслэхийн тулд долгионы нөлөөллийг нарийвчлан судлах шаардлага гарсан. Долгионы физик шинж чанарыг ойлгохын тулд усны гадаргуу дээр үүсэх давлагааны хурд, давтамж, чиглэл, тархалтын хэлбэр зэрэг үзүүлэлтүүдийг судлав. Гүний усанд долгион хэрхэн тархаж, хурд нь хэрхэн өөрчлөгдөх, объектуудын хөдөлгөөнд хэрхэн нөлөөлөхийг тодорхойлохын тулд шинжлэх ухааны судалгаанууд болон бодит бичлэгүүдийг харьцуулан судалсан.

Эдгээр үзүүлэлтүүдийг Cinema 4D орчинд дуурайлган дүрслэхийн тулд Displacer, Turbulence, Gravity зэрэг эффектүүдийг ашигласан. Displacer эффект нь усны гадаргуугийн долгионы хэлбэрийг шугаман бус хөдөлгөөнтэйгөөр өөрчлөхөд ашиглагдсан бөгөөд, процедур текстээ (Noise, Wave, Ripple гэх мэт) ашиглан нарийвчилсан долгионы бүтэц бий болгосон. Turbulence эффект нь усан доорх орчинд жижиг хэмжээний урсгалын хөдөлгөөнийг нэмэхийн тулд хэрэглэгдсэн бөгөөд энэ нь далайн урсгалын нөлөөллөөр шингэний жижиг хэсгүүдийн тархалт, хөдөлгөөнийг илүү натурал болгох боломжийг олгов. Gravity эффектийг ашиглан усан доорх объектуудын жингийн нөлөөллийг бодит мэт гаргахын зэрэгцээ усны динамикийн дагуу тэдний хөдөлгөөнийг хянах боломжийг судалсан.

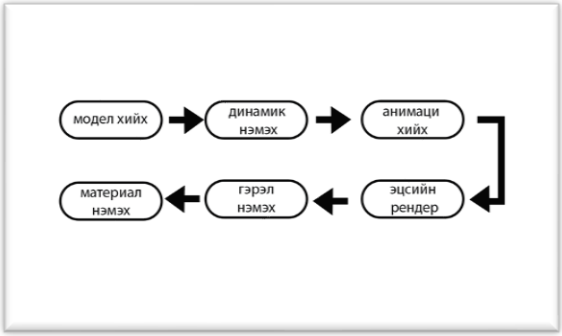


1-р зураг. Усан доорх орчны динамик симуляц

Хэрэглэгчийн сэтгэл ханамжийн судалгааг явуулж үзэхэд доорх нэгдсэн үр дүн гарав.

2-р зураг. Усан доорх орчны динамик симуляцын сэтгэл ханамжийн судалгаа

Судалгаанд оролцогчдын дийлэнх хувь буюу 59% нь уран дүрслэл нэмэх шаардлагатай хэмээн санал ирүүлсэн байгаа тул дараагийн туршилтад үүнийг чухалчлан авч үзэх шаардлага гарсан. Мөн үр дүнд тулгуурлан хийх ажлын дарааллыг төлөвлөгөө болгон доорх байдлаар хавсаргав.

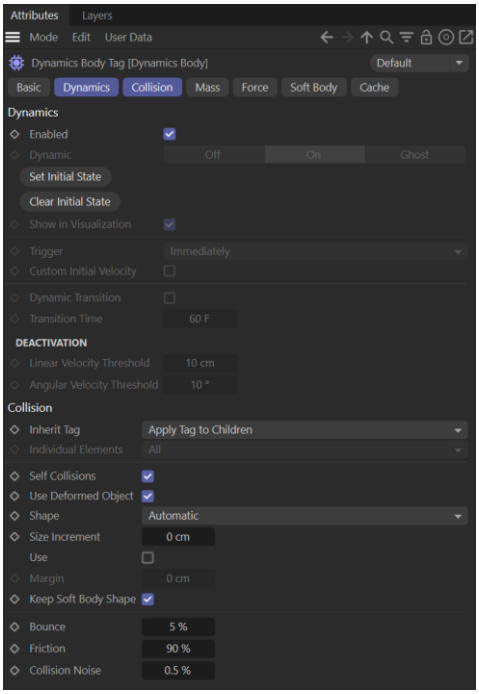


3-р зураг. Судалгааны үр дүнд үндэслэн гаргасан туршилтын төлөвлөгөө

В. Динамик симуляцийн туршилт

Cinema 4D-ийн Emitter, X-Particles болон Dynamic Body системийг ашиглан усан доорх

объектуудын хөдөлгөөнийг нарийвчлан судлав. Эрдэнийн чулуу, сувд зэрэг жижиг хэсгүүдийн уналт, шингэн доторх хөдөлгөөн болон хоорондын мөргөлдөөний динамикийг тестлэхийн тулд Soft Body, Rigid Body, Collision Detection зэрэг тохиргоог ашигласан. Үүнээс гадна, усны хөдөлгөөнд орчны нөлөө үзүүлэхийн тулд Vorticity, Drag Force, Buoyancy зэрэг физик үзэгдлүүдийг симуляц хийж туршсан.



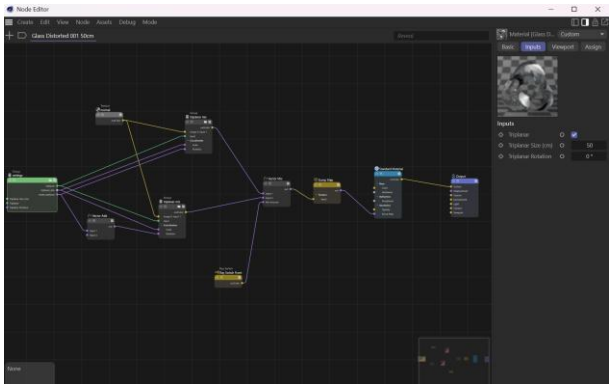
4-р зураг. Dynamics Body tag ашиглан зарим объектуудад хийсэн тохиргоо

С. Объектын материал ба текстийн судалгаа

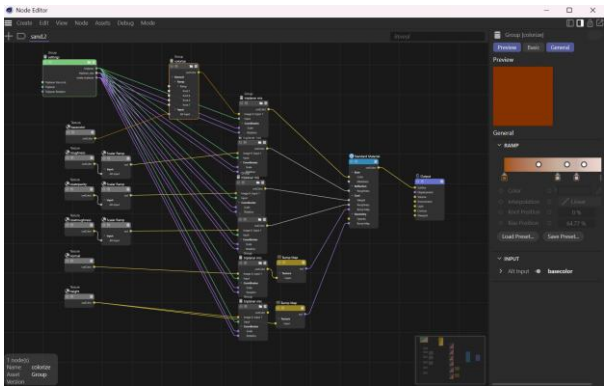
Усан орчинд байгаа объектуудын материал, гэрлийн ойлт, хугарал, уусалтыг бодитой гаргахын тулд Cinema 4D-ийн Node-based Material Editor болон Redshift Material системийг ашиглав.

Объектын гадаргуугийн тусгал, өнгөний тархалтыг илүү натурал харагдуулахын тулд Subsurface Scattering (SSS), Specular Roughness, Refraction Index зэрэг параметрүүдийг тохируулсан.

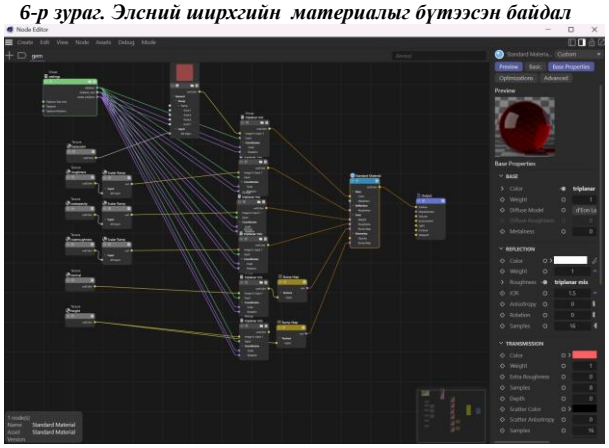
Үүнээс гадна, Gems объектуудын хугарлын индекс, өнгөний гүн болон гэрлийн ойлтыг бодит байдалд ойртуулахын тулд Redshift-ийн Dispersion, Fresnel Effect тохиргоог ашиглаж туршив.



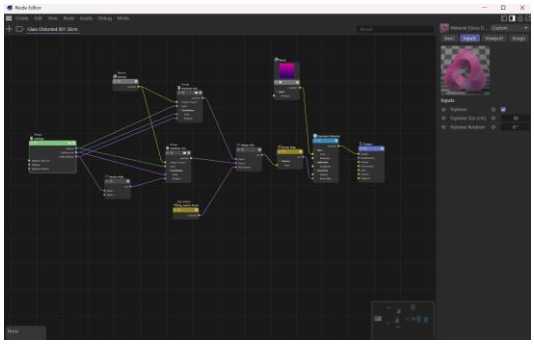
5-р зураг. Усны материалыг бүтээсэн байдал



6-р зураг. Элсний ширхгийн материалыг бүтээсэн байдал



7-р зураг. Алмаазын материалыг бүтээсэн байдал



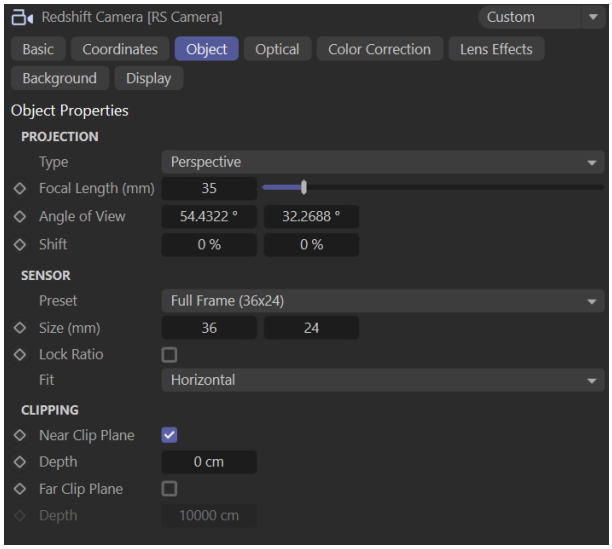
8-р зураг. Гол дүр болох усны могойны материалыг бүтээсэн байдал

D. Хөдөлгөөнт камер болон уран сайхны найруулга

Усан доорх орчны динамикийг илүү бодит болгохын тулд камерын хөдөлгөөн, гүнзгийрэл болон фокусын өөрчлөлтийг судлав.

Cinema 4D-ийн RS Camera ашиглан Depth of Field (DOF), Motion Blur, Chromatic Aberration зэрэг эффектийг тохируулж, бодит камерын динамикийг дуурайлгасан.

Түүнчлэн, далайн ёроолд урсгал даган хөвөх мэт камерын хөдөлгөөнийг Natural Motion Path, Camera Shake болон Underwater Distortion эффектийг ашиглан найруулж, үзэгчид усан дор буй мэт мэдрэмж төрүүлэх боломжийг судлав.



9-р зураг. Redshift Camera-д хийсэн тохиргоо

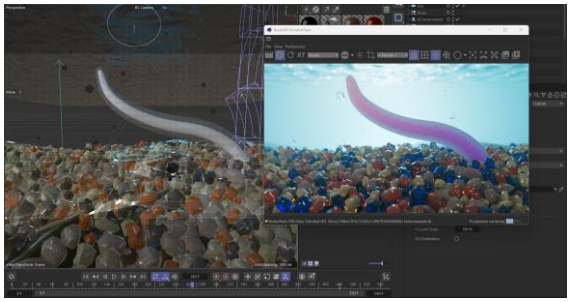
10-р зураг. Redshift Camera-ын keyframe ашиглан хийсэн анимаци

Е. Усан доорх гэрэлтүүлэг ба өнгөний тохируулга

Гэрэлтүүлгийн хувьд Redshift Environment болон HDRI Lighting ашиглан усан доорх орчны гэрлийн уусалт, сарнилт, шүүлтийн нөлөөллийг туршсан. Гэрэл шингээх болон сарниулах динамикийг бодитой гаргахын тулд Volumetric Lighting, Global Illumination тохиргоог ашиглаж, усан орчны натурал харагдах байдлыг нэмэгдүүлсэн.

Үүнээс гадна, өнгөний тохируулгын хувьд Color Grading, Blue Tint Adjustment болон Light Scattering эффектийг ашиглаж, усан доорх орчны уусалтыг илүү натурал харагдуулах туршилтуудыг хийв.

Эдгээр судалгаа, туршилтуудын үр дүнд усан доорх динамик симуляцийн бодит байдалд ойртсон дүрслэлийг гаргах боломжтой болсон бөгөөд цаашдын сайжруулалт нь рендэрийн хурд, материалын бодит байдал болон хөдөлгөөнт найруулгын нарийвчлалд чиглэгдэх болно.



11-р зураг. Redshift Renderview-т харагдах байдал

12-р зураг. Эцсийн рендер

ДҮГНЭЛТ

Усан доорх орчныг бодитой дүрслэхийн тулд долгионы нөлөөллийг нарийвчлан судалсан. Долгионы физик шинж чанарыг ойлгохын тулд усны гадаргуу дээр үүсэх давлагааны хурд, давтамж, чиглэл, тархалтын хэлбэр зэрэг үзүүлэлтүүдийг судалж, гүний усанд долгион хэрхэн тархаж, хурд нь хэрхэн өөрчлөгдөх, объектуудын хөдөлгөөнд хэрхэн нөлөөлөхийг тодорхойлохын тулд шинжлэх ухааны судалгаанууд болон бодит бичлэгүүдийг харьцуулан судалсан.

Эдгээр үзүүлэлтүүдийг Cinema 4D орчинд дуурайлган дүрслэхийн тулд Displacer, Turbulence, Gravity зэрэг эффектүүдийг ашигласан. Displacer эффект нь усны гадаргуугийн долгионы хэлбэрийг шугаман бус хөдөлгөөнтэйгөөр өөрчлөхөд ашиглагдсан бөгөөд процедур текстээ (Noise, Wave, Ripple гэх мэт) ашиглан нарийвчилсан долгионы бүтэц бий болгосон. Turbulence эффект нь усан доорх орчинд жижиг хэмжээний урсгалын хөдөлгөөнийг нэмэхийн тулд хэрэглэгдсэн бөгөөд далайн урсгалын нөлөөллөөр шингэний жижиг хэсгүүдийн тархалт, хөдөлгөөнийг илүү натурал болгоход чухал үүрэг гүйцэтгэсэн. Gravity эффектийг ашиглан усан доорх объектуудын жингийн нөлөөллийг бодит мэт гаргахын зэрэгцээ усны динамикийн дагуу тэдний хөдөлгөөнийг хянах боломжийг олгосон.

Долгионы хэлбэр, давтамж болон усны гадаргуугийн динамикийг илүү нарийвчлалтай болгохын тулд Wave Deformer, Ripple Shader, Ocean Modifier зэрэг хэрэгслүүдийг нэмж туршсан. Wave Deformer ашиглан шингэний давлагаа, усны хөдлөлтийг илүү бодитой дүрслэх боломжийг судалж, түүний давтамж, өндөр, өргөн болон хурдыг өөрчилж үзсэн. Үүний зэрэгцээ, Ocean Shader болон Water Surface Material ашиглан усны гадаргуугийн хугарал, гэрлийн ойлт, тунгалаг байдлыг илүү нарийвчилсан.

Эдгээр туршилтуудын үр дүнд усан доорх орчны хөдөлгөөнийг бодит мэт дүрслэх боломжтой болсон бөгөөд далайн гадаргуугийн чичиргээ, усан доорх урсгал, долгионы сарнилын бодитой дүрслэлийг бий болгоход чухал үүрэг гүйцэтгэсэн. Цаашид симуляцийг илүү нарийвчлалтай болгохын тулд Fluid Simulation, Navier-Stokes Equation, Vorticity Confinement зэрэг илүү нарийн физик хөдөлгөөний алгоритмуудыг судалж, хэрэглэх боломжтой.

НОМ ЗҮЙ

[1]. David Panos, “The Problems and Potentials of the Digital Moving Image in Contemporary Art of the 21st century”, 2022

[2]. O’Pray. M. “Avant-Garde Film, Forms, Themes and Passions. London: Wallflower Press”, 2003

[3]. Michael H. G. “Cinema 4D Studio: The Complete Guide”, 2024

[4]. Matt Milburn “Cinema 4D: The Artist’s Guide to 3D Animation”, 2018

[5]. Sean A. Reedy “Making 3D Movies with Cinema 4D”, 2015

ВЕБ АППЛИКЕЙШНУУД ДАХЬ ОЛОН ШАТЛАЛТ БАТАЛГААЖУУЛАЛТЫГ ТОЙРОХ ХАЛДЛАГЫН ТУРШИЛТ БА ХАМГААЛАЛТЫН АРГАЧЛАЛУУД

Шүрэнцэцэгийн НАНДИНДУЛАМ[1], Лхагвын ОДОНЧИМЭГ[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: nnandia370@gmail.com [1], odno@must.edu.mn[2]

***Хураангуй*: Олон шатлалт баталгаажуулалт (MFA) нь веб аппликейшнуудын аюулгүй байдлыг нэмэгдүүлэх гол механизм боловч халдагчид үүнийг тойрох шинэ аргачлалуудыг тасралтгүй хөгжүүлж байна. Энэхүү судалгааны зорилго нь MFA-ийг тойрох халдлагын аргуудыг тодорхойлох, турших болон хамгаалалтын үр дүнтэй арга хэмжээнүүдийг боловсруулах явдал юм. Судалгааны хүрээнд фишингийн аргаар баталгаажуулалтын токен хулгайлах, MITM (Man-in-the-Middle) халдлага хийх, сесс хулгайлах, мөн нөөц баталгаажуулалтын сул талуудыг ашиглах зэрэг MFA-г тойрох түгээмэл аргуудыг туршсан. Туршилтын үр дүнгээс харахад SMS-д суурилсан OTP баталгаажуулалт халдлагад өртөмтгий байгааг тогтоолоо. Мөн халдлагын үр нөлөөг нэмэгдүүлэхэд нийгмийн инженерчлэл болон фишингийн хэрэгслүүдийг ашиглаж болох нь ажиглагдсан. Судалгааны үр дүнд үндэслэн MFA хамгаалалтыг сайжруулах хэд хэдэн аргачлалыг санал болгож байна. Энэхүү судалгаа нь олон шатлалт баталгаажуулалтын хамгаалалтын цоорхойг багасгах, MFA хэрэгжүүлэлтийг сайжруулахад хувь нэмэр оруулах зорилготой юм.**

Түлхүүр үг: Веб аппликейшн, олон шатлалт баталгаажуулалт, фишинг, нийгмийн инженерчлэл

I. УДИРТГАЛ

Сүүлийн жилүүдэд олон шатлалт баталгаажуулалт (MFA) нь веб аппликейшнуудын аюулгүй байдлыг хангах гол хэрэгслүүдийн нэг болж хөгжсөн. Энэ нь зөвхөн нууц үг ашиглах хамгаалалтаас давж, нэмэлт баталгаажуулалтын давхаргыг нэвтрүүлснээр хэрэглэгчдийн мэдээллийг хамгаалах үр дүнтэй аргачлал болж байна. Гэсэн хэдий ч халдлагын арга техникүүд тасралтгүй хөгжиж байгаатай холбоотойгоор MFA-г тойрох боломжтой шинэ халдлагууд илэрсээр байна. Иймд эдгээр халдлагыг тодорхойлох, тестлэх, хамгаалах аргачлалыг судлах нь мэдээллийн аюулгүй байдлыг сайжруулахад чухал ач холбогдолтой юм.

MFA нь хэрэглэгчийг баталгаажуулахын тулд хэд хэдэн төрлийн танилт хийх аргыг (жишээ нь, нууц үг, нэг удаагийн код, биометр, физик төхөөрөмж гэх мэт) хослуулан ашигладаг. Гэвч кибер халдлагын шинэ арга техникүүдийн хөгжлийн улмаас MFA-г тойрох хэд хэдэн халдлагын төрлүүд бий болсон. Үүнд:

Фишинг халдлага: Хуурамч вебсайтууд болон хортой программ ашиглан хэрэглэгчийн MFA кодыг хулгайлах.

Сесс булаах: Нэгэнт баталгаажсан хэрэглэгчийн сессийг булаах замаар халдагч системд хандах.

Man-in-the-Middle (MitM) халдлага: Шифрлэгдээгүй эсвэл хамгаалалт муутай холбоосыг ашиглан MFA баталгаажуулалтын мэдээллийг олж авах.

SIM Swapping: Хэрэглэгчийн SIM картын хяналтыг авах замаар нэг удаагийн кодыг хянах.

Эдгээр халдлагууд нь MFA хамгаалалтын арга хэмжээг сайжруулах шаардлагатайг харуулж байна. 2024 оны байдлаар, томоохон (10000-аас дээш ажилтантай) компаниудын 87%, дунд хэмжээний (26-100 ажилтантай) компаниудын 34%, жижиг (25 хүртэл ажилтантай) бизнесүүдийн 27% нь MFA ашигладаг болохыг тогтоосон[1][2]. Бусад компаниуд нь 2FA ашигладаг эсвэл өөр нэмэлт баталгаажуулалт ашигладаггүй гэж мэдээллэсэн. Одоогийн байдлаар хамгийн сайн хэмээн нэрлэгдэж буй MFA баталгаажуулалтын хувьд автоматжуулсан кибер халдлагын 99.9%, фишинг халдлагын 86%, тодорхой чиглэсэн халдлагын 76%-ийг зогсоодог [3] ба энэ нь хангалттай хэмжээний үзүүлэлт биш юм. Ихэнх байгууллагууд зөвхөн MFA баталгаажуулалтад итгэн бусад сайжруулалтыг хэрэгжүүлэхгүй байх хандлагатай ба үүнээс үүдэн халдагчдад боломж олгодог.

Судалгааны гол зорилго нь веб аппликейшнууд дахь MFA-г тойрох халдлагыг тестлэх, тэдгээрийн үр нөлөөг тодорхойлох, хамгаалалтын аргачлалыг боловсруулахад оршино.

Судалгааны гол асуултууд:

1. Веб аппликейшн дээр MFA-г тойрох ямар төрлийн халдлагууд хамгийн өргөн тархсан бэ?
2. Эдгээр халдлагууд хэрхэн ажилладаг бөгөөд ямар нөхцөл байдалд амжилттай хэрэгжих магадлалтай вэ?
3. MFA-г тойрох халдлагуудаас сэргийлэх үр дүнтэй хамгаалалтын арга техникүүд юу вэ?

Энэхүү судалгаа нь веб аппликейшн хөгжүүлэгчид болон аюулгүй байдлын мэргэжилтнүүдэд MFA хамгаалалтын сул талыг

тодорхойлох, сайжруулах арга хэмжээг боловсруулахад туслах болно.

II. ӨМНӨ СУДЛАГДСАН АЖЛУУД

A. MFA-ийн үр дүнтэй байдлын үнэлгээ

Өмнөх судалгаануудын ихэнх нь MFA нь уламжлалт нууц үг дээр суурилсан баталгаажуулалтаас илүү найдвартай гэдгийг баталсан байдаг. Ometov et al. (2018) [4] судалгаандаа MFA-ийн түгээмэл хэрэглэгддэг аргууд болох SMS OTP, TOTP (Time-based One-Time Password), биометр баталгаажуулалт болон токен ашиглалт нь фишинг халдлагад бага өртөмтгий боловч хэрэглэгчийн туршлага, хэрэгжүүлэх өртөг өндөртэй болохыг тогтоосон.

B. MFA-г тойрох халдлагууд

Fassl et al. (2021) [5] судалгаандаа хуурамч вэбсайт ашиглан хэрэглэгчдийг хуурч MFA кодыг авах фишинг халдлагын үр дүнг шинжилсэн. Тэдний судалгаа нь хүнээс хамааралтай хүчин зүйлс MFA-г хэрхэн сулруулж болохыг харуулсан.

Өөр нэг судалгаанд Kiivan et al. (2020) [6] веб аппликейшнд MitM (Man-in-the-Middle) халдлагыг туршиж, шифрлэгдээгүй холбооснууд болон хяналтгүй хандалтын токенууд MFA-г тойроход чухал үүрэг гүйцэтгэж байгааг тогтоосон.

C. SIM Swapping халдлагын судалгаа

MFA-г тойрох түгээмэл аргуудын нэг болох SIM Swapping халдлагыг Gupta et al. (2019) [7] нар гүнзгий судалж, үүрэн холбооны операторуудын баталгаажуулалтын сул талууд энэ төрлийн халдлагыг амжилттай хэрэгжүүлэх үндсэн шалтгаан болдог гэдгийг онцолсон.

1-Р ХҮСНЭГТ.СУДАЛГААНЫ АЖЛУУДЫН ЯЛГААТАЙ БАЙДАЛ

Судалгаа	Судлагдсан MFA төрөл	Тойрох халдлагын арга	Үр дүн
Bonneau et al. (2018)	SMS OTP, TOTP, биометр, токен	Ерөнхий хамгаалалтын үнэлгээ	Биометр, токен хамгаалалт сайн ч хэрэгжүүлэх өртөг өндөр
Krombholz et al. (2021)	TOTP, SMS OTP	Фишинг халдлага	Хэрэглэгчийн мэдлэггүй байдал MFA сулруулах хүчин зүйл
Oli et al. (2020)	SMS OTP, TOTP	MitM, Session Hijacking	Шифрлэгдээгүй холбоос, хяналтгүй токен нь халдлагыг хөнгөвчилдөг
Gupta et al. (2019)	SMS OTP	SIM Swapping	Үүрэн холбооны операторын баталгаажуулалт хангалтгүй

Эдгээр судалгаануудаас харахад MFA нь уламжлалт баталгаажуулалтаас илүү найдвартай ч тодорхой төрлийн халдлагад өртөмтгий хэвээр байгааг үзүүлж байна. Иймд MFA-г тойрох халдлагын эсрэг илүү найдвартай хамгаалалтын аргачлалуудыг боловсруулах нь энэ судалгааны гол зорилтуудын нэг юм.

III. СУДАЛГААНЫ АРГА ЗҮЙ

A. Туршилтын орчин

Судалгааны хүрээнд MFA-г тойрох халдлагуудыг туршихын тулд тестийн орчин бэлтгэж, дараах хэрэгслүүдийг ашигласан.

Үйлдлийн систем: Kali Linux
Penetration testing хэрэгслүүд:

- Burp Suite – Веб траффик хянах, халдлагын симуляци хийх
- Evilginx2 – Reverse Proxy ашиглан фишинг хийх
- Gophish – Фишинг кампанит ажил үүсгэх
- Сүлжээний урсгалыг хянах, халдлагын үеийн мэдээллийг задлан шинжлэх

Тестийн орчны сервер нь AWS cloud сервер дээр байрласан.

B. Туршсан MFA төрлүүд

Туршилтад 2-р хүснэгт дэх олон шатлалт баталгаажуулалтын төрлүүдийг хамруулсан бөгөөд тус бүр дээр MFA-г тойрох боломжтой эсэхийг судалсан

2-Р ХҮСНЭГТ.ТУРШИЛТАД АШИГЛАСАН БАТАЛГААЖУУЛАЛТЫН ТӨРЛҮҮД

MFA төрөл	Тайлбар	Тойрох халдлагын боломж
TOTP (Time-based One-Time Password)	Google Authenticator, Authy зэрэг апп ашиглан нэг удаагийн код үүсгэх	Фишинг халдлага, Reverse Proxy (Evilginx2)
SMS-based OTP	Нэг удаагийн кодыг SMS-ээр илгээх	SIM Swapping, Man-in-the-Middle (MitM) халдлага
Push Notification (Approval-based)	Хэрэглэгчид баталгаажуулалтын хүсэлт илгээх (Microsoft Authenticator, Duo Security)	Session Hijacking, Push Notification Spamming (Fatigue Attack)
FIDO2/WebAuthn (Security Key, Biometric)	Физик токен эсвэл биометр ашиглан баталгаажуулах	Фишингээс хамгаалагдсан боловч USB токенийг хулгайлах, төхөөрөмжийн найдвартай байдлаас хамаарна

C. Туршилтын аргачлал

1. Фишинг халдлага (Reverse Proxy ашиглах)

Evilginx2 ашиглан хууль ёсны вэбсайтын хуулбар үүсгэх;

Хэрэглэгчийн нууц үг болон нэг удаагийн MFA кодыг хулгайлах оролдлого хийх;

2. Session hijacking (Сесс булаах халдлага)

Burp Suite ашиглан хэрэглэгчийн нэвтэрсэн сессийг олж авах;

MFA-г тойрон шууд серверт хандах боломжтой эсэхийг шалгах;

3. SIM Swapping халдлага

Үүрэн холбооны үйлчилгээ үзүүлэгчийн сул талуудыг ашиглан хэрэглэгчийн дугаарыг өөр SIM карт руу шилжүүлэх туршилт хийх;

4. Push Notification Fatigue (Хэрэглэгчийг залхаах халдлага)

Хэрэглэгчид олон тооны баталгаажуулалтын хүсэлт илгээж, эцэст нь санамсаргүйгээр зөвшөөрүүлэх боломжтой эсэхийг тестлэх;

5. Man-in-the-Middle (MitM) халдлага

Wireshark болон Burp Suite ашиглан веб урсгалыг хянах;

HTTP траффикаар дамжуулан нууцлалгүйгээр илгээсэн MFA кодыг барих оролдлого хийх;

D. Судалгааны хязгаарлалт

Ёс зүйн асуудал: Бодит хэрэглэгчдийн мэдээлэлд халдаагүй, зөвхөн симуляцийн орчинд туршсан.
Бодит хамгаалалттай системүүд дээрх үр дүн: Зарим компаниудын хамгаалалтын нэмэлт механизмууд (device fingerprinting, IP-based protection) тестийн үр дүнд нөлөөлж болохыг тооцсон.
FIDO2/WebAuthn-д тулгарсан хүндрэл: Фишингээс хамгаалагдсан энэхүү технологийг шууд тойрох нь хүндрэлтэй байсан ч хэрэглэгчийн төхөөрөмж болон токен найдвартай байдалд суурилсан эрсдэл байсаар байгааг тэмдэглэсэн.

Энэхүү аргачлалаар дамжуулан MFA-г тойрох халдлагуудын амжилтын түшинг тодорхойлж, хамгаалалтын үр дүнтэй арга хэмжээг боловсруулах боломж бүрдсэн.

IV. ТУРШИЛТ БА ҮР ДҮН

A. MFA тойрох халдлагын тестийн ерөнхий үр дүн

3-Р ХҮСНЭГТ.ХАЛДЛАГУУДЫН АМЖИЛТЫН ТҮВШИНГ ХЭМЖСЭН БАЙДАЛ

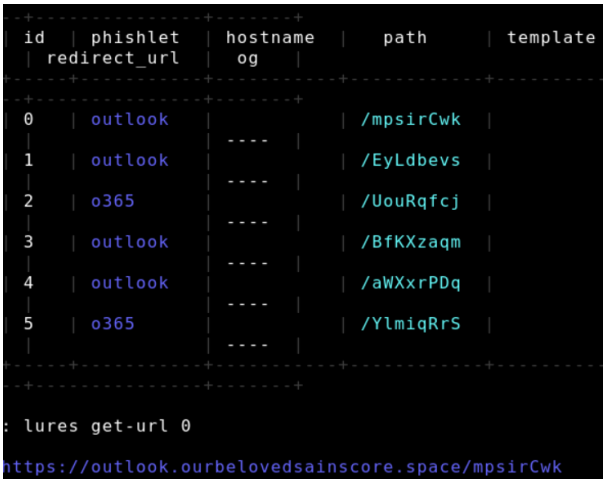
MFA төрөл	***Тойрох халдлагын төрөл***	***Амжил-тын хувь (%)***	***Тайлбар***
SMS-based OTP	Фишинг (Reverse Proxy)	85%	Evilginx ашиглан амжилттай халдсан
SMS-based OTP	SIM Swapping	0%	Үүрэн операторын хамгаалалтуудыг шалган өөр хэрэглэгчийн SIM авах боломжийг судалсан
TOTP (Google auth)	Фишинг (MitM Proxy)	60%	Session Hijacking ашиглан сесс хулгайлсан тохиолдолд амжилт өндөр
Push Notif (Microsoft auth)	Push Spam (Fatigue Attack)	40%	Хэрэглэгч олон хүсэлтээс залхаж, зөвшөөрсөн
FIDO2 / WebAuth	Бие даасан халдлага боломжгүй	0%	Фишинг болон MitM халдлагад өртөөгүй

Гол дүгнэлт: SMS-based болон TOTP MFA нь фишинг, MitM халдлагад өндөр өртөмтгий байсан. Харин FIDO2/WebAuthn MFA болон SIM Swapping нь эдгээр халдлагад өртөөгүй.

B. Фишинг халдлагын үр дүн (Evilginx2 ашигласан тест)

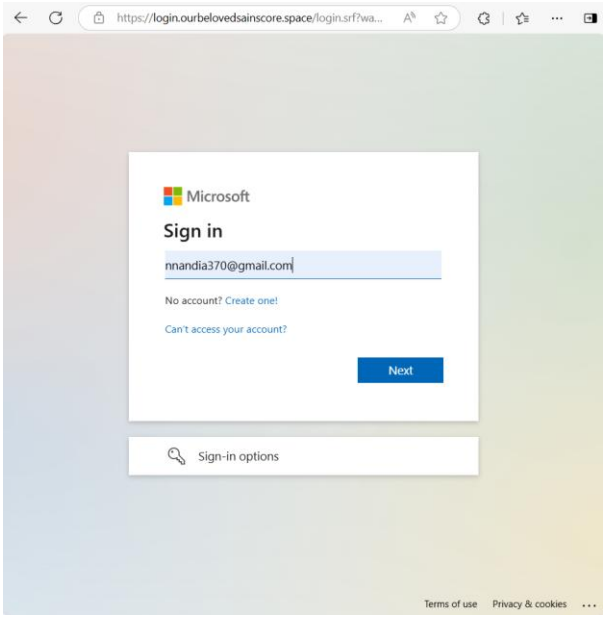
Тестийн алхмууд:

1. Evilginx2 ашиглан жинхэнэ вэбсайтын хуулбар үүсгэсэн.

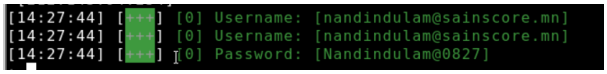


1-р зураг. Хуурамч холбоос үүсгэсэн байдал

Холбоосоор дамжин 2-р зурагт үзүүлж буй хуурамч веб хуудас харагдах ба Gophishing хэрэгсэл ашиглан хүссэнээрээ өөрчлөх боломжтой.



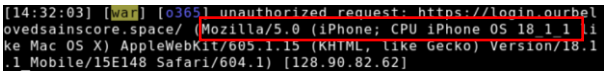
2-р зураг. Хуурамч веб хуудас



3-р зураг. Хохирогчийн нэвтрэх нэр, нууц үг зэргийг авсан байдал

Хэрэглэгчийн нэвтрэх нэр, нууц үг зэргийг авах нь хангалтгүй ба MFA хэрэгжүүлсэн тохиолдолд туршиж байгаа учир баталгаажуулалтын кодыг авах нь чухал юм.

2. Хуурамч вэбсайтаар дамжуулж MFA кодыг хулгайлах оролдлого хийсэн.



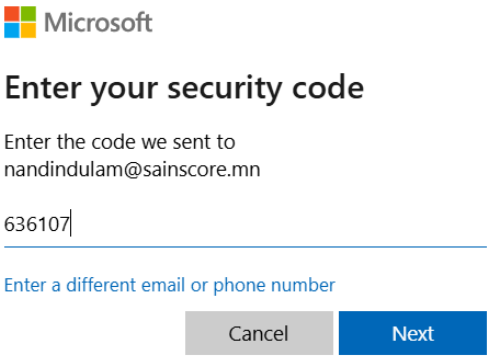
4-р зураг. MFA кодыг хулгайлах оролдлого

Туршилтаар MFA кодыг авч чадаагүй зөвхөн ямар төхөөрөмж ашиглан MFA хийж буйг олж авсан учир session хулгайлахаар шийдсэн. Өөрөөр хэлбэл, аль хэдийн MFA кодоо хийгээд нэвтэрсэн сесс-ийг авахыг оролдсон гэсэн үг.

3. Session hijacking ашиглан MFA-г тойрох боломжтой эсэхийг туршсан.

Хэрхэн сесс авсан болохыг 6-р зурагт үзүүлэв.

Тестийн үр дүн:

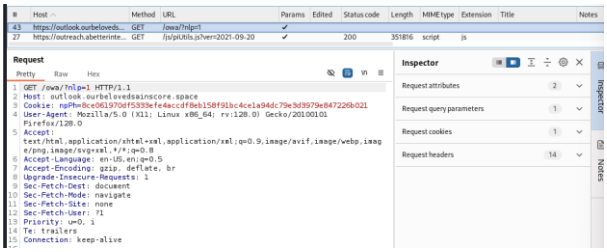


5-р зураг. Фишинг халдлагын үр дүнд сесс аван хандаж чадсан.

C. Session Hijacking тестийн үр дүн (Burp Suite ашигласан тест)

Тестийн алхмууд:

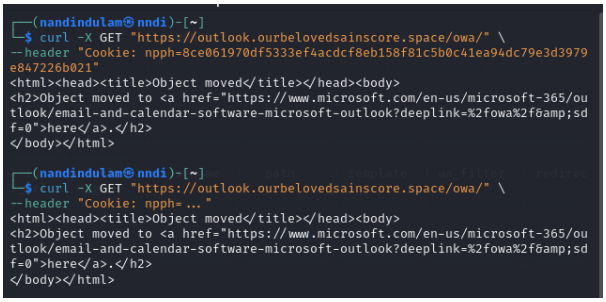
1. Burp Suite ашиглан хэрэглэгчийн сессийг хянах.



6-р зураг. Хэрэглэгчийн cookie-г авсан.

2. Хулгайлагдсан сессээр нэвтрэх оролдлого хийх.

Тестийн үр дүн:



7-р зураг. Cookie нэвтрэх оролдлого хийх.

7-р зурагт хэрэглэгчийн cookie нь идэвхтэй байгаа эсэхийг шалгаж байна. Мөн session нь олон платформ дээр ажиллах эсэхийг тестлэж үзсэн.

Дээрх сесс нь Outlook Web App (OWA) руу очих үед "Object moved" гэсэн хариу авсан байна. Энэ нь домэйн (outlook.ourbelovedsainscore.space) Microsoft-ийн албан ёсны Outlook сайт руу шилжсэн гэсэн үг юм. Өөрөөр хэлвэл сесс ашиглах хугацаа дууссан байна.

Зөвхөн туршилтын энэ тохиолдолд гарсан үр дүн хэдий ч цаашид burpsuite прокси сервер ашиглан хуурамч вебсайт луу хандаж буй хэрэглэгчийн cookie, session-ийг хулгайлах бүрэн боломжтойг харуулж байна.

V. ХЭЛЭЛЦҮҮЛЭГ

MFA нь хэрэглэгчийн аккаунтын 99.9%-ийг халдлагаас хамгаалдаг хэмээн Microsoft компанийн албан ёсны веб хуудас дээрээ зарласан мэдээллийг дээрх энгийн туршилтаар үгүйсгэж болох юм.

Тэгвэл MFA хангалтгүй байх шалтгаан болон тэдгээрийг сайжруулж болох шийдлүүдийг авч үзье.

A. Фишинг болон MitM халдлагад өртөх эрсдэл

Шийдэл: FIDO2/WebAuthn зэрэг фишингийн эсрэг хамгаалалттай MFA аргуудыг хэрэгжүүлэх.

B. OTP болон SMS баталгаажуулалтын сул тал

Шийдэл: Тусгай аппликейшнд суурилсан баталгаажуулалт ашиглах. Кодыг богино хугацаанд ашиглах боломжтой болгож, нэг удаа хэрэглэгддэг байдлыг хангах.

C. Биометрийн мэдээлэлтэй холбоотой аюулгүй байдлын асуудлууд

Шийдэл: Хэрэглэгчийн зан төлөвийн үнэлгээ хийн хэвийн бус үйлдлийг илрүүлэх AI суурилсан системийг нэвтрүүлэх.

D. MFA ашиглахад төвөгтэй байдал

Шийдэл: Хэрэглэгчийн байршил, төхөөрөмжийн итгэлцэл дээр үндэслэн уян хатан MFA бодлого хэрэгжүүлэх.

ДҮГНЭЛТ

Энэхүү судалгаагаар веб аппликейшнууд дахь олон шатлалт баталгаажуулалтыг (MFA) тойрох халдлагын аргуудыг судалж, бодит туршилтуудыг хийснээр хамгаалалтын сул талуудыг тодорхойллоо.

Судалгааны үр дүнд фишингийн халдлага, MITM (Man-in-the-Middle) халдлага, сесс хулгайлах, fallback баталгаажуулалтын эмзэг байдал зэрэг олон төрлийн MFA тойрох техникүүд халдлагад өртөмтгий болохыг тогтоосон.

Судалгааны үр дүнд үндэслэн фишингээс хамгаалах FIDO2/WebAuthn, нэмэлт биометр болон төхөөрөмжийн итгэлцэлд суурилсан баталгаажуулалт зэрэг хамгаалалтын арга шийдлүүдийг санал болгож байна. Эдгээр шийдлүүд нь MFA-ийн аюулгүй байдлыг сайжруулж, халдлагад өртөх магадлалыг бууруулах боломжтой.

Цаашдын судалгааны чиглэлд хиймэл оюун ухаанд суурилсан MFA хамгаалалт, динамик буюу хэрэглэгчийн зан төлөвт суурилсан баталгаажуулалтын аргачлалууд, веб аппликейшнуудын MFA хамгаалалтыг автомат шалгах систем зэрэг сэдвүүдийг гүнзгийрүүлэн судлах болно.

Энэхүү судалгаа нь MFA-ийн хамгаалалтыг улам боловсронгуй болгоход хувь нэмэр оруулж, веб аппликейшнуудын аюулгүй байдлыг дээшлүүлэхэд чухал ач холбогдолтой юм.

ТАЛАРХАЛ

Энэхүү судалгааны ажлыг хийж гүйцэтгэх явцыг удирдан явуулсан удирдагч багш доктор (Ph.D) Л.Одончимэг болон ШУТИС-ийн Мэдээлэл Холбоо Технологийн Сургуулийн Мэдээллийн сүлжээ, аюулгүй байдлын салбарын багш нартаа талархсанаа илэрхийлье.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Multi-Factor Authentication (MFA) Statistics You Need To Know In 2025. Available from https://expertinsights.com/insights/multi-factor-authentication-statistics/

[2] 2025 SME IT Trends Report Learn how IT is steering innovation and security in 2025. Grab Your Copy Toggle Search JumpCloud, Cloud Directory, Logo 2025 Multi-Factor Authentication (MFA) Statistics & Trends to Know. Available from https://jumpcloud.com/blog/multi-factor-authentication-statistics

[3] 17 Essential Multi-factor Authentication (MFA) Statistics [2023]. Available from https://www.zippia.com/advice/mfa-statistics/

[4] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1.

[5] Fassl, M., Gröber, L. T., & Krombholz, K. (2021, May). Exploring user-centered security design for usable authentication ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

[6] Klivan, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023, November). " We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 3138-3152).

[7] Otta, S. P., Panda, S., Gupta, M., & Hota, C. (2023). A systematic survey of multi-factor authentication for cloud infrastructure. *Future Internet*, *15*(4), 146.

[8] Sinha, A., Shrivastava, G., & Kumar, P. (2019). A pattern-based multi-factor authentication system. *Scalable Computing: Practice and Experience*, *20*(1), 101-112.

ОРЧИН ҮЕИЙН КИНО УРЛАГТ SIDEFX HOUDINI ПРОГРАММЫН CGI БА VFX ЭФФЕКТҮҮДИЙН ХЭРЭГЛЭЭ

Дагвын АРИУНБИЛЭГ[1], Ламжавын ЭРДЭНЭБАЯР[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Холбооны салбар
Холбоо барих зохиогчийн и-мэйл хаяг: aakadagva203@gmail.com[1], erdenebayar.l@must.edu.mn[2]

***Хураангуй*: Орчин үеийн кино урлагийн салбарт SideFX Houdini программ нь CGI (Computer-Generated Imagery) болон VFX (Visual Effects)-ийн голлох хэрэгсэл болж байна. Энэхүү судалгаагаар Houdini программын Vellum Solver болон Pop Axis Force хэрэгслүүдийг ашиглан дижитал хувцасны хөдөлгөөний симуляцийг боловсронгуй болгох боломжийг судаллаа. Динамик физик суурилсан процедурчлалын аргуудыг ашигласнаар хувцасны материалын хөдөлгөөн, салхины нөлөөлөл, бодит цагийн дүрслэл зэрэг хүчин зүйлсийг сайжруулах боломжтойг тогтоосон. Судалгааны хүрээнд Houdini-ийн Procedural Modeling аргыг ашиглан VFX-д зориулсан хотын динамик орчныг үүсгэж, бодит мэт архитектурын дүрслэлийг гаргаж авсан болно. Энэхүү аргачлал нь кино болон тоглоомын үйлдвэрлэлд өргөн хэрэглэгдэх боломжтой бөгөөд Монголын VFX салбарт шинэчлэлт хийх чухал алхам юм.**

Түлхүүр үг: динамик симуляци, хөдөлгөөнт дүрслэл, процедурчлал, загварчлал

I. УДИРТГАЛ

Орчин үеийн кино урлаг, видео тоглоомын үйлдвэрлэлд компьютер график (CGI) болон харагдах эффектүүд (VFX) чухал үүрэг гүйцэтгэж байна. Эдгээр технологи нь бодит мэт дүрслэл, динамик хөдөлгөөн, орчны нарийвчилсан симуляцийг бий болгох боломжийг олгодог. SideFX Houdini программ нь процедурчлалын загварчлал (Procedural Modeling) болон физик суурьтай симуляци хийх [1]. өргөн боломжтой тул орчин үеийн VFX үйлдвэрлэлд голлох хэрэгслүүдийн нэг болж байна.

Энэхүү судалгааны ажлаар Houdini программын хоёр өөр чиглэлд ашиглах боломжийг судалсан. Эхний судалгаанд Vellum Solver болон Pop Axis Force хэрэгслүүдийг ашиглан хувцасны динамик симуляцийг боловсруулж, 3D орчинд VFX бүтээх туршилт хийгдсэн. Энэ нь хувцасны материалын хөдөлгөөн, салхины нөлөөллийг боловсруулах үндэс болсон.

Хоёр дахь судалгаанд Houdini-ийн Procedural Dependency Graph (PDG)-ийг ашиглан хотын орчны процедурчлалын загварчлалын аргыг судалсан. Энэхүү аргачлалаар VFX-д зориулсан хотын динамик орчныг үүсгэж, архитектурын бодит дүрслэл бүхий 3D загвар боловсруулах боломжийг шинжилсэн.

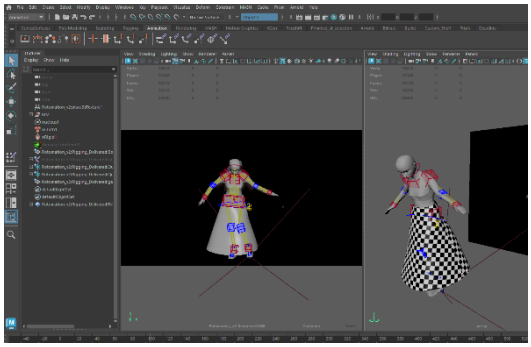
Судалгааны ажлын зорилго нь VFX үйлдвэрлэлд Houdini программын хэрэглээг гүнзгийрүүлэн судалж, процедурчлалын загварчлалын давуу талыг тодорхойлох, Монголын VFX салбарт хэрэгжүүлэх боломжийг үнэлэхэд оршино.

II. SIDEFX HOUDINI ПРОГРАМ ДЭЭР ХИЙСЭН ТУРШИЛТ

A. Хувцасны олон давхар хормойн хөдөлгөөний симуляцийг хийх аргачлал

Хувцасны хөдөлгөөнийг Houdini дээр симуляци хийхийн өмнө дараах үе шатуудыг гүйцэтгэнэ.

1. Дүрс бичлэг ба 3D өгөгдөл бэлтгэх

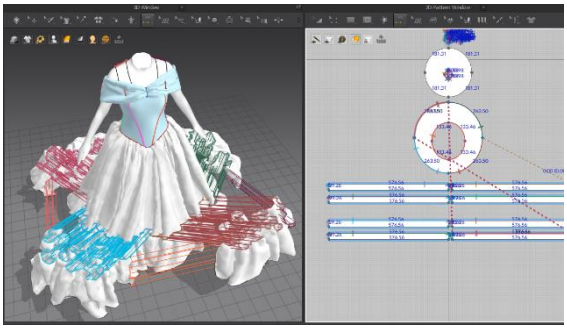


1-р зураг. 3D өгөгдөл бэлтгэх (дүрсэд тохируулан биеийн хөдөлгөөнийг бэлдэх үйл явц)

- Ногоон дэлгэцтэй бичлэг хийх: Камер, гэрэлтүүлгийн тохиргоог стандартын дагуу бэлтгэж, дүрийн хөдөлгөөнийг өндөр чанартайгаар бичлэгт буулгах.
- 3D скан хийх: Хүний биетийн хэлбэр, хэмжээг үнэн зөв дүрслэхийн тулд EinScan Pro 2X эсвэл үүнтэй дүйцэх сканер ашиглан өндөр нарийвчлалтай 3D өгөгдөл үүсгэх.
- Скан өгөгдлийг боловсруулж, цэвэрлэх: Илүүдэл өгөгдлийг шүүж, ZBrush эсвэл Maya программд импортлон retopology хийж, полигоны тоог оновчтой болгох.
- Rigging ба Skinning: Хөдөлгөөнтэй нийцүүлэхийн тулд Maya дээр Quick Rig ашиглан rigging хийх, skin weights тохируулах.

2. Хувцасны загварчлал ба материалын тохиргоо

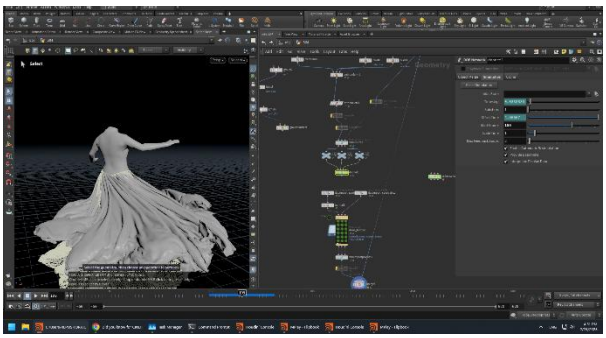
- Marvelous Designer ашиглан хувцасны 2D загвар үүсгэж, 3D хувилбарт шилжүүлэх.
- Даавууны физик шинж чанарыг тохируулах (уян хатан байдал, үрэлт, хүндийн жин).
- OBJ эсвэл Alembic формат руу хөрвүүлж, Houdini-д импортлох.



2-р зураг. Marvelous Designer программ дээр хувцасны загварчлал хийх явц

Houdini-д хувцасны хөдөлгөөний симуляци хийх

1. Геометр дүрслэлийн бэлтгэхдээ хувцасны Geometry SOP (Surface Operators) үүсгэх, UV Mapping хийх.
2. Vellum Solver ашиглан хувцасны динамик систем үүсгэх
   - Уян хатан байдлыг тохируулах: 0.1 – 1.0 (stretch stiffness)
   - Нугаралтын хэмжээг тохируулах: 0.01 – 0.5 (bend stiffness)
   - Self-Collision Enabled: Хувцас хоорондоо нэвчихээс сэргийлэх
3. Салхины динамик тохиргоо (DOP Network) хийхдээ Pop Axis Force ашиглан салхины чиглэл, хүчийг тохируулах, Pop Wind ашиглан салхины хэлбэлзэл, хөдөлгөөнийг илэрхийлэх.
4. Collision тохиргоо
   - Хувцасны хөдөлгөөнийг бодит хүнтэй уялдуулахын тулд Static Object (Collision Geometry) үүсгэх.
   - Хувцас болон биетийн үрэлтийн тохиргоо: 0.2 - 0.5 (friction).
5. Симуляци болон Cache хийх
   - Substeps: 2 - 3
   - Save to Disk (.bgeo.sc) форматаар хадгалах.

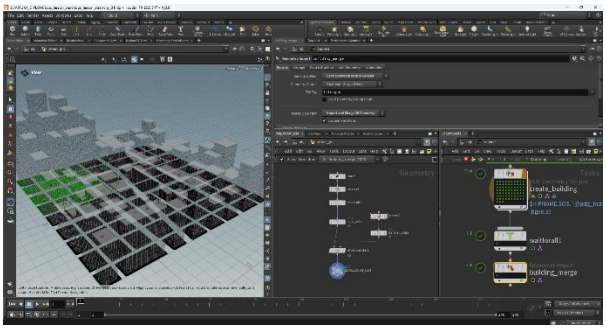


3-р зураг. Houdini программ дээр хувцасны симуляци хийх явц

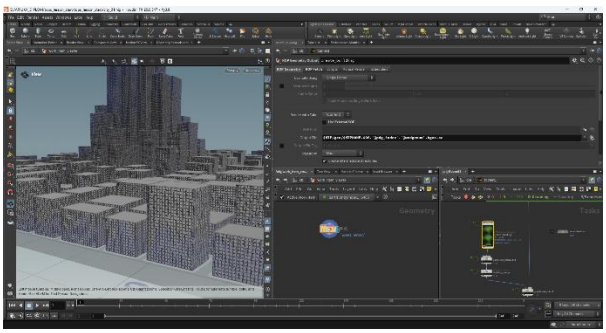
B. Хотын орчны процедурчлалын загварчлал

Procedural Dependency Graph (**PDG**) ашиглан хотын динамик загварчлалыг гүйцэтгэх үндсэн үе шатууд:

1. Хотын зураглалын өгөгдлийг геометр болгон хөрвүүлэх
   - Хар, цагаан өнгийн газрын зургаас Trace Node ашиглан геометр үүсгэх
2. Барилгуудын өндөр, хэлбэрийг процедурчлалаар тохируулах
   - PolyExtrude ашиглан барилгын өндрийг тохируулах
   - Attribute Create ашиглан байшингийн өндөрт санамсаргүй утга өгөх
3. Хотын төв болон орчны ялгаа гаргах
   - Attribute Transfer ашиглан төв хэсгийн барилгуудын өндрийг нэмэгдүүлэх “height_variation= rand(@pdg_index)*15 + @Cd.g*30”
   - Cd.g (ногоон өнгөний утга) ашиглан динамик өндөр тохируулах
4. Гудамж, замын геометр үүсгэх
   - PolyExtrude ашиглан замуудыг 3D болгож гүнзгийрүүлэх
5. Олон янзын хотын загварыг шалгах (Wedge)
   - Wedge Node ашиглан өөр өөр хувилбар турших



4-р зураг. Ногоон өнгөний утгад хотын төвийн барилгуудын нэмэлт өндрийг тодорхойлж байна



5-р зураг. Өөр өөр газрын зургууд дээр тест хийсэн байдал

III. СИМУЛЯЦИЙН ҮР ДҮН

A. Хувцасны хөдөлгөөний симуляцийн үр дүн

SideFX Houdini программын Vellum Solver болон Pop Axis Force хэрэгслүүдийг ашиглан хувцасны хөдөлгөөний динамик симуляцийн судалгааг хийлээ. Туршилтын явцад дараах үр дүнг гаргасан:

- Материалын уян хатан байдал: Stretch stiffness-ийг 0.1–1.0, bend stiffness-ийг 0.01–0.5 хооронд тохируулахад бодит хөдөлгөөнийг дуурайлган дүрслэх боломжтой байв.
- Салхины нөлөөлөл: Pop Axis Force ашигласнаар салхины чиглэл, хурдыг динамикаар тохируулж, даавууны хөдөлгөөний бодит байдлыг нэмэгдүүлсэн.
- Collision тохиргоо: Self-Collision болон Static Object тохиргоог оновчтой хийснээр хувцас хүний биетэй мөргөлдөхгүй байх нөхцөлийг бүрдүүлэв.
- Cache болон хадгалалт: Хөдөлгөөний нарийвчлалыг сайжруулахын тулд Substeps-ийг 2–3 болгож, үр дүнг .bgeo.sc форматаар хадгалснаар рендерлэх үед өгөгдөл алдагдахгүй байх боломжтой болов.

Эдгээр тохиргооны тусламжтайгаар бодит цагийн симуляци хийх боломж бүрдэж, VFX болон анимейшн бүтээхэд оновчтой орчин бүрдүүлэв.

B. Хотын орчны процедурчлалын загварчлалын үр дүн

PDG (Procedural Dependency Graph) ашиглан хотын динамик орчныг загварчлах судалгааг явуулж, дараах үр дүнг гаргав:

- Барилгын хэлбэр, өндрийг процедурчлалаар удирдах: PolyExtrude болон Attribute Create аргуудыг хослуулснаар хотын төвийн барилгуудыг санамсаргүй утгаар өндөрсгөж, илүү бодит дүрслэлтэй болгосон.
- Гудамж, замын бүтэц: Trace Node болон PolyExtrude ашиглан газрын зургийг 3D орчинд хөрвүүлж, бодит хотын дүрслэлийг бий болгосон.
- Оновчтой ажиллагаа: Wedge Node ашиглан өөр өөр хувилбаруудыг автоматаар үүсгэж, загварчлалын процессыг хурдасгасан. Үүний үр дүнд бүтээх хугацаа богиносож, ажлын зардал буурах боломжтой боллоо.

Эдгээр үр дүн нь процедурчлалын загварчлалыг VFX болон тоглоомын үйлдвэрлэлд үр ашигтай хэрэглэх боломжтойг харууллаа. Эдгээр аргууд нь симуляцийн бодит байдлыг сайжруулаад зогсохгүй, ажлын урсгалыг оновчтой болгож, цаг болон нөөцийг хэмнэх ач холбогдолтой юм.

ДҮГНЭЛТ

Энэхүү судалгаагаар SideFX Houdini программыг VFX-д ашиглах боломжийг судалж, дараах гол дүгнэлтүүдийг гаргав:

Хувцасны хөдөлгөөний симуляци: Vellum Solver, Pop Axis Force ашигласнаар бодит хувцасны хөдөлгөөнийг дүрслэх боломжтой болсныг баталлаа. Үүний зэрэгцээ, симуляцийн үр ашгийг нэмэгдүүлж, рендерлэх процессын зардлыг бууруулах боломжтой гэдгийг тогтоов.

Хотын орчны процедурчлалын загварчлал: PDG ашиглан хотын орчныг динамикаар загварчлах нь илүү хурдан, бодит дүрслэлтэй загвар гаргах нөхцөлийг бүрдүүлсэн. Энэ нь гар ажиллагааг багасгаж, цаг хэмнэх чухал давуу талтай.

Монголын VFX салбар дахь хэрэглээ: Houdini программ нь процедурчлалын загварчлал, физик суурьтай симуляцийн аргуудыг ашиглах өргөн боломжтой тул Монголын кино, тоглоомын салбарт цаг хугацаа, зардлыг хэмнэх давуу талтай болохыг тогтоолоо.

Цаашдын судалгааны чиглэл: Хувцасны хөдөлгөөнийг илүү нарийвчлалтай болгох, салхины нөлөөллийг бодит байдалд ойртуулах, хотын загварчлалд машин, хүн зэрэг нэмэлт элементүүдийг оруулах шаардлагатай байна.

Энэхүү судалгааны үр дүн нь кино, тоглоомын үйлдвэрлэлд CGI болон VFX ашиглалтыг сайжруулах боломжийг нэмэгдүүлж, Монголын VFX салбарын хөгжлийг урагшлуулах чухал суурь болох юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] SideFX, "Houdini Foundations 19.5," SideFX Software, 2022.

[2] Eran Dinur, The Complete Guide to Photorealism in VFX, Routledge, 2021.

[3] Richard J. Radke, Computer Vision for Visual Effects, Cambridge University Press, 2012.

[4] SideFX, "Procedural Dependency Graphs (PDG) in Game Development," Houdini Technical Documentation, 2023.

[5] Ubisoft, "Procedural World Generation with Houdini in Far Cry 5," Ubisoft Developer Conference, 2018.

[6] Insomniac Games, "Building New York City in Spider-Man: Miles Morales," GDC Conference Proceedings, 2021.

[7] Guerrilla Games, "Horizon Forbidden West: Procedural Environments and Worldbuilding," Game Developers Conference, 2022.

[8] Rockstar Games, "Red Dead Redemption 2: World Creation using Houdini," Rockstar Tech Blog, 2019.

[9] Henrik Wann Jensen, Realistic Image Synthesis Using Photon Mapping, A. K. Peters, Ltd., 2001.

[10] M. Müller, B. Heidelberger, M. Teschner, and M. Gross, "Meshless Deformations Based on Shape Matching," ACM Transactions on Graphics (SIGGRAPH), vol. 24, no. 3, pp. 471-478, 2005.

[11] Ronald T. Krigger, *CGI & VFX in Film Production*, Journal of Digital Media, vol. 15, no. 3, pp. 245-260, 2020.

ЭМИЙН ЖОР БИЧЭЭЧ УХААЛАГ СИСТЕМ

Үүрцайхын МӨНХТУЯА[1], Гантулгын МАГВАН – ЭРДЭНЭ[1], Батжаргалын ДОЛГОРСҮРЭН[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар, Компьютерын ухааны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: munkht46@gmail.com[1], b.dolgorsuren@must.edu.mn[2]

***Хураангуй*: Монгол улсын эрүүл мэндийн байгууллагууд, эмчээс өвчтөнд зориулж бичдэг эмийн жорыг механикаар буюу гар аргаар үйлдэж, цаасан хэлбэрээр иргэдэд үйлчилдэг. Энэ нь эмч, эмнэлгийн ачааллыг нэмэгдүүлэх, иргэд эмийн жорыг хаяж үрэгдүүлснээс үүдэн шаардлагатай эмээ авч чадахгүй байх, цаасны хэрэглээ ихэссэнээр байгаль орчинд сөрөг нөлөө үзүүлэх зэрэг дутагдалтай талуудыг үүсгэж байна. Энэ үйл явцыг хиймэл оюун ухааны дэвшилтэт технологийг ашиглан судалгаа, хөгжүүлэлтэд дээр үндэслэн автоматжуулахаар зорьсон бөгөөд оновчтой загварыг хэрэгжүүлсэн ухаалаг системийн шийдлийг боловсруулсан болно. Уг систем нь эмчийн үзлэгийн яриаг хүлээн авч, эмийн тун хэмжээ, бэлтгэх арга, яаж хэрэглэхийг заасан эмийн жорыг MNS 5376:2016 стандартын дагуу гаргах юм. Үүний үр дүнд боловсруулагдсан эмийн жорыг эмийн сангийн систем болон E-Mongolia систем рүү илгээх, ингэснээр иргэд, эмийн санч, эмнэлэг эм олгох үйл явцыг хянах боломжийг судалсан болно. Түс сэдвийн хүрээнд бусад улс орнуудад ашиглагддаг ижил төстэй системүүдийг судалж, түүнд чиглэсэн оновчтой үр дүнг боловсруулаа.**

Түлхүүр үг: цахим жор, эм зүйн салбар, whisper, pyannote, LLM

I. Удиртгал

Хиймэл оюун ухаан (AI) нь эрүүл мэнд, анагаахын шинжлэх ухааны салбарт инновац, өөрчлөлтийн шинэ эрин үеийг бий болгож байна. “AI” технологи ашигласнаар уламжлалт байдлаар буюу хүний оролцоотой хийгддэг үйлдлүүдийг автоматжуулах боломжтой бөгөөд цаашид илүү ухаалаг системүүд бүтээгдсээр байна [1]. Ухаалаг танилтын технологи нь хиймэл оюун ухааны үндсэн ангилалд хамаарагддаг. Үүнийг хоёр хэсэгт хуваадаг. Эдгээр нь дүрс таних технологи болон яриа таних технологиуд юм. Хиймэл оюун ухаан нь цаг хугацааг хэмнэх, мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хангах зэрэг эрүүл мэндийн салбарт өргөн хүрээний боломжит хэрэглээтэй. Монгол улсад үйл ажиллагаагаа явуулдаг эрүүл мэндийн байгууллагууд эмийн жорыг эмч, мэргэжилтнүүд механикаар буюу гар аргаар бичиж, цаасан хэлбэрээр ард иргэдэд үйлчилдэг үйл явцыг хиймэл оюун ухаан, машин сургалт, гүн сургалтын аргуудыг ашиглан ухаалаг веб системийн оновчтой шийдлийг боловсруулан шийдвэрлэхээр зорилоо. Энэ нь эмчийн ачааллыг бууруулах, эмийн жорыг хуурамчаар үйлдэх, хаяж гээгдүүлэх зэрэг асуудлыг шийдвэрлэхэд чухал нөлөө үзүүлж байна [3].

Судалгааны зорилго: Энэхүү судалгааны ажлын зорилго нь эмчийн үзлэгийн яриаг боловсруулж, тогтсон стандарт, загварын дагуу өвчтөнд зориулсан эмийн жорыг хиймэл оюун ухааны яриа танилтын дэвшилтэт технологид суурилагдсан веб системийн оновчтой шийдэл боловсруулан, анагаах ухааны салбарт нэвтрүүлэх боломжийг судлахад оршино.

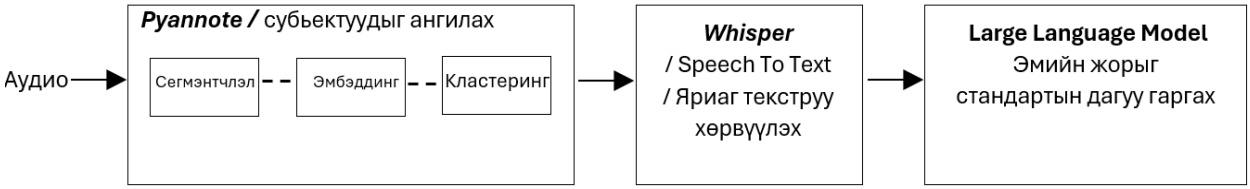
Судалгааны зорилт:

1. Яриаг бичвэрт хөрвүүлэх, ярьж буй субьектуудыг таних, эмийн жорыг стандарт, шаардлагын дагуу боловсруулахад шаардлагатай онолын судалгааг хийнэ.
2. Өгөгдөл цуглуулж, бэлтгэнэ.
3. Хөгжүүлэлт хийнэ.
4. Алдааны хувийг тооцоолно.

II. Онолын хэсэг

Хиймэл оюун ухааны машин сургалт, гүн сургалтын фреймворк дээр хөгжүүлэгдсэн дуу хоолойг текст рүү хөрвүүлэх, ярьсан субьектуудыг ялгах, текст боловсруулах олон технологиуд байдаг бөгөөд үүнээс хамгийн өргөн ашиглагддаг Google Text To Speech, Kaldi, DeepSpeech, IBM, Whisper, Pyannote, LLM гэх мэт сангуудыг тодорхой үзүүлэлтүүдээр харьцуулсны үндсэн дээр хамгийн оновчтойг нь сонгон, бэлтгэсэн өгөгдлөөр сургаж бодит бүтээгдэхүүн болгоход энэхүү судалгааны ажил тулгуурласан болно. Харьцуулсан судалгааны үр дүнг Хүснэгт 1-т оруулаа. Үүний үр дүнд яриаг текст рүү хөрвүүлэхэд хамгийн бага алдааны хувьтай, мөн хамгийн олон буюу 100 гаруй хэл дээр хөрвүүлэлт хийх боломжтой whisper, яриа танилт болон ярианы хэлбэр таних (speaker diarization) зэрэг дууны дохио боловсруулахад чиглэгдсэн Pyannote сан, эмийн

жорыг тогтсон стандарт шаардлагын дагуу боловсруулахад LLM моделиудыг ашиглахаар сонгосон болно. Зураг 1-т системийн ажиллах үйл явцыг харуулав.



1-р зураг системийн үйл ажиллагааны диаграм

2.1 Өгөгдлийн багц

Бид судалгааны ажилдаа дараах өгөгдлийн багцуудыг бэлтгэж, ашигласан болно. Үүнд:

- Монгол улсад бүртгэлтэй 4788 эмийн худалдааны нэр, олон улсын нэр, тун хэмжээ, эмийн мэдээлэл [8,9].
- Эмч, эрүүл мэндийн ажилтны эмийн жорыг тайлбарласан 68 цагийн аудио өгөгдөл.

2.2 Өгөгдлийн урьдчилсан боловсруулалт

Бидний цуглуулж бэлтгэсэн өгөгдлийн багц нь Монгол им импекс концерн болон Монголын гаалийн ерөнхий газраас авсан бүртгэл, мэдээлэл байсан тул хоосон утга болон давхардсан утга байгаагүй. Харин эмийг зориулалтаар нь ангилж шошголох шаардлагатай болсон.

Аудио өгөгдөлд өгөгдлийн цэвэрлэгээ хийх:

- Хүн хоорондын харилцан ярианы өгөгдлийн “аа”, “ммм” гэх мэт сул үгсийг хассан.

Эмийг зориулалтаар нь шошгололт хийх:

- Эмийг зориулалтаар нь ангилж (антибиотик, элэг, нойр гэх мэт) шошгололтыг гараар үүсгэсэн.

2.3 Whisper /Яриаг бичвэрт хөрвүүлэх/

Бидний сонгосон Whisper нь дэвшилтэт яриа танилтын (ASR – Automatic Speech Recognition) модель бөгөөд олон хэлнээс яриаг текст болгон хөрвүүлэх чадвартай [2]. Whisper сан нь яриаг текст рүү хөрвүүлэх (Speech To Text), яриа танилт, дууны дохио боловсруулах салбарт ашиглагддаг нээлттэй эхийн “toolkit” юм. Үүний давуу талуудыг дурдвал:

1. **Орчин үеийн дэвшилтэт технологи**: Whisper нь яриаг текст рүү хөрвүүлэх, яриа танилт, ярианы сегментаци, илрүүлэлт зэрэгт хамгийн сүүлийн үеийн гүн сургалтын технологийг ашигладаг.
2. **Олон хэл дээр боловсруулалт хийх**: Монгол улс 51 орноос эм импортолдог бөгөөд, 100 гаруй хэл дээр боловсруулалт хийн яриаг текст рүү хөрвүүлдэг нь энэхүү санг эм зүйн салбарт ашиглахад оновчтой болгож байна [2].
3. **Алдааны хувь бага**: Whisper нь бусад яриаг текст рүү хөрвүүлдэг технологиудтай харьцуулбал хамгийн бага буюу 5-10% алдааны хувьтай байна.

Эдгээр давуу талууд нь Whisper-г яриаг текст рүү хөрвүүлэх, яриа таних, яриа сегментацлах гэх мэт нарийн дууны дохио боловсруулах ажлуудад хүчирхэг хэрэгсэл болгодог.

Whisper санг бусад яриа танилтын сангуудтай харьцуулсан хүснэгт [2]

1-Р ХҮСНЭГТ

Үзүүлэлт	*Whisper*	*Google Speech To Text*	*DeepSpeech-Mozilla*	*Kaldi*	*IBM Watson*
Олон хэл дээр ажиллах чадамж	100 гаруй хэл, Монгол хэл дээр сургах боломжтой	70 гаруй хэл	Зөвхөн англи хэл	20 гаруй хэл	10 гаруй хэл
Яриа танилтын сантай хамтран ажиллах чадамж	(Pyannote, DeepSeek зэрэгтэй холбож болно)	Google AI – тай хамтран ажиллаг аг	Бусад сангуудтай холбох боломжгүй , бие даасан загвар	Яриа танилт дэмждэг	IBM AI ашиглад аг
Үнэ төлбөр	Нээлттэй, үнэ төлбөргүй	Төлбөрт эй API	Үнэгүй	Үнэгүй	Төлбөрт эй
Урьдчилан боловсруулагдсан эсэх	Pre-trained модель, fine-tuning хийх боломжтой	Google API модель ашиглад аг	Тохиргоо шаардлага тай	Гараар тохирго о хийнэ	AI модель ашиглад аг
Алдааны хувь	5-10%	4-10%	15-25%	10-20%	6-12%

2.3.1 Whisper-Текст хөрвүүлэлт (Speech-to-Text)

Whisper модель нь дарааллаас дараалал **Seq2Seq (Sequence-to-Sequence)** хосолсон загвараар яриаг текст болгон хөрвүүлдэг.

Томьёо 2.2.1: Seq2Seq алгоритмын томьёо

$$P(Y|X) = \prod_{t=1}^{T'} P(y_t|y_1, y_2, ..., y_{t-1}, X; \theta) \quad (1)$$

Хувьсагчид:

- X - өгөгдлийн орж ирсэн дараалал
- Y - гарах текст
- θ - моделийн параметрүүд
- P(yt|y1,...,yt−1,X) - оролтын дагуу дараагийн текст үүсгэх функц

2.4 Pyannote /Ярьж буй субъектийг ангилах/

Пианнот бол Pytorch машин сургалтын фреймворк дээр тулгуурлан ажилладаг Python хэл дээр бичигдсэн яриа танилтын сан юм. Үүнийг аудио өгөгдлөөс эмч болон өвчтөнийг танихад ашиглана. Ингэснээр эмийн жортой холбоотой хэсгийг ялгаж, стандартын дагуу текст болгоно. Энэ үйл явц нь сегментчлэл, эмбеддинг, кластеринг гэсэн үе шатуудтай.

2.4.1 Pyannote-Сегментчлэл (Segmentation)

Сегментчлэл нь аудио бичлэгийг хэд хэдэн хэсэг болгон хуваж, хүн ярьж байгаа эсэхийг шүүх, шуугианыг бууруулах зэргээр өгөгдлийн цэвэрлэгээ хийгддэг. Ингэснээр тухайн аудионоос ярьж буй субъектүүдийг ангилах боломжийг олгодог [5]. Сегментчлэл нь Recurrent Neural Network (RNN) алгоритм дээр суурилагдаж гүйцэтгэгддэг [томьёо 2.4.1].

$$h_t = \sigma(W_x X_t + W_h h_{t-1} + b) \quad (2)$$

Томьёо 2.1.2 Recurrent Neural Networks алгоритмын томьёо

Хувьсагчид:

- X_t : Аудио сигналын оролт
- h_{t-1} : Илрүүлэх хувьсагчийн утга
- W_x : Матрицын оролтын утгын жин
- W_h : Матрицын хувьсагчийн утгын жин
- b : Хазайлтын утга
- σ : Идэвхжүүлэлтийн функц

2.4.2 Pyannote-Эмбеддинг (Embedding)

Энэхүү шатанд сегментүүдээс буюу ярьж буй субъектуудээс хоолойны өнгө, ярианы хурд, ярианы зангилаа(pitch) зэрэг шинж чанаруудыг илрүүлэх үйл явц хийгддэг [5]. Эмээлдэнэ нь Deep Neural Network (DNN) алгоритм дээр суурилагдаж гүйцэтгэгддэг [томьёо 2.4.2].

Томьёо 2.4.2 Deep Neural Network алгоритмын томъё

$$E(X) = f_{NN}(X) \quad (3)$$

- X : Оролтын аудио сигнал
- f_{NN}: Нейрон сүлжээ

2.4.3 Pyannote-Кластеринг (Clustering)

Энэхүү шатанд эмбеддинг хийгдсэний үр дүнд илэрсэн шинж чанаруудыг ангилах үйл явц хийгддэг [5]. Кластеринг нь Agglomerative Hierarchihal Clustering (AHC) алгоритм дээр суурилагдаж гүйцэтгэгддэг [томьёо 2.4.3].

Томьёо 2.4.3: AHC алгоритмын томьёо

$$D(E_i \cdot E_i) = 1 - (E_i \cdot E_j) / || E_i || || E_i || \quad (4)$$

Хувьсагчид:

- $E_i \cdot E_j$ = *Эмбеддинг үе шатны үр дүн*
- $|| E_i || || E_i ||$ = *Эвклидийн зай*

2.5 Large Language Model

/Эмийн жорыг стандартын дагуу боловсруулах/

Эмч, эрүүл мэндийн мэргэжилтэн болон өвчтөний хоорондын аудио өгөгдлөөс хөрвүүлэгдсэн текстийг бүх шатны эрүүл мэндийн байгууллага, эмийн сангууд үйл ажиллагаандаа ашигладаг MNS 5376:2016 стандартын дагуу эмийн жор боловсруулж гаргахад бүтэцлэгдсэн өгөгдлийг нейрон сүлжээний алгоритмаар боловсруулдаг трансформер моделийг ашиглав. Энэ нь “self-attention” функц дээр тулгуурлан ажилладаг.

III. Судалгааны хэсэг

3.1 Ижил төстэй системийн судалгаа

Эрүүл мэндийн салбарын эмч, мэргэжилтнээс өвчтөнд зориулан бичдэг эмийн жорыг хиймэл оюун ухааны дэвшилтэт технологи ашиглан автоматжуулах, эмчийн ачааллыг бууруулах, цаасан эмийн жорын хэрэглээг дижитал хэлбэрт шилжүүлэх системүүдийг дэлхийн улс орнууд хэрэглээндээ нэвтрүүлсэн байна. Харин АНУ, Их Британи, Швед зэрэг европын ихэнх орнууд эм олгох цахим системийг ашигладаг байна. Тэдгээрийн ажиллах зарчим, ашигласан технологиудыг судалсны үндсэн дээр үр дүнг хүснэгт 2-т оруулаа.

Төстэй системийн судалгааны үр дүн

2-Р ХҮСНЭГТ

Улс	АНУ	Их Британи	Швед
Систем	ERX Network	Electronic Prescription Service (EPS)	ePrescription
Ажиллах зарчим	Эмч нар эмийн жорыг цахимаар бичиж, эмийн сан руу илгээдэг	Эмч нар эмийн жорыг цахимаар үүсгэж, өвчтөн сонгосон эмийн сангаасаа эмээ авдаг	Өвчтөн эмийн сангаас иргэний үнэмлэхээрээ эмээ авдаг
Ашигласан технологи	**NLP** **- Graph-based AI**: Эмийн харилцан үйлчлэлийг шинжлэх	**NLP**: Эмийн жорын өгөгдлийг боловсруулах **- Predictive Analytics**: Өвчтөний эмийн хэрэглээг таамаглах	**Machine Learning**: Эмийн жорын хэв маягийг шинжлэх **- Anomaly Detection**: Хуурамч жор илрүүлэх

3.2 Монгол улсын эм зүйн салбарт ашиглагддаг программ хангамжуудтай холбогдох боломжийн судалгаа

Монгол улсын хувьд E-Mongolia төрийн нэгдсэн мэдээлэл, үйлчилгээний системд байршсан эмийн жор цэс нь одоогийн байдлаар ажиллагаагүй байна [13]. Эрүүл мэндийн салбарт үйл ажиллагаа явуулж буй эмийн сангууд нь ORION PHARM [12], MEDACCOUNT[10], MPharmaPOS, Smart Pharmacy [11] зэрэг программ хангамжуудыг ашигладаг байна. Эдгээр системүүдийн ажиллах орчин, ашигласан технологи, давуу, сул талуудыг судлан хүснэгт 3-т харуулав. Үүний үр дүнд эмийн жор бичээч ухаалаг системд эмийн жор нь тухайн өвчтөний регистрийн дугаараар бүртгэгдэж, эдгээр программ хангамжуудад холбогдох боломжтой.

Эмийн санд ашиглагддаг системүүдийн судалгаа [10,11,12]

3-Р ХҮСНЭГТ

Систем	ITPark - ORION PHARM	Andromeda MEDACCOUNT	MindGolia Smart Pharmacy	MindGolia MPharma POS
Ажиллах орчин	Windows	Windows	Windows	Windows
Ашигласан технологи	C#, .NET Framework, SQL Server	Java, PostgreSQL	JavaScript	Python, Django, SQLite
Давуу тал	ЭМДСангаас хөнгөлөлт үзүүлэх 200 эмийн бүртгэлтэй.	Агуулахын бүртгэл хийх боломжтой.	Олон салбартай эмийн сангууд ашиглахад тохиромжтой.	ЭМД-ын цахим системтэй холбогдсон.
Сул тал	Эмийг жороор олгохдоо	Эмийн бүртгэлийг гар	Жороор олгох эмийн	Эмийн жорын бүртгэл
	иргэний мэдээллийн үнэн зөв эсэхийг шалгадагүй.	аргаар, өөрсдөө хийдэг.	бүртгэл огт хийдэггүй.	огт байхгүй.

IV. Хөгжүүлэлт

Эрүүл мэндийн байгууллагад ажилладаг эмч, эмийн жор бичиж өгөх эрх бүхий этгээд үзлэгийн аудиог оруулах юм. Үүнээс стандартын шаардлагад нийцсэн эмийн жор болон өвчтөнд зориулсан зөвлөгөөг боловсруулан эмийн сангийн систем, E-Mongolia систем рүү илгээх боломжтой юм. Мөн боловсруулагдсан эмийн жорыг pdf, docx өргөтгөлтэйгөөр татаж авах боломжтой.

4.2 Алдааны тооцоолол

Яриан дээрх үг хэллэгүүдийг зав таньж, бичсэн эсэхийг Word Error Rate(WER) метрикээр, стандартын дагуу бүрэн бүтэн, үнэн зөв эмийн жор бичсэн эсэхийг Cross Entropy Loss (CEL) метрикээр тус тус хэмжиж гаргав. Үүний үр дүнд үгийн алдааны хувь = 6.3722, эмийн жорын алдааны хувь = 23.8542 гарлаа.

$$\textit{Яриа танилтын алдааны хувь} = \frac{\textit{алдаж таньсан хугацааны тоо}}{\textit{нийт ярианы хугацаа}} = 5.8542$$

Томьёо 4.3.1 DER метрикийн томьёо

$$\textit{Үгийн алдааны хувь} = \frac{\textit{зассан үгийн тоо} + \textit{устгасан үгийн тоо}}{\textit{нийт үгийн тоо}}$$

Томьёо 4.2.2 WER метрикийн томьёо

Эмийн жорын алдааны хувь = бодит утга * log(боловсруулагдсан утга)

Томьёо 4.2.1 LLM моделийн алдааг тооцох томьёо

ДҮГНЭЛТ

Энэхүү судалгааны ажлаар эрүүл мэнд, байгаль экологийн салбарт тулгамдаж буй асуудлуудын нэг болох эмийн жорыг гар аргаар бичиж, цаасан хэлбэрээр ашигладаг үйлдлийг хиймэл оюун ухааны дэвшилтэт технологийн тусламжтайгаар автоматжуулах, ингэснээр эмч, эмнэлгийн ачааллыг бууруулах, эмийн жорын цаасан хэрэглээг халах ухаалаг, эрүүл мэндийн ногоон технологийг шийдлийг боловсруулахаар зорилоо. Тус систем нь эмчийн үзлэгийн ярианаас стандартын шаардлагад нийцсэн эмийн жорыг боловсруулан, эмийн сангийн систем болон E-Mongolia систем рүү илгээснээр иргэд, эмийн санч, эмнэлэг эм олгох үйл явцыг хянах боломжоор хангасан болно. Ингэснээр эмийн жор олгоход зарцуулагддаг 20-40 минутын хугацааг, 3 минут хүртэл бууруулах, байгалийн гаралтай, эко

амьдралын хэв маягийг дэмжсэн, ахуйн нөхцөлд хэрэгжүүлэх боломжтой эмчилгээ, зөвлөгөөг боловсруулах юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Rajpurkar, P., Chen, E., Banerjee, O., & Topol, E. J. (2022). AI in health and medicine. *Nature medicine*, *28*(1), 31-38.

[2] Batta, A., & Singh, B. (2018). Rational approach to prescription writing: A preview. *Neurology India*, *66*(4), 928-933.

[3] Wang, S., Yang, C. H., Wu, J., & Zhang, C. (2024, April). Can whisper perform speech-based in-context learning?. In *ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 13421-13425). IEEE.

[4] Sharaf, N. I. (2024). PRESCRIPTION AUTOMATION: ENHANCING MEDICATION SAFETY AND HEALTHCARE EFFICIENCY. *Gland Surgery*, *9*(2), 416-442.

[5] Soeny, K., Pandey, G., Gupta, U., Trivedi, A., Gupta, M., & Agarwal, G. (2021). Attended robotic process automation of prescriptions' digitization. *Smart Health*, *20*, 100189.

[6] Chen, H. K., Chen, F. H., & Lin, S. F. (2021). An ai-based exercise prescription recommendation system. *Applied Sciences*, *11*(6), 2661.

[7] Bredin, H. (2023, August). pyannote. audio 2.1 speaker diarization pipeline: principle, benchmark, and recipe. In *24th INTERSPEECH Conference (INTERSPEECH 2023)* (pp. 1983-1987). IS4CA.

[8] Монголын гааль - https://customs.gov.mn/

[9] Монгол эм импекс концерн - meic.mn

[10] https://andromeda.mn/

[11] https://mindgolia.mn/

[12] http://www.orion.mn/

[13] https://e-mongolia.mn/service/emiin-jor

[14] Эмийн жор бичих MNS 5376:2016 стандарт

[15] Ач интернешнл эмнэлэг

[16] АШУҮИС-ийн Монгол-Японы эмнэлэг

3D ХЭВЛЭМЭЛ ГАРЫГ УДИРДАХ ХИЙМЭЛ ОЮУНЫ ЗАГВАРЫН ХӨГЖҮҮЛЭЛТ

Мөнхзулын САРАНГЭРЭЛ[1], Бадарчийн ЛУУБААТАР[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Электроникийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: msarka0310@gmail.com[1], luubaatar@gmail.com[2]

Хураангуй*: Сүүлийн жилүүдэд 3D хэвлэмэл гар болон био-хянагддаг протезын хэрэгцээ дэлхий даяар нэмэгдэж байна. Одоогийн байдлаар зах зээл дээрх уламжлалт протез гарууд өндөр үнэтэй, хүнд жинтэй, хэрэглэгчийн хэрэгцээнд бүрэн нийцэхгүй байх асуудалтай байна. 3D хэвлэмэл гар нь бодит гарын хөдөлгөөний үйлдлийг гүйцэтгэх боломжтой төхөөрөмж юм. Энэхүү судалгааны ажлаар EMG (electromyography) мэдрэгч дээр суурилсан хиймэл оюун ухааны загвараар 3D хэвлэмэл гарыг удирдах технологийг хөгжүүлэх зорилготой. Энэхүү судалгааны ажлаар EMG (булчингийн цахилгаан идэвхжил) мэдрэгч дээр суурилсан хиймэл оюун ухааны (ХОУ) загвараар 3D хэвлэмэл гарыг удирдах технологийг хөгжүүлэх зорилготой. Судалгаанд EMG сигналын шүүлтүүрийн аргууд (Notch, High-pass, Low-pass), онцлог шинж чанар гарган авах техникүүд (RMS, MAV, FFT) болон нейрон сүлжээнд суурилсан ангиллын аргуудыг ашигласан.

Түлхүүр үг: EMG дохио, хиймэл оюун ухаан, нейрон сүлжээ, микроконтроллер, серво мотор

I. УДИРТГАЛ

Хиймэл гар нь дээд мөчний тайралттай хүмүүст байгалийн гарын зарим функцийг хангах зориулалттай төхөөрөмж юм. Өнөө үед арилжааны хэд хэдэн протезын төхөөрөмжүүд байдаг. Эдгээр төхөөрөмжүүд нь идэвхгүй хиймэл гараас эхлээд биеийн бэхэлгээний цахилгаан дэгээ, миоэлектрик дэгээтэй гар хүртэл гэх мэт байдаг. Миний хийхээр зорьж буй уг төсөл нь байгалийн гарын хөдөлгөөнийг бүрэн орлох хэмжээний робот гарыг хийх юм. Судалгаанаас үзэхэд манай улсад жилд нийт 1500-1700 хүн хиймэл гар хөлийг хийлгэдэг. Дэлхийн зах зээлд протез нь 2024 оны байдлаар 8,7 тэрбум долларын үнэлгээтэй байна[1].

Энэхүү судалгааны ажлаар робот гарын хөдөлгөөнийг гарын шуунаас авсан EMG дохиог боловсруулан робот гар дээрх микроконтроллерт дамжуулж хиймэл оюун ухаан машин сургалт ашиглан моторын хөдөлгөөнийг удирдах зорилго тавин ажиллав.

II. СУДЛАГДСАН БАЙДАЛ

A. Төсөөтэй сэдвийн судалгаа

Энэхүү ажлыг өмнө нь судалж, хэрэгжүүлсэн судалгааны аргачлалуудыг нарийвчлан судлахын тулд дараах гурван ижил төстэй сэдвийг шинжиллээ.

- **1. Deep Learning Approach to Control of Prosthetic Hands with Electromyography Signals**

Энэхүү судалгаанд **8 сувагтай хуурай электрод** ашиглан EMG дохиог хүлээн авч, **CNN (Convolutional Neural Network)** загварын оролтод өгч **15 төрлийн гарын хөдөлгөөн** таних байдлаар сургасан.

- **Дээж авах хурд:** 2000 өгөгдөл/секунд
- **Техник хангамж:**
  a) EMG өгөгдөл цуглуулах схем
  b) GPGPU хөгжүүлэлтийн платформ
  c) Актуаторын драйверын хэлхээ
  d) Хүчдэл тогтворжуулагч хэлхээ
  e) Робот гарын байрлал шалгах хэлхээ

- **2. Design and Implementation of Prosthetic Hand Control using Myoelectric Signal**

Энэхүү систем нь **шууны 3 сувгаас EMG өгөгдөл** хүлээн авч, **ANN (Artificial Neural Network)** ашиглан **атгах, чимхэх, нээх** гэсэн **3 төрлийн хөдөлгөөнийг** ангилсан.

- **Онцлог шинж тэмдэг:** 21 төрлийн онцлог
- **Ангилалтын нарийвчлал:** 87-91%
- **Техник хангамж:**
  a) Хүчдэл тогтворжуулах хэлхээ
  b) Булчингийн дохио хүлээн авах хэлхээ
  c) Микроконтроллер драйверын хэлхээ

- **3. Real-time Bionic Arm Control Via CNN-based EMG Recognition**

Энэхүү судалгаанд **шууны 8 сувагтай EMG мэдрэгч** ашиглан, **Bluetooth** холболтоор микроконтроллерт дамжуулан **CNN загвараар 4 төрлийн гарын хөдөлгөөн** ангилж, **3 серво мотор** удирдан робот гарыг хөдөлгөсөн.

- **Техник хангамж:**
  a) EMG мэдрэгчийн өгөгдлийг хүлээн авах ба дамжуулах хэлхээ
  b) Өгөгдөл боловсруулах нэгж
  c) Тэжээлийн блок

Эдгээр судалгааны ажлууд нь **EMG дохиог ашиглан робот гарын хөдөлгөөнийг удирдах** аргачлалд **гүн сургалт (CNN), нейрон сүлжээ (ANN)** ашиглах боломжийг харуулсан бөгөөд техник хангамжийн хувьд **микроконтроллер, хүчдэл тогтворжуулагч, драйверын хэлхээнүүд** зэрэг нийтлэг элементүүдийг ашигласан байна.

B. Протезийн судалгаа

Протезийн анхны хэрэглээ нь МЭӨ 3000 оны үеэс Египетийн соёл иргэншилд илэрч байжээ (Salminger et al., 2019). Дундад зууны үед мод болон төмөр материалаар хийсэн механик протезүүд хэрэглэгдэж байсан бөгөөд 20-р зуунд бионик болон электроник удирдлагатай протезүүд хөгжиж эхэлсэн байна (Zuo & Olson, 2014).

Орчин үед дараах төрлийн протезууд байна. Үүнд:

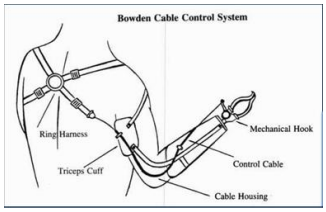
Идэвхгүй протез

Идэвхгүй протез нь хүнд илүү гоо сайхан талаасаа хэрэглэгддэг ямар нэгэн хөдөлгөөнгүй төхөөрөмж юм.

1-р зураг. МЭӨ 950-710 оны үеийн Египетийн мумми дахь хиймэл хөл

Механик протез

Мөр болон тохойн хөдөлгөөнөөр хиймэл гарыг удирддаг. Энэ нь маш энгийн бөгөөд ихээр хэрэглэгддэг протезын төрөл



2-р зураг. Биеийн хөдөлгөөнөөр хөдөлдөг хиймэл гар

Миоэлектрикт суурилсан хиймэл гар

Энэ протез нь хүний булчингийн агшилтаас үүссэн цахилгаан миографи дохиог хэмждэг. Эдгээр дохиог арьсны гаднаас эсвэл булчингийн дунд суурилуулсан электродоос дохиог авч тэрхүү дохиог боловсруулан микроконтроллероор гарын хөдөлгөөнийг удирддаг.

Зураг 3. EMG дохионд суурилсан хиймэл гар

Тархины дохиогоор удирдах

Хамгийн сүүлийн үеийн хяналтын төрөл бол тархины мэдрэлийн интерфейс юм. Өвчтөн бодлоороо робот гарын хөдөлгөөнийг удирддаг төрөл юм. Энэ төрлийн технологи нь анхан шатандаа байгаа хэдий ч хөгжлийн бэрхшээлтэй хүмүүст зөвхөн өөрсдийн бодлоор бионик төхөөрөмжийг удирдаж байгааг харуулсан.

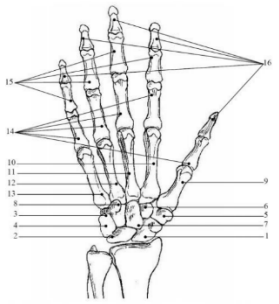
4-р зураг. Тархины мэдрэлийн мэдээллийг ашигласан хиймэл гарын загвар

C. Хүний гарын антомийн судалгаа

3D хэвлэмэл гарын хэлбэр загвар болон хурууны хөдөлгөөнийг удирдах гол булчинг сонгохийн тулд хүний гарын антомийн судалгааг хийх нь чухал юм.

Хүний гар нь олон янзын хэсэг, зургаан өөр үе, хоёр өөр булчингийн бүлэг, гурван өөр мэдрэл, ясаас бүрдэнэ [7]. Хүний гар нь гурван бүлэгт хуваагддаг 27 яснаас бүрддэг.

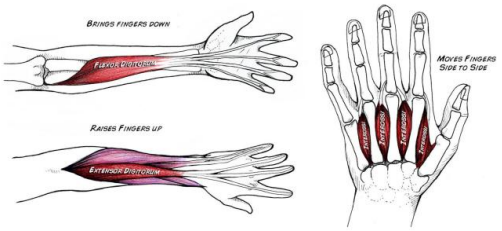
- 14 хурууны шивнүүр яс
- Алганы яс
- Бугуйн яс



5-р зураг. Хүний гарын ясны бүтэц

(1. Scaphoid, 2. Lunate, 3. Triquetrum, 4. Pisiform, 5. Trapezium, 6. Trapezoid, 7. Capitate, 8. Hamate)

Хүний гарын шууны агших булчин (flex digitorum), сунгах булчингууд (extensor digitorum) шөрмөсөөр дамжууран хуруунуудын хөдөлгөөнийг удирддаг. Ийм учраас уг ажилаар робот гарын сарвууны хөлгөөнийг гарын шууны булчингаас мэдээлэл авч хийж гүйцэтгэхээр зорив.



6-р зураг. Хүний гарын шууны булчин

D. EMG электрод судалгаа

Булчингийн цахилгаан идэвхийг (EMG) хэмжихийн тулд электродыг ашигладаг. EMG электродыг хоёр үндсэн төрөлд ангилна:

Гадаргуун электрод (Surface EMG) – Арьсан дээр байршуулдаг электрод.

- **Давуу тал**: Ашиглахад хялбар, өвдөлтгүй.
- **Сул тал**: Гадны шуугианд өртөмтгий, гүн булчингийн дохиог сайн хэмжиж чаддаггүй.
- **Хэрэглээ**: Робот гарын судалгаа, сэргээн засах эмчилгээ, спортын биомеханик, нейроинтерфэйс.

Зүү электрод (Needle EMG) – Булчин руу хатгаж байрлуулдаг электрод.

- **Давуу тал: Гүн булчингийн дохиог өндөр нарийвчлалтай хэмждэг.**
- **Сул тал: Өвдөлт үүсгэх, байрлуулахад төвөгтэй.**
- **Хэрэглээ**: Анагаах ухааны судалгаа, биомеханик, спортын шинжилгээ, протез, нейроинтерфэйс, тархи-булчингийн интерфэйс.

Эдгээр электродыг судалгаа, анагаах ухаан, роботик, спортын шинжилгээ зэрэг олон салбарт ашигладаг. Гадаргуун электрод нь хэрэглэхэд хялбар тул ихэвчлэн гадаргуугийн булчингийн идэвхийг судлахад тохиромжтой бол зүү электрод нь нарийвчлал шаардсан, гүн булчингийн дохиог хэмжих хэрэгцээтэй нөхцөлд илүү үр дүнтэй байдаг.[2]

Энэхүү судалгааны ажлын хүрээнд гадаргуун электродуудыг ашиглан туршилтуудаа хийсэн. Гадаргуун электрод нь дараах 2 төрөл байна.

Хуурай электрод (Dry Electrode) – Арьсанд шууд хүрч, гель түрхэх шаардлагагүй.

Гельтэй электрод (Gel-based Electrode) – Арьс ба электродын хооронд гель түрхэж, дохио дамжуулалтыг сайжруулна.

Уг 2 электродын аль алинийг нь ашиглах боломжтой боловч олон удаагийн туршилтанд зориулан хуурай электродыг сонгон авч туршилтуудыг хийж гүйцэтгэв.

III. АРГА ЗҮЙ БА ҮР ДҮН

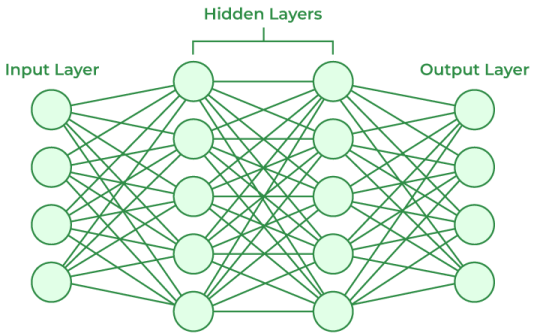
A. EMG дохио

Хүний булчингийн эдүүд нь агшиж сунаж байхдаа тархины мэдрэлийн эсээс үүдэлтэйгээр бага хэмжээний цахилгаан дохиог ялгаруулдаг. Энэ цахилгаан дохиог электромиографи буюу EMG гэж нэрлэдэг. Хүний булчингийн эд нь бүтэц, агшилт суналтын шинж чанараас хамааран хөндлөн судалт булчин (skeletal muscle), гөлгөр булчин (smooth muscle), өвөрмөц хөндлөн судалт булчин (cardiac muscle) гэсэн 3 төрөл байна. EMG дохиог хөндлөн судалт булчингаас мэдээлэл авдаг. Хөндлөн судалт булчин нь хүний ясанд наалддаг бөгөөд хөдөлгөх үүрэгтэй байдаг. Мэдрэлийн эсийн өдөөлтөд булчингийн өгсөн хариу үйлдлийг деполяризаци гэдэг бөгөөд энэ деполяризаци нь булчингийн ширхэг бүрийн ойролцоо цахилгаан орон үүсгэдэг. EMG дохио нь өсгөөгүй үедээ 0-10 мВ амплитудтай 0-500Гц хооронд хэлбэлздэг дохио юм[3].

B. Нейрон сүлжээ

Нейрон сүлжээний арга нь хяналттай сургалтын нэг хэсэг бөгөөд оролтод харгалзах гаралтыг таамаглахад регресс, ангиллын аргыг ашигладаг. Нейрон сүлжээ нь бүтцийн хувьд оролт, гаралт, нуугдмал давхаргуудаас бүрддэг.

Нейрон сүлжээний чухал зүйлс нь forward propagation, back propagation. алдааны функц гэх ойлголтууд юм.



7-р зураг. Нейрон сүлжээний архитектур

1. Жинтэй нийлбэр олох

$$Z = W \cdot X + b$$

- W – жингийн матриц
- X – оролтын өгөгдөл
- b – хазайлт

2. идэвхжүүлэгч функц ашиглах

$$A = f(Z)$$

- $f -$ идэвхжүүлэгч функц
- ReLU: $f(Z) = \max(0, Z)$
- Sigmoid: $f(Z) = \frac{1}{1+e^{-Z}}$
- Tanh: $f(Z) = \frac{e^{Z}-e^{-Z}}{e^{Z}+e^{-Z}}$

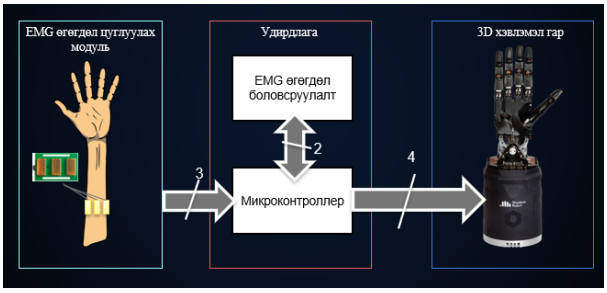
3. Сүлжээний давхарга бүр дээр ийм үйлдэл хийгдэж сүүлийн давхаргад гаралтыг утга гарна.

C. Системийн ажиллах зарчим

Санамсаргүй байдлаар гараа алдсан хүний гараа удирдах дохио болон гартай хүний гараа удирдах дохио ижил тул эхний ээлжид өөрийн гарын шуунаас гарыг атгах болон тэнийх 2 байрлалд дохио авч боловсруулсан.

Хүний гарын шууны булчингаас хуурай электрод ашиглан атгах болон тэнийг гэсэн 2

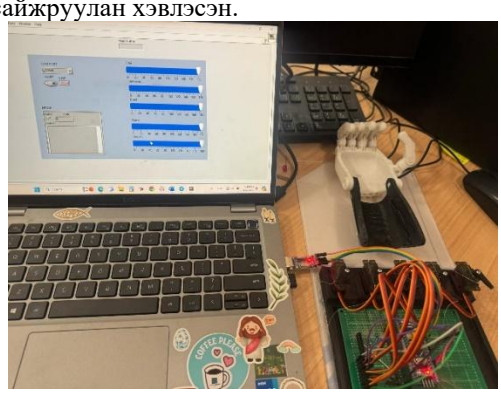
төрлийн хөдөлгөөний дохиог авсан бөгөөд уг дохиог микроконтроллерын ADC (analog to digital converter) ашиглан компьютерт өгөгдлийг авсан. Авсан өгөгдлөөс онцлогуудыг гаргаж машин сургалтын CNN загварын оролтод өгч сургасан бөгөөд гаралтад 0, 1 гэсэн шошго гарч ирнэ. Уг тоог серво моторын удирдлагат өгч гарын хөдөлгөөнийг удирдсан. Доор системийн бүтцийн схемийг харуулав.



7-р зураг. Системийн бүтцийн схем

D. Үр дүн

Эхний ээлжид механик хэсгийн удирдлагыг ажиллуулахын тулд labview программ ашиглан робот гарын хөдөлгөөнийг удирдсан. Эхний загварын гарын хөдөлгөөн болхи буцаж татах хөдөлгөөн хийж чадахгүй байсан тул робот гарыг илүү сайжруулан хэвлэсэн.



8-р зураг. Робот гарын механик хэсгийн туршилт

9-р зураг. Робот гарын сайжруулсан загвар.

Өгөгдөл цуглуулахдаа 2 төрлийн аргаар цуглуулсан бөгөөд эхний удаа хуурай электродтой мэдрүүрийг flexor булчин дээр, гелэн электродтой мэдрүүрийг extensor булчин дээр тавьж 7000 мөр дата цуглуулсан. Дээж цуглуулахдаа 1 секундэд 1000 өгөгдөл байхаар авсан бөгөөд CNN загварыг ашиглан сургасан.

10-р зураг. Хуурай электродыг байрлал

11-р зураг. Гелэн электродын байрлал

12-р зураг. Сургалтын үр дүн

Дараагийн туршилтад хуурай электрод 3г байршуулан. 1кГц давтамжтай 200000 өгөгдөл бэлтгэж CNN загвараар сургав.

13-р зураг. Хуурай электродуудын байрлал.

14-р зураг. Үр дүнгээс

ДҮГНЭЛТ

Emg дохио нь 50-500 Гц-н давтамжтай дохио бөгөөд энэ удаа атгах болон тэнийх хөдөлгөөнийг секундэд 1000 дээж авч өгөгдөл цуглуулан neural network ашиглан сургав. Эхний ээлжид 40% н нарийвчлалтай байсан ч машин сургалтын оролтыг нэмэгдүүлэн өгөгдлөө 10р нь багцалж өгөн дахин сургахад 70% нарийвчлалтай болж нэмэгдсэн. Дараагийн удаа мэдрүүрийн тоо болон өгөгдлийн нэмэгдүүлж дахин сургахад 80% нарийвчлалтай болж нэмэгдэв.

Үүнээс харахад мэдрүүрийн тоо болон өгөгдлийн тоо нь сургалтын чанарт нөлөөлж байна.

Цаашид өгөгдлөө цонхолж машин сургалтын загварын оролтод өгч робот гарын хөдөлгөөний тоог олшруулан сургах төлөвлөгөөтэй байна.

НОМ ЗҮЙ

[1] Prosthetics and Orthotics Market Size to Hit USD 13.94 Bn by 2034

[2] https://en.wikipedia.org/wiki/Electromyography

[3] De Luca, C. J. (1997). The use of surface electromyography in biomechanics. *Journal of Applied Biomechanics*, 13(2), 135-163

[4] Akif Rahmatillah, L. S. (2019). Design and Implementation of Prosthetic Hand Control using Myoelectric Signal.

[5] Manan Kubaj Gupta (2021). Prosthetic Arm with Microcontroller.

[6] Reinis Geizans (2018) Developing 3D Printed Prosthetic Hand Model controlled by EMG Signal from Forearm.

[7] Ж. Билгүүн. Гар сарвууны гэмтэл

[8] Kothamangalam. Biomic hand

[9] https://embedded-lab.com/blog/lab-21-servo-motor-control/

[10] https://eguur.mn/334133/

ДРОН УНАГААХ ТӨХӨӨРӨМЖИД ЗОРИУЛСАН ӨНДӨР ҮЗҮҮЛЭЛТТЭЙ АНТЕНЫ ХӨГЖҮҮЛЭЛТ

Түвшинтөгсийн АМАРТӨР[1], Баярсайханы ПҮРЭВДЭМБЭРЭЛ[1], Ганбаатарын ДӨЛМАНДАХ[1], Баярсайханы ПҮРЭВЦЭРЭН[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Холбооны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: pvrwee799@gmail.com[1], gdolmandah@gmail.com[2]

Хураангуй: **Технологийн эрин зууны онцлох технологи нь дрон буюу нисгэгчгүй нисэх төхөөрөмж болоод байна. Дроныг худалдаа, аюулгүй байдал, хэвлэл мэдээлэл, медиа болон цэрэг армийн зориулалтаар өргөнөөр ашиглах болсон байна.Гэвч зарим нэг хууль эрх зүйн зохицуулалтгүй дроны хэрэглээнд эсрэг арга хэмжээ авах технологи хөгжүүлэх шаардлага нэмэгдэж байна. Дрон саармагжуулах судалгаанууд байгаа ч, ялангуяа дрон эсэргүүцэгч (жаммер) антенуудын талаарх судалгаанууд цөөн байна.Ихэвчлэн Yagi-Uda антен ашигласан судалгаа болон төхөөрөмжүүд байна.Харин энэхүү судалгаанд дрон саатуулах зориулалттай өндөр хүчин чадалтай 'helix' антеныг боловсруулж, оновчтой болгосон болно. 'Helix' антен нь чиглэлийн диаграмм нарийн, өндөр өсгөлттэй тул 2.4 ГГц болон 5.8 ГГц давтамжийн цард дроны ажиллагааг үр дүнтэйгээр саатуулах боломжтой. Антены загварыг** CST Microwave Studio **программ ашиглан боловсруулж, симуляцийн орчинд туршсан.Антены өсгөлтийг нэмэгдүүлж, чиглэлийн диаграммыг багасгахын тулд чиглүүлэгч линзийг нэмж оруулсан. Туршилтын үр дүнд уг антен нь 5.8ГГц давтамж дээр** 14 dBi **өсгөлттэй, 29⁰ чиглэлийн өргөнтэй болсон ба дрон саатуулахад төхөөрөмжид тохиромжтой.**

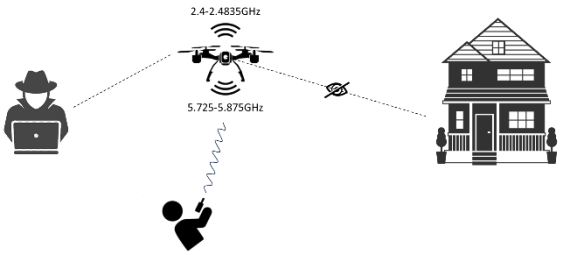
Түлхүүр үг: 2.4ГГц, 5.8ГГц, Өсгөлт, helix антен, чиглэлийн диаграмм

I. УДИРТГАЛ

Сүүлийн үед дронуудын тоо хурдацтай нэмэгдэж, энгийн иргэдээс эхлээд цэргийн зориулалт хүртэлх олон салбар, хэрэглээнд өргөн ашиглагдах болсон. Дронуудын тоо өсөхийн хэрээр тэдгээрийг саармагжуулах, гажуудуулах (жаммер) төхөөрөмжийн хэрэгцээ улам бүр нэмэгдэж байна. Өмнө нь дронуудыг жаммер ашиглан эсэргүүцэх талаар судалгаа хийгдэж байсан [1]. Гэвч ихэнх ийм төрлийн төхөөрөмжүүд болон дрон эсэргүүцэх системүүд зөөврийн бус байдаг. Зөөврийн дрон эсэргүүцэх төхөөрөмж нь дроны аюулд яаралтай хариу арга хэмжээ авахад чухал ач холбогдолтой. Тэдгээрийн дотроос радио давтамжийн (RF) бууг ашиглан дронуудыг саармагжуулах арга тохиромжтой юм. Дрон эсэргүүцэх төхөөрөмжийн антен нь олон төрлийн давтамжийн зурвасуудыг хамрах ёстой. Дронууд нь өөрийн байршлыг тодорхойлоход Глобал Байршил Тогтоох Систем (GPS) L1 зурвас (1562.92–1587.92 МГц)-ыг ашигладаг [2,3].

ISM 2.4 ГГц (2.4–2.4835 ГГц) болон 5.8 GHz (5.725–5.875 ГГц) зурвасууд нь дрон болон алсын удирдлагатай холбоо тогтооход өргөн хэрэглэгддэг [4,5]. Мөн эдгээр зурвасууд нь дронуудаас газарт зураг болон бичлэг дамжуулахад ашиглагддаг.

Өргөн чиглэлийн диаграмм нь том талбайг саармагжуулах боломжтой ч зорилтот бус бусад дронууд эсвэл объектуудыг санамсаргүйгээр ажиллагаагүй болгох эрсдэлтэй.Иймд нарийн чиглэлийн диаграмм илүү тохиромжтой.

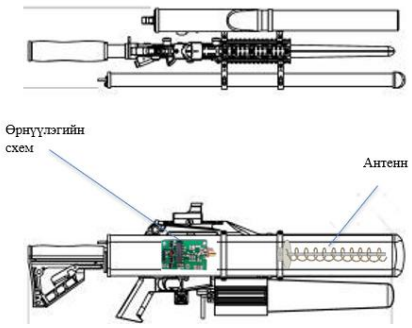


1-р зураг. Ажиллагааны зарчим

Дрон саатуулах системийн гол бүрэлдэхүүн хэсэг болох антен нь өндөр өсгөлттэй, нарийн чиглэлийн диаграммтай, тогтвортой ажиллах чадвартай байх шаардлагатай. Тэгвэл "Helix" антен нь тойрог туйлшралтай, бага алдагдалтай, авсаархан хэмжээтэй тул дрон саатуулах хэрэглээнд хамгийн тохиромжтой шийдэл болох юм.

II. ТӨХӨӨРӨМЖИЙН БҮТЭЦ

RF саатуулах төхөөрөмжийг нэгэн төрлийн долгионы буу гэж үзэж болох бөгөөд одоогийн байдлаар судлагдаж буй ихэнх төхөөрөмжүүд дараах хэлбэртэй болно. Энэхүү төхөөрөмж нь хэд хэдэн үндсэн хэсгээс бүрдэх бөгөөд уг бүтцийг Зураг.2-т үзүүлэв.

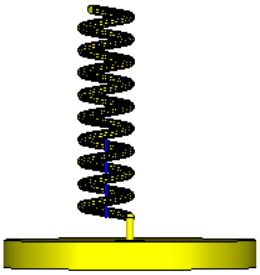


2-р зураг. Төхөөрөмжийн бүтэц

1. Антен нь 2.4ГГц болон 5.8ГГц ажлын давтамжтай мушгиа хэлбэрийн өндөр өсгөлттэй нарийн чиглэлтэй байна .
2. Дохио өрнүүлэх хэлхээ нь тухайн давтамжийн зурваст үр дүнтэй ажиллах чадвартай, өндөр үр ашигтай хэлхээ байна.
3. Гадна их бие нь 3D дизайны тусламжтай гаргасан сайжруулсан хуванцар материалаар хийсэн загвар.

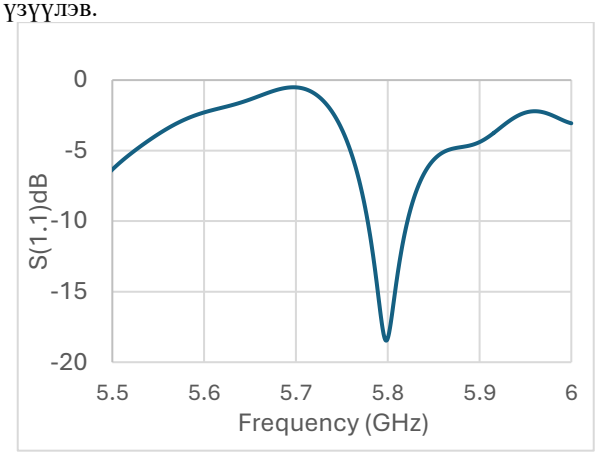
III. АНТЕН ДИЗАЙН

Энэхүү антен нь зураг.2-т үзүүлсэн мушгиа хэлбэртэй антеныг загварчилж зэс линзийг байрлуулж 2.4ГГц болон 5.8ГГц давтамжууд дээр тааруулсан. Ингэхдээ CST Studio Suite симуляцийн программ дээр гүйцэтгэсэн. Зэс утасны диаметр 2 мм, урт 133 мм, алхамт хоорондын зай 3 мм.

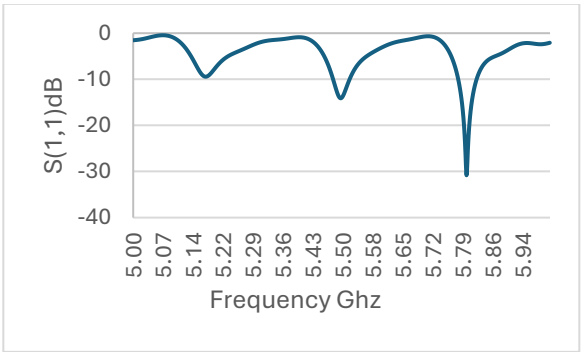


3-р зураг. а.5.8 ГГц Helix *б. 5.8 ГГц Tape Helix антены бүтэц*

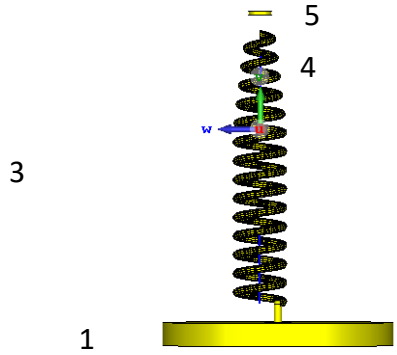
Одоогоор 5.8ГГц-ийн антеныг загварчилсан. Энэ нь ойлгогч(1), тэжээлийн хэсэг(2), антен(3), tape антен(4), линз(5) зэргээс бүрдэнэ. Зураг.4-т антены симуляцийн үр дүнд гарсан ойлтын коэффициентыг үзүүлэв.

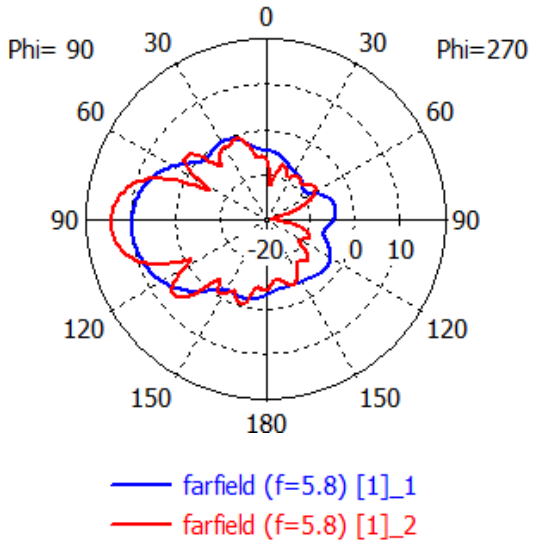


4-р зураг. а 5.8 ГГц антенны симуляци дээрх ойлтын коэффициент



5-р зураг. б 5.8 ГГц tapered линзтэй антены симуляци дээрх ойлтын коэффициент





Зураг.4.в 5.8 ГГц антены симуляци дээрх чиглэлийн диаграмм

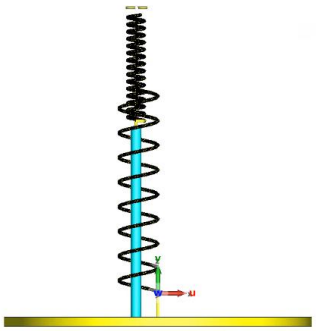
Зураг.3.а дээр энэ антен нь -18.4 dB Зураг.3.б-д -31 dB-г 5.8 ГГц давтамж дээр үзүүлж байна. Зураг (3а), (3б)-д харуулснаар дрон ажиллах давтамж дээр ‘helix’ антены үзүүлэлтийг сайжруулан ажиллуулах боломжтойг харуулж байна. Мөн 5.8ГГц давтамжийн helix антен дээр нэмэлтээр металл линзийг байрлуулснаар чиглэлийн диаграммыг 52.1º(зураг.3.в.1)-с 29º (зураг.3.в.2) болгож бууруулсан. Энгийн helix антены өсгөлт 9.63dbi байсан бол tapered helix антен 14dbi юм.

1-Р ХҮСНЭГТ TAPERED БОЛОН ЭНГИЙННELIX АНТЕНЫ СИМУЛЧЦИЙН ХАРЬЦУУЛАЛТ

	S1.1 (db)	Өсгөлт (dbi)	Цацраг-ийн өргөн
Helix	-18.4	9.63	52º
Tapered helix	-31	14	29º

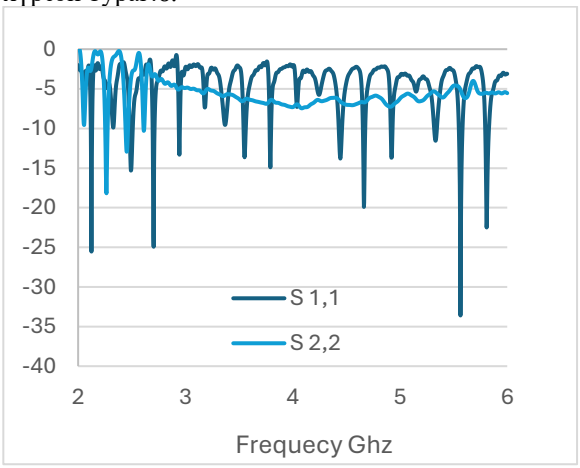
IV. ҮР ДҮН

Мөн хосолсон зурваст ажиллах нь үндсэн зорилгын нэг бөгөөд үүнийг хийхийн тулд тухайн 2 антеныг нэгтгэж тэжээлийн 2 порттой байхаар зохицуулсан бөгөөд үүний загварыг зураг.5-т харуулав. Антены нийт урт 20.4см.

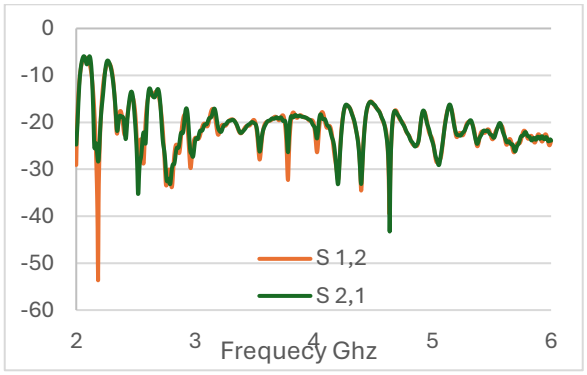


Зураг.5 Хосолсон зурвасын Helix антены загвар

Дээрх загвар нь 2 тусдаа антеныг нэг нэгэн дээр нь давхарлах байдлаар хосолсон зурвасын антеныг гаргаж авах туршилтыг хийсэн бөгөөд дараах үр дүнд хүрсэн Зураг.6.



6-р зураг.. Хосолсон зурвасын helix антены ойлтын коэффициент



7-р зураг. Хосолсон зурвасын helix антены дамжууллын коэффициент

Энэ симуляцийн үр дүнд хоёр антены хоорондын нөлөөллийг Зураг.6.б-д $S_{2,1}$ болон $S_{1,2}$ буюу дамжууллын коэффициентоор харуулав.

Дамжууллын коэффициентоос харахад хоорондоо 2.4ГГц, 5.8ГГц давтамжийн зурваст нөлөөлөл үүсгээгүй буюу дамжууллын коэффициент -15-аас бага байна.

Үр дүнгээс харахад хосолсон зурвасын антеныг гаргаж авч болох бөгөөд параметр тооцоолол дахин хийх шаардлагатай бөгөөд одоогийн загварчилсан антены өсгөлт 10.7 dBi цацрагийн өргөн нь 31.1º байна.

ДҮГНЭЛТ

Энэхүү өгүүлэлд өсгөлт сайжруулсан, нарийн чиглэлийн диаграммтай helix антеныг загварчилсан. Ихэнх дрон эсэргүүцэх төхөөрөмжид Yagi-Uda антен ашигладаг бол энэ судалгаагаар үүний оронд helix төрлийн антеныг ашиглан хосолсон зурваст ажиллуулах боломжтой гэдгийг Зураг.6-д харуулж байна.

Хосолсон зурвасын антены чиглэлийн диаграмм дээр ажиллах, хэмжээг бага байлгах нь дараагийн судалгаагаар хийгдэх болно.

НОМ ЗҮЙ

[1] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, “Survey on anti-Drone systems: Components, designs, and challenges,” *IEEE Access*, vol. 9, pp. 42635–42659, 2021, doi: 10.1109/ACCESS.2021.3065926.

[2] E. Horton and P. Ranganathan, “Development of a GPS spoofing apparatus to attack a DJI matrice 100 quadcopter,” J. Glob. Position. Syst., vol. 16, no. 9, Jul. 2018, doi: 10.1186/s41445-018-0018-3.

[3] A. D. B. A. Rahman, K. A. Ghani, N. H. H. Khamis, and A. R. M. Sidek, “Unmanned aerial vehicle (UAV) GPS jamming test by using software defined radio (SDR) platform,” J. Phys.: Conf. Ser., vol. 1793, no. 1, pp. 12–60, 2021, doi: 10.1088/1742-6596/1793/1/012060.

[4] Z. Cui, C. Briso-Rodríguez, K. Guan, Z. Zhong, and F. Quitin, “Multi frequency air-to-ground channel measurements and analysis for UAV communication systems,” IEEE Access, vol. 8, pp. 110565–110574, 2020, doi: 10.1109/ACCESS.2020.2999659. [5] M. Ghamari, P. Rangel, M. Mehrubeoglu, G. S. Tewolde, and R. S. Sherratt, Access, “Unmanned aerial vehicle communications for civil applications: A review,” IEEE vol. 10, 10.1109/ACCESS.2022.3208571.

ГҮН СУРГАЛТЫН АРГААР КОНТЭЙНЕРИЙН ДУГААРЫГ ТАНИХ НЬ

Г. ЭНХБАЯР[1], Э.ЖАВХЛАН[1], С.ӨЛЗИЙБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: ganboldenkhbayar0823@gmail.com[1], enhpurevjawhlan@gmail.com[1], ulziibayar@must.edu.mn[2]

Хураангуй: **Өнөөгийн дэлхийд улс орнуудын хооронд худалдаа, арилжаа хурдацтай хөгжиж, барааг хадгалж нэг цэгээс нөгөө цэг рүү зөөвөрлөх шаардлагаас үүдэн агуулахын хэрэгцээ нэмэгдсэн. Энэ нь логистик болон олон улсын худалдааны салбарт контейнерыг ачааг тээвэрлэх гол хэрэгсэл болгох нөхцөлийг бүрдүүлсэн. Ачаа тээвэрлэлтийн ихэнх хэсэг нь далайн болон төмөр замын тээвэр ашиглан хийгдэж, энэ нь дэлхийн тээврийн 80-90% болон 5-10%-ийг эзэлж байна. Контейнерын хэрэглээ нэмэгдэхийн хэрээр эдгээр контейнеруудыг бүртгэх шаардлага ч мөн өсөн нэмэгдэж, дугаар таних аргачлалууд хөгжсөөр ирсэн нь тухайлбал, гараар бүртгэх, RFID төхөөрөмж ашиглан таних болон OCR ашиглан таних аргачлалууд юм. Гэвч, өртөг багатай, өндөр нарийвчлалтай дугаар таних арга барилын хэрэгцээ байсаар байгаа юм. Контейнерын дугаар таних асуудлыг шийдвэрлэх нь улс орнуудын эдийн засагт чухал нөлөөтэй бөгөөд жил тутам Монгол улсын болон дэлхийн импорт, экспорт жил бүр өссөөр байна. Орчин үеийн компьютерын хараа болон гүн сургалтын алгоритмууд хурдацтай хөгжиж байгаа энэ үед бид гүн сургалтын сегментчлэлийн аргыг OCR (Оптик Тэмдэгт Таних) аргачлалтай хослуулан ашиглах шинэ аргачлалыг танилцуулах зорилго тавин энэхүү судалгаа хийсэн. Бид өөрсдийн судалгааны хүрээнд уг асуудлыг шийдэх гэж оролдсон нь контейнерын дугаарын сегментчлэлийн хувьд 99.5%, тэмдэгтийн түвшний танилтын хувьд 72.63%-ын үр дүнг үзүүлсэн. Энэхүү судалгаа нь контейнерын дугаар танилтыг бага өртөгтэй боловч илүү нарийвчлал өндөртэй шийдэл гаргахад суурь болж болох юм.**

Түлхүүр үг: ***Text Mining, Word Extracting, OCR, YOLO, Tesseract, Контейнер***

I. УДИРТГАЛ

Орчин үеийн логистик болон олон улсын худалдааны салбарт контейнерууд бараа тээвэрлэх үндсэн хэрэгсэл болоод байна. Дэлхий дээрх тээврийн 80-90 хувийг далайн тээвэр 5-10 хувийг төмөр замын тээвэр эзэлдэг [1] бөгөөд эдгээр тээврүүдэд контейнер өргөн хэрэглэгддэг. Контейнерын дугаар нь тухайн контейнерыг ялган таних код бөгөөд логистикийн үйл явц, ачаа бараг оновчтой хянах чухал хэрэгсэл болдог. Монгол улсын болон дэлхийн импорт, экспортын хэмжээ жил ирэх тусам өсөн нэмэгдэж буйтай холбоотойгоор эдгээрийг бүртгэх нь чухал шаардлагатай болсон байна.

Одоогийн IoT шийдлүүд голчлон баркод уншигч болон RFID төхөөрөмжүүдийг контнейрийн дугаар танихдаа ашигладаг. Эдгээр аргачлалууд нь гүйцэтгэл өндөр байдаг ч тодорхой хязгаарлалтуудтай бөгөөд, үүнд нэмэлт тоног төхөөрөмж хэрэгтэй байдал, болон өндөр засвар үйлчилгээний зардал орно. Энэхүү судалгаанд бид орон нутгийн хяналтын камеруудаар өгөгдөл цуглуулах шийдлийг санал болгож байна. Энэ нь нэмэлт тоног төхөөрөмжийн хэрэгцээг арилгаж, өгөгдөл цуглуулах, таних явцыг илүү үр ашигтай болгох юм. Гар аргаар контейнерын дугаар таних болон бүртгэх нь удаан хугацаа, өндөр зардал шаарддаг тул Радио Давтамжаар таних арга(RFID)-д суурилсан ACCR системүүд өндөр нарийвчлалтай танилтуудыг олгодог ч суурилуулах болон засвар үйлчилгээний зардал өндөр байдаг

Сүүлийн жилүүдэд компьютерын хараа болон гүн сургалтын алгоритмууд эрчимтэй хөгжиж, олон салбарт амжилттай ашиглагдаж байгаа ба гүн сургалтын аргууд нь өгөгдлийн боловсруулалтыг автоматжуулах, бодит нөхцөл байдалд дасан зохицох өндөр чадвартай тул контейнерын дугаар таних асуудлыг шийдвэрлэхэд оновчтой арга болох боломжтой. Контейнерын дугаар таних явцад хэд хэдэн хүндрэлүүд тулгарсан нь контейнерын зургийн гэрэлтүүлэг, дүрсний бүдгэрэл, контейнерын гадаргуугийн элэгдэл нь танилтыг хүндрэлтэй болгодог. Түүнчлэн контейнерыг дугаарлах нь стандарттай байдаг боловч дугаарыг хөндлөн эсвэл босоогоор тэмдэглэдэг ба хэд хэдэн мөр дамнаж тэмдэглэсэн, мөн контейнер камерт хэрхэн бууснаас хамааран төгс хэвтээ эсвэл босоо байрлалтай байдаггүй нь дугаар танилтыг хүндрэлтэй болгосон.

II. СУДАЛГАА

1. Контейнерын дугаар таних системүүдийн хөгжлийн тойм

Далайн болон газрын тээврийн салбарт контейнерын дугаар нь тухайн контейнерыг таних, түүний байршил болон тээвэрлэлтийн явцыг хянахад ашиглагддаг. Анх гараар тэмдэглэх арга хэрэглэгдэж байсан бол RFID болон OCR (Оптик тэмдэгт таних) системүүд түгээмэл хэрэглэгддэг болсон. Гэсэн хэдий ч эдгээр аргууд нь үр ашиг болон нарийвчлалын хувьд хязгаарлагдмал хэвээр байна. RFID нь өндөр гүйцэтгэлтэй бүртгэл хийх боловч тоног төхөөрөмжийн зардал ихтэй, харин OCR нь бага зардлаар ажиллах боловч нарийвчлалын асуудалтай тулгардаг.

2. Одоогийн контейнерын дугаар таних аргачлалууд

Контейнерын дугаарыг таних одоогийн системүүдийг дараах байдлаар ангилж болно:

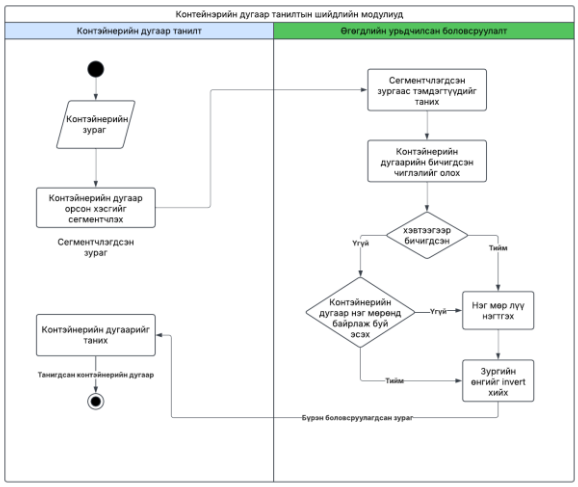
Гар аргаар бүртгэх арга нь контейнерын дугаарыг хүн гараар бичиж тэмдэглэх үйл явц юм. Энэ нь бага хэмжээний ачаа тээвэрлэлтийн үед боломжтой ч томоохон боомтуудад хүндрэлтэй байдаг. Гар аргаар бүртгэх арга нь алдаа гарах эрсдэл өндөр бөгөөд цаг хугацаа их шаарддаг тул боомтын үйл ажиллагааны хурдыг удаашруулж, үр ашиггүй байдал үүсгэдэг. Энэ аргыг ашиглахад ажиллах хүчний өндөр зардал шаарддаг учир энэ арга нь орчин үеийн тээврийн салбарт тогтвортой шийдэл болж чадахгүй.

RFID суурьтай танилтын систем нь контейнер бүрд RFID шошго суурилуулж, үүнийг RFID уншигч төхөөрөмж ашиглан бүртгэдэг автоматжуулсан технологи юм. Энэ систем нь өндөр нарийвчлалтай ажиллаж, контейнерын хөдөлгөөнийг бодит цагийн горимоор хянах боломж олгодог. Гэвч RFID системийг хэрэгжүүлэхэд өндөр өртөгтэй тоног төхөөрөмж шаардлагатай бөгөөд суурилуулах, засвар үйлчилгээ хийх зардал ихтэй байдаг. Иймээс энэ арга нь зөвхөн санхүүгийн боломжтой томоохон логистикийн компаниудад илүү тохиромжтой байдаг.

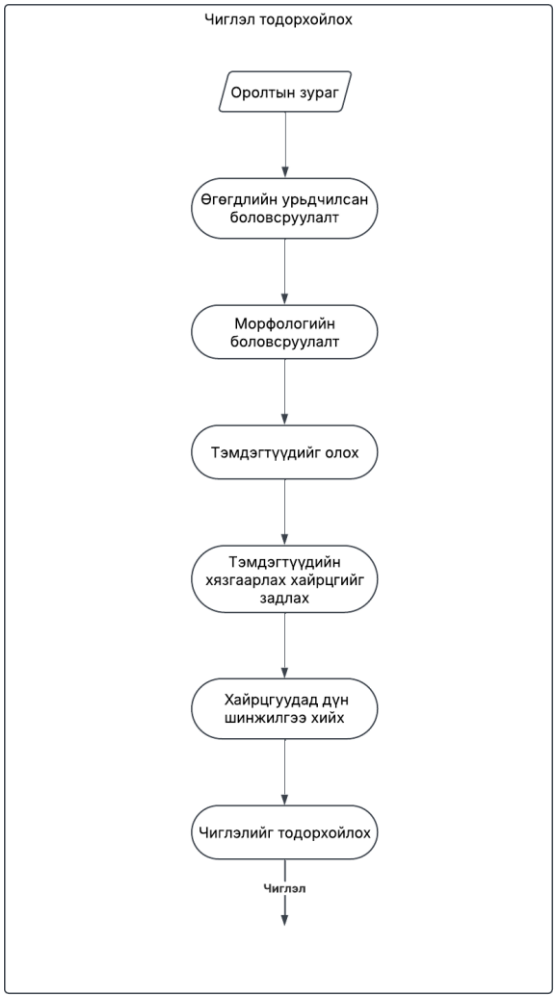
OCR (Оптик тэмдэгт таних) суурьтай систем нь контейнер дээрх тэмдэгтийг дүрс болгон уншиж, OCR алгоритмаар боловсруулан таних арга юм. Энэ нь RFID-ээс илүү бага өртөгтэй бөгөөд хэрэгжүүлэхэд харьцангуй хялбар боловч нарийвчлалын хувьд тодорхой асуудлуудтай тулгардаг. Гэрэлтүүлэг хангалтгүй, бүдэг зурагтай үед OCR системүүд алдаа гаргах магадлал өндөр байдаг. Мөн контейнерын дугаарын байрлал, хэмжээ нь өөр өөр байх тохиолдолд OCR нь зөв уншихгүй байх асуудал үүсдэг.

III. ТЕХНОЛОГИЙН ШИЙДЭЛ

Судалгааны эхний хэсэгт бид контейнерын зургийг OCR ашиглан унших гэж оролдоход 27.36%-ын нарийвчлалтай байсан нь контейнерын зургийн гэрэлтүүлэг, зургийн ямар өнцгөөс хэрхэн авсан, дүрсний бүдгэрэл, контейнерын гадаргуугийн элэгдэл зэрэг хүндрэлүүдээс шалтгаалсан. Мөн энэ төрлийн ижил төстэй IoT технологид суурилсан шийдлүүд нь нарийвчлал өндөртэй байдаг боловч суурилалт, засвар үйлчилгээ болон ажиллах хүчний зардал өндөртэй байдаг. Бид хямд өртгөөр контейнерын дугаарыг таньж сайжруулахын тулд доорх алхмуудыг гүйцэтгэв. Үйл ажиллагааны ерөнхий дарааллыг зураг 1, 2-д харуулсан.



1-р зураг. Контейнерын дугаар таних үйл ажиллагааны диаграмм

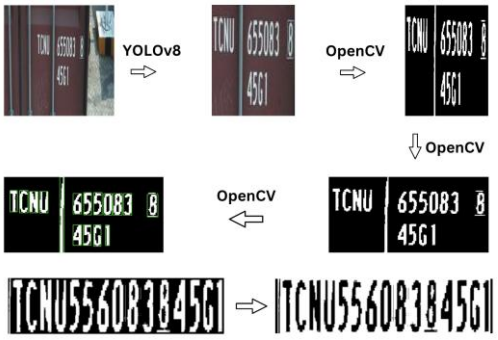


2-р зураг. Контейнерын дугаарын бичигдсэн чиглэлийг олох үйл ажиллагааны диаграмм

I. Контейнерын дугаарыг үр дүнтэй танихын тулд контейнерын зургаас тухайн контейнерын дугаарыг агуулсан хэсгийг сегментчлэл хийн ялган авсан.

II. Контейнерын зургийн гэрэлтүүлэг, дүрсний бүдгэрэл, контейнерын гадаргуугийн элэгдэл зэрэг хүндрэлүүдийг багасгахын тулд бид дүрс боловсруулалтын хэд хэдэн арга хэрэглэсэн. OpenCV-г ашиглан дүрсийг өнгөтөөс саарал болгож, өгөгдлийг цэвэрлэж, otsu's thresholding ашиглан зургийг хар-цагаан болгон хөрвүүлж, текстийн ялгаралтыг сайжруулж, морфологийн боловсруулалт (Morphological Processing) хийн бичигдсэн дугааруудыг тодруулсан.

III. Урьдчилан боловсруулагдсан зургууд дээр тооцоолол хийн тухайн контейнерын дугаар нь хөндлөн эсвэл босоогоор бичигдсэн эсэхийг хамгийн их болон хамгийн бага х,у тэнхлэгүүдийг тооцоолон(зураг 2) хөндлөн тохиолдолд уншилтыг шууд хийж хөндлөн боловч 2 буюу түүнээс дээш мөр дамнаж бичигдсэн бол тухайн мөрүүдийг хооронд нь нэгтгэж нэг мөр болгон нэгтгэсэн. Хэрэв контейнер нь босоогоор бичигдсэн бол үсэг бүрийг хооронд нь нэгтгэн нэг мөр болгон нэгтгэсэн. OCR-ийн танилтыг сайжруулахын тулд нэгтгэсэн зургийг хөрвүүлэн цагаан гадаргуу дээр хар текст агуулсан болгож хувиргасан. Танилтыг хийхдээ хэд хэдэн OCR сангуудыг туршин үзсэний үндсэн дээр tesseract санг ашиглан уншилтыг гүйцэтгэсэн.



3-р зураг. Контейнерын дугаар таних үйл явцын жишээ

IV. ТУРШИЛТ

Энэхүү туршилтын зорилго нь контейнерын дугаарыг автоматаар таних болон түүний гүйцэтгэлийг үнэлэхэд оршино. Туршилтын орчин нь Google Colab дээр суурилсан бөгөөд энэ нь машин сургалт болон компьютерын харааны чиглэлээр ажиллахад тохиромжтой орчин юм. Туршилтын явцад бид NVIDIA Tesla T4 GPU-г ашигласан бөгөөд энэ нь гүн сургалт болон дүрс боловсруулалтын ажлыг хурдан, үр ашигтай хийх боломжийг олгодог. Мөн Intel Xeon CPU ашигласан ба энэ нь өндөр гүйцэтгэлтэй тооцооллын хүчин чадалтай.

I. Өгөгдлийн багц

Туршилтад ашиглагдсан өгөгдлийн багцыг kaggle-ын нээлттэй өгөгдлийн багцаас авсан бөгөөд контейнерын зургаас контейнерын дугаарыг агуулсан хэсгийг сегментчлэл хийх сургалтад 4501, баталгаажуулалтын 1002 болон туршилтын 786 зургаас бүрдсэн өгөгдлийн багцыг ашигласан бол контейнерын дугаарын танилтыг хийхэд санамсаргүй сонгогдсон 100 зургийг ашигласан.

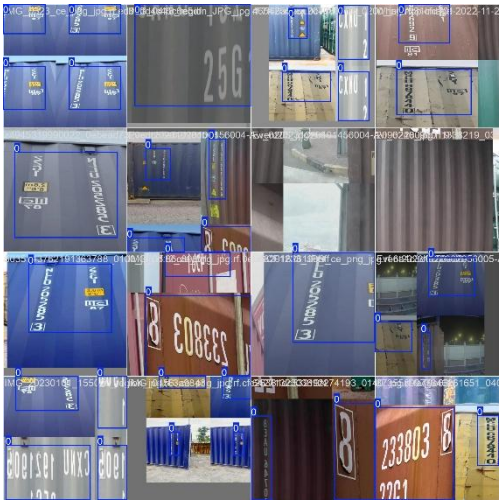
4-р зураг. Туршилтад хэрэглэгдсэн өгөгдлийн багцын жишээ

II. Контейнерын зургийг сегментчлэх

Контейнерын зургийг сегментчлэхэд YOLO төрлийн YOLOv5, YOLOv7, YOLOv8 загваруудыг туршсан(Хүснэгт 1) ба уг туршилтын үр дүнд YOLOv8 загварыг сегменчлэлд ашиглан 99.5%-ын accuracy, 99.85%-ын precision үр дүнд хүрсэн.

ХҮСНЭГТ 1. СЕГМЕНТЧЛЭЛИЙН ЗАГВАРУУДЫН ГҮЙЦЭТГЭЛИЙН ҮНЭЛГЭЭ

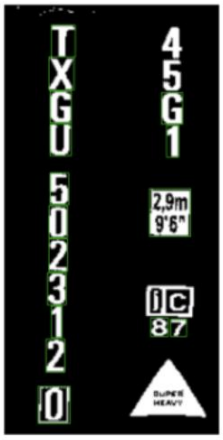
Загвар	Accuracy	Precision
YOLOv5	98.74%	99.01%
YOLOv7	98.57%	98.89%
YOLOv8	99.50%	99.85%



5-р зураг. Сегментчлэлийн үр дүнгийн жишээ

III. Контейнерын дугаарыг таних

Туршилтын үр дүнд контейнерын дугаар танилтын үр дүн нь 72.63% гарсан. Энэ нь ихэвчлэн контейнерын гэмтэл, контейнерын дугаарын тэмдэгт нь байхгүй болсон эсвэл ойролцоо текст дээр ихэвчлэн алдаа гарч буйг илэрхийлж байна.




```
Characters saved in: /content/characters/vertical/test_15_cropped_0
/content/characters/vertical/test_15_cropped_0
```


```
TXGU5023120
extracted_text :  TXGU5023120
```

ДҮГНЭЛТ

Энэхүү судалгааны зорилго нь контейнерын дугаарыг таних системийг хөгжүүлэхэд оршиж байсан бөгөөд бид гүн сургалтын YOLOv8 загвар болон OCR-д суурилсан аргуудыг ашиглан танилтуудын нарийвчлал болон тогтвортой байдлыг сайжруулахыг зорьсон. Судалгааны явцад гарсан гол хүндрэлүүдийг өгөгдлийн урьдчилсан боловсруулалт, сегментчлэл, болон OCR аргуудыг ашиглан шийдвэрлэхээр оролдсон бөгөөд эдгээр аргачлалууд нь тэмдэгтийн түвшинд 72.63%-ийн нарийвчлалтай танилт хийх боломжийг олгосон.

Гэвч, үгийн түвшний нарийвчлал нь буурч байгааг бид ажигласан бөгөөд энэ нь контейнерын дугаарыг бичих үед илрэх алдаа, контейнерын гэмтэл, байршлын асуудлаас үүдэлтэй. Ирээдүйд бид компьютерын харааны техникүүдийг хөгжүүлснээр системийн нарийвчлалыг улам сайжруулах, мөн алдааны шалтгаануудыг илрүүлж, шийдэх боломжийг судлах зорилго тавин ажиллах болно. Тус судалгаа нь контейнерын дугаар таних системийг автоматжуулан сайжруулах, тээврийн салбарт үр ашигтай шийдлийг боловсруулах суурь болж байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] “Review of Maritime Transport 2021 | UN Trade and Development.” *UNCTAD*, United Nations Conference on Trade and Development, 2021, https://unctad.org/publication/review-maritime-transport-2021. Accessed 10 March 2025.

[2] Kumano, Shintaro, et al. *Development of container identification mark recognition system*. 2004.

[3] Shi, Xiaoning, and Stefan Voss. *RFID Technology and its Application to Port-Based Container Logistics*. 2011.

АЛБАН ЁСНЫ Э-МЭЙЛ ХАЯГИЙГ БАТАЛГААЖУУЛАХ АППЛИКЭЙШН ХӨГЖҮҮЛЭХ НЬ

Мандахбаярын МӨНХ-ЭРДЭНЭ[1], Лхагваагийн ОДОНЧИМЭГ[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Мэдээллийн сүлжээ, Аюулгүй Байдлын Салбар
Холбоо барих зохиогчийн и-мэйл хаяг: monkhm02@gmail.com[1], odno@must.edu.mn[2]

***Хураангуй*:Энэхүү судалгаа нь банк, санхүүгийн байгууллагуудын аюулгүй байдлыг сайжруулах зорилгоор цахим шуудангийн баталгаажуулалтын системийг хөгжүүлэхэд чиглэгддэг. Гол зорилго нь цахим шуудангийн хаягийг баталгаажуулах иж бүрэн техникээр баталгаажуулах замаар болзошгүй кибер халдлагыг илрүүлэх, урьдчилан сэргийлэх явдал юм. Систем нь цахим шуудангийн баталгаажуулалтын дэвшилтэт аргуудыг хэрэгжүүлэх замаар байгууллагын болон хэрэглэгчийн аюулгүй байдлыг хамгаалах зорилготой. Үүнд и-мэйлийн синтаксийг шалгах, домэйн үнэн эсэхийг шалгах, хуурамч эсвэл сэжигтэй и-мэйл хаягийг тодорхойлох зэрэг орно. Нэмэлт хамгаалалтын давхаргыг бий болгосноор судалгаа нь зөвшөөрөлгүй хандалт, фишинг хийх оролдлого, нийгмийн инженерийн халдлагатай холбоотой эрсдэлийг бууруулахыг зорьдог. Гол давуу талууд нь хэрэглэгчийн баталгаажуулалтыг сайжруулж, кибер аюулгүй байдлыг сайжруулж, санхүүгийн салбарын аюулгүй байдлын дүрэм журмыг илүү сайн дагаж мөрддөг. Баталгаажуулах систем нь олон платформ дээр цахим шуудангийн мэдээллийг хооронд нь холбож, баталгаажуулахын тулд дэвшилтэт алгоритмууд болон машин сургалтыг ашиглах болно. Боломжит программууд нь банк, зээлийн хоршоо, онлайн санхүүгийн платформ зэрэг санхүүгийн янз бүрийн үйлчилгээг хамардаг бөгөөд эцэст нь байгууллага болон хэрэглэгчдийн аль алинд нь илүү найдвартай дижитал орчныг бүрдүүлдэг.**

Түлхүүр үг: Халдлага, аюулгүй байдал, баталгаажуулах

I. УДИРТГАЛ

Сүүлийн жилүүдэд цахим орчны хэрэглээ нэмэгдсэнтэй зэрэгцэн кибер халдлага, ялангуяа фишинг болон сошиал инженеринг халдлага улам өргөн дэлгэрсэн. Фишинг нь хэрэглэгчийн хувийн болон санхүүгийн мэдээллийг хуурамч вэбсайт эсвэл и-мэйл ашиглан хуурч авах явдал юм. APWG-ийн тайлан (2022) мэдээлснээр фишинг халдлага жил бүр 42.8%-иар нэмэгдэж, банк, санхүүгийн салбарт ихээр чиглэсэн байна. COVID-19 цар тахлын үед цахим орчинд ажиллах, харилцах хэрэгцээ эрс нэмэгдсэн тул фишинг халдлага 521%-иар өссөн нь хэрэглэгчдийн и-мэйл хаягт чиглэсэн аюул заналыг улам ноцтой болгосон. Хуурамч и-мэйлүүдээс үүсэх эрсдэлүүд нь:

- Хувийн мэдээлэл алдагдах
- Санхүүгийн залилан гарах
- Байгууллагын нэр хүнд унах зэрэг үр дагаварт хүргэж байна.

II.СЭДЭВ СОНГОСОН ҮНДЭСЛЭЛ

СУДАЛГАА

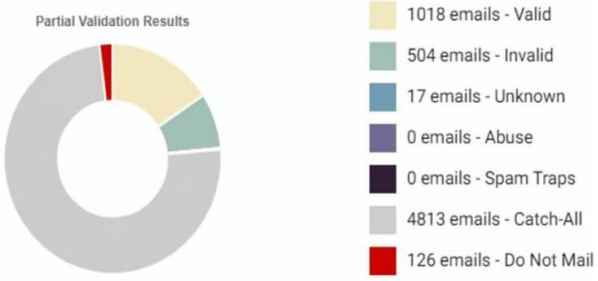
(A) Дэлхийн хэмжээнд

Statista судалгаа: 2023 оны судалгаагаар байгууллагуудын 60% нь цахим шуудангийн хаяг баталгаажуулах технологийг ашигладаг. Энэ нь и-мэйл маркетингийн кампанийн амжилтыг 25% хүртэл нэмэгдүүлэх боломжтой гэж үзэж байна.

Email Service Providers (ESP) судалгаа: Mailgun-ийн судалгаагаар и-мэйл хаяг баталгаажуулалттай хэрэглэгчдийн и-мэйл илгээгдэх амжилтын хувь 98% хүрдэг, харин баталгаажуулалтаас гадуур и-мэйл хаягтай хэрэглэгчдийн хувьд 60% хүрэхгүй байдаг.

Gartner судалгаа: Gartner-ийн судалгаагаар, и-мэйл хаяг баталгаажуулалтыг хэрэгжүүлсэн байгууллагуудын 50% нь хэрэглэгчдийн мэдээллийн чанар, аюулгүй байдалд 30% -иар нэмэгдсэн байна.

Zerobounce.net: дээр явуулсан судалгаагаар 6500 хүнээс цахим шуудан баталгаажуулалт явуулсны үр дүнг доор харуулав.



1-р зураг. 6500 ширхэг цахим шуудан баталгаажуулалтын үзүүлэлт

Үүнээс харахад 1500 цахим шуудан тутмын 500 нь баталгаажуулаагүй гэж гарсан байна.

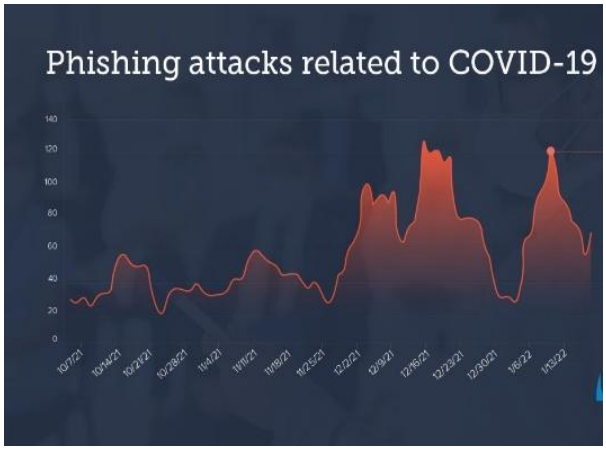
(B) ***Монголын хэмжээнд***

Монгол банк: Монгол банк 2023 онд банк, санхүүгийн байгууллагуудын мэдээллийн аюулгүй байдлын судалгаа явуулж, 70% орчим байгууллага цахим шуудангийн хаяг баталгаажуулах шийдлийг ашиглаж байгааг тодорхойлсон. Энэ нь хэрэглэгчдийн итгэлцлийг 20% нэмэгдүүлэхэд нөлөөлжээ.

Мэдээллийн технологийн стандарт: Монголын мэдээллийн технологийн стандартын байгууллагаас 2023 онд явуулсан судалгаагаар, цахим шуудангийн баталгаажуулалт нь хэрэглэгчийн мэдээллийн 15% -ийг бууруулахад тусалдаг гэж үзсэн.

Судалгааны байгууллага: Монголын судалгааны байгууллагуудын нэг нь 2024 оны 1-р улиралд явуулсан судалгаагаар, банк, санхүүгийн 100 байгууллагаас 75% нь цахим шуудангийн хаяг баталгаажуулах системийг нэвтрүүлсэн байна.

C. COVID-19 шинжилгээний эрэлт сүүлийн хэдэн долоо хоногт нэмэгдэж буйтай холбоотойгоор шинжилгээний хомсдолыг ашигласан залилангийн тоо мөн өссөн. Манай судлаачид сүүлийн хоёр сарын хугацаанд COVID-19 шинжилгээтэй холбоотой фишингийн халдлагуудын өсөлтийг ажигласан. Октябрээс январь хүртэл COVID-19 шинжилгээтэй холбоотой залилангийн тоо 521%-иар нэмэгдсэн. Өдөр тутмын дундаж тоо 1-р сарын эхээр хамгийн ихэд хүрч, сүүлийн үед буурч байсан боловч дахин өсөлттэй болж байна.



2-р зураг. COVID-19 шинжилгээтэй холбоотой фишингийн халдлагууд.

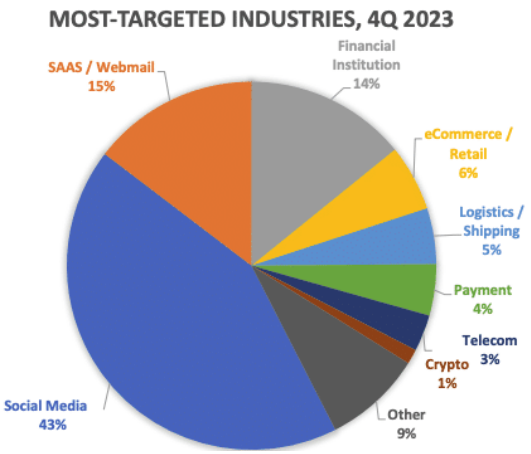
D. Фишинг халдлагын чиг хандлага

1-Р ХҮСНЭГТ

Industry	Percentage of phishing attacks
Financial Institutions	27.70%
Software-as-a-Service Providers	17.70%
Other	18.20%
Social Media Providers	10.40%
Logistics / Shipping	9.00%
Payment Services	6.00%
eCommerce / Retail	5.60%
Telecom	3.10%
Cryptocurrency	2.30%

E. **Хамгийн их онилогдсон салбарууд 2023 оны 4-р улирал**

Банк санхүүгийн байгууллага руу олон нийтийн мэдээллийн хэрэгсэл ашиглан social engineering халдлага хийж хэрэглэгчийн мэдээллийг залилж авах нь дэлхий дахинд томоохон хөнөөл учруулж буй томоохон шалтгаан болж байгаа билээ. 2023 оны 4-р улиралд хамгийн их зорилтот салбар бол сошиал медиа байсан бөгөөд энэ нь нийт фишинг халдлагын 42.8%-ийг эзэлж байна. Энэ нь 3-р улиралд бүртгэгдсэн нийт халдлагын 18.9%-ийн маш харьцангуй тэсрэлт юм. [3]



3-р зураг. Хамгийн их халдсан чиг хандлага

III. СУДАЛГААНЫ АЧ ХОЛБОГДОЛ

1. **Мэдээллийн аюулгүй байдлын тулгамдсан асуудал:** Сүүлийн жилүүдэд мэдээллийн аюулгүй байдал дэлхий дахинд ноцтой асуудал болоод байна. Тухайлбал, фишинг, спам, сошиал инженеринг гэх мэт халдлагууд нь санхүүгийн байгууллагууд болон хэрэглэгчдэд ихээхэн хохирол учруулж байна. Barracuda-ийн судалгаагаар 2022 онд фишинг халдлагын тоо 521%-иар өссөн нь COVID-19-ийн цар тахалтай холбоотой онлайн харилцааны эрс нэмэгдлээс үүдэлтэй.

2. Банк, санхүүгийн байгууллагуудад тулгарч буй эрсдэл: Банк, санхүүгийн байгууллагууд цахим орчинд хэрэглэгчдийн мэдээллийг хамгаалах, найдвартай байдлыг хангах нь үйл ажиллагааны гол зорилт болсон. Хуурамч и-мэйл хаяг ашиглан залилан хийх нь хэрэглэгчийн хувийн мэдээлэл болон санхүүгийн өгөгдлийг алдагдуулах эрсдэлийг бий болгож байна. Тиймээс:

Нишинг халдлагаас сэргийлэх: Хэрэглэгчийн мэдээллийг хуурамч и-мэйлээр дамжуулан хулгайлахыг бууруулах.

Санхүүгийн хохирол багасгах: Хуурамч и-мэйлээс үүсэх залилангийн гэмт хэргээс урьдчилан сэргийлэх.

3. Үйл ажиллагааны үр ашгийг нэмэгдүүлэх шаардлага: И-мэйл баталгаажуулалтын систем ашигласнаар:

- Гар ажиллагааг багасгах: И-мэйл хаягийг гараар шалгах цаг, зардлыг хэмнэх.
- Бодит цагийн хяналт: И-мэйл бүртгэлийн явцад шууд шалгаж, хэрэглэгчийн найдвартай байдлыг баталгаажуулах.
- Өгөгдлийн чанарыг сайжруулах: Зөвхөн баталгаатай и-мэйл хаягтай хэрэглэгчтэй харилцах нь банкны үйл ажиллагааны үр дүнг сайжруулна.

4. Хууль, дүрмийн шаардлага

Цахим мэдээллийн аюулгүй байдлын олон улсын болон орон нутгийн хууль тогтоомжуудыг дагаж мөрдөх нь банкны салбарт зайлшгүй шаардлагатай. GDPR (Европын мэдээлэл хамгаалах журам) болон Монгол Улсын Мэдээллийн аюулгүй байдлын хууль зэрэг хууль тогтоомжууд нь хувийн мэдээллийг зөв зохистой хамгаалахыг шаардаж байна.

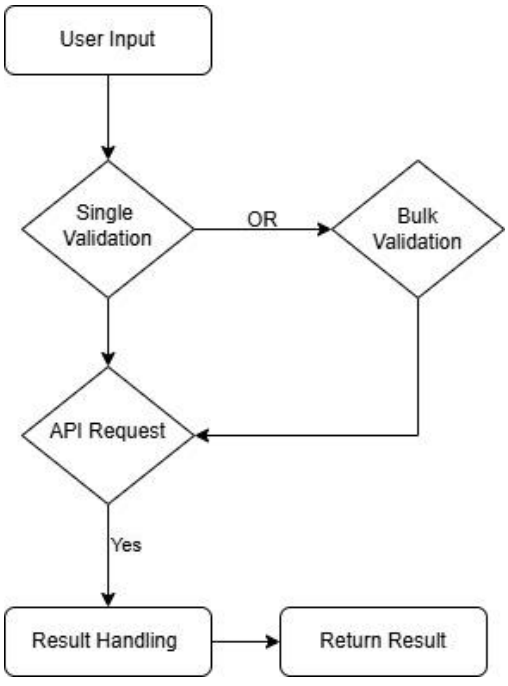
5. Технологийн дэвшил

И-мэйл баталгаажуулалт нь орчин үеийн технологийн дэвшил болох API, машин сургалт, мэдээлэл боловсруулах алгоритм зэрэгтэй хослуулан ашиглах боломжтой. Энэ нь зөвхөн банк, санхүүгийн салбар гэлтгүй бусад цахим үйлчилгээ үзүүлэгч байгууллагуудад ч ашигтай байж болно.

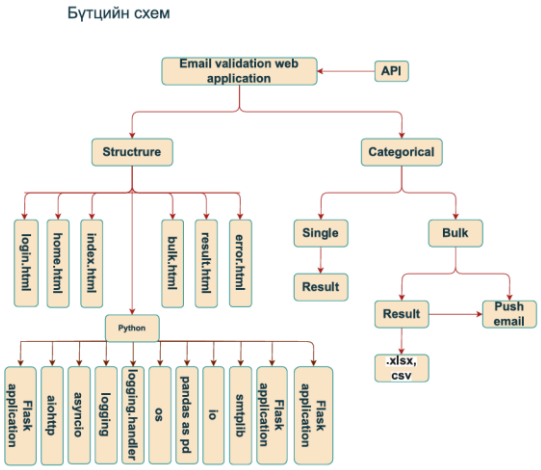
IV. ХЭРЭГЖҮҮЛЭЛТ

Хэрэглэгчийн цахим шууданг баталгаажуулснаар 2 талт аюулгүй байдал болон санхүүгийн үр ашигтай. Эхлээд application хийхийн тулд гол тулгуур болох шалгах процессыг үнэн зөв баталгаажуулдаг байх ёстой. Тийм учраас олон хүний итгэлийг ихээр хүлээн авсан IPqualityscore.com сайтын API -ыг сонгон авсан. Гол баталгаажуулах процесс API тусламжаар баталгаажна. Үүн дээр нэмэлтээр FRAUD SCORE болон RISK LEVEL тогтоох функц нэмсэн. Ингэснээр аюулын түвшин тодорхойлж аюултай цахим эсэхийг ялгаж ангилах боломжтой болно.

Схем зураг



4-р зураг. Бүтцийн схем



5-р зураг. Бүтцийн схем

Цахим шуудан баталгаажуулах веб аппликейшн хийгээд API code шаардлагатай. Ерөнхий 2 бүрэлдэхүүн хэсэгтэй. Бүтэц хэсэг нь python хөгжүүлэлт, login.html, home.html, index.html, bulk.html, result.html, error.html гэсэн долоон хэсгээс бүрдсэн. Python дотроо Flask web application, aiohttp, asyncio, logging, logging handler, os, pandas as pd, io, smtplib гэсэн 9н ширхэг сангийн тусламжтай хөгжүүлэлт явагдаж дууссан.

Single & Bulk гэсэн хоёр ангиллаар цахим шуудан баталгаажуулах сонголттой. Single баталгаажуулалт нь нэг ширхгээр баталгаажуулна, Харин Bulk процессын хувьд нэг дор олон ширхэг цахим шууданг баталгаажуулах боломжтой мөн PUSH EMAIL -ын хувьд Bulk-аас гарч ирсэн үр дүнг өөрийн цахим шуудангаар автоматаар хүлээн авах боломжтой.

V.ХӨГЖҮҮЛЭЛТ

Хөгжүүлэлтийн хэсэгт HTML, CSS, Python зэрэг программчлалын хэл ашигласан юм. Бид BULK-аар баталгаажуулахыг хүсвэл excel болон csv файл upload хийх хэрэгтэй

A. Бүтэц

1. Нэг И-мэйл Баталгаажуулалт:

Хэрэглэгчид гол хуудас (index.html) дээр текстийн талбарт и-мэйл хаягаа оруулдаг.

"Баталгаажуулах" товчийг дарснаар POST хүсэлт хийгдэнэ (/). index.py скрипт нь формын өгөгдлөөс и-мэйл хаягийг авдаг. Баталгаажуулалтын логикийг гүйцэтгэхийн тулд Validate ангийн экземпляры үүсгэдэг. Validate анги нь өгөгдсөн API түлхүүрийг ашиглан гадаад и-мэйл баталгаажуулах үйлчилгээ рүү асинхрон функц (email_validation_api) дуудагдаг. API-ийн хариуг шинжиж, fraud score, disposable байдал, spam trap статус, сүүлийн хугацааны хүчингүйчил, хүчинтэй байдал, хүргэх чадвар гэх мэт мэдээллийг гаргаж авдаг. risk level-ийг тодорхойлох функц (determine_risk_level) нь эдгээр мэдээллийг ашиглан и-мэйлийн эрсдэлийн түвшин (аюулгүй, сэжигтэй, аюултай, өндөр эрсдэл) ангилдаг. Хэрвээ эрсдэлийн түвшин сэжигтэй эсвэл түүнээс өндөр байвал, и-мэйл мэдэгдэл нь кодод заагдсан хүлээн авагч хаяг (SENDER_EMAIL болон RECEIVER_EMAIL) руу сэжигтэй и-мэйлийн талаарх мэдээлэлтэйгээр илгээгдэнэ. Мэдэгдэл нь бүлгийн бусад сэжигтэй и-мэйлүүдийн мэдээллийг агуулсан spreadsheet хавсралттай байж болно (дараа нь тайлбарлана). Баталгаажуулалтын үр дүнг separate page (result.html) дээр үзүүлж, анхны и-мэйл хаяг, API-аас авсан бүх мэдээлэл, болон тооцоолсон эрсдэлийн түвшин багтаасан.

2. Олон И-мэйл Баталгаажуулалт:

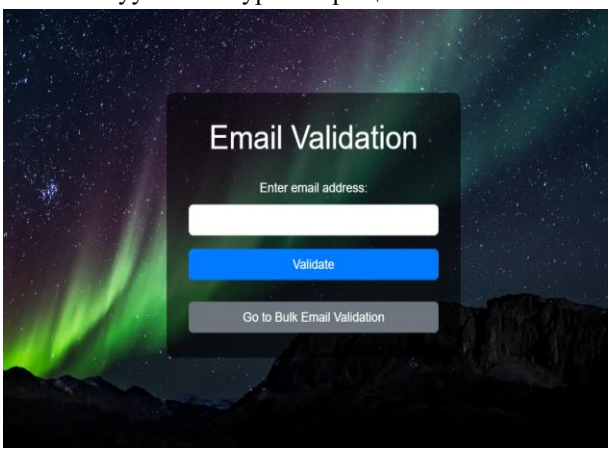
Хэрэглэгчид CSV эсвэл Excel файлыг и-мэйл хаягийн жагсаалт агуулсан хуудсан дээр (bulk.html) оруулж болно. Формыг илгээх үед POST хүсэлт /bulk URL рүү хийгдэнэ. bulk.py скрипт нь файлыг ачаалсан эсэхийг шалгаж, түүний форматыг (CSV, XLSX, XLS) баталгаажуулдаг. Хэрвээ файл зөвшөөрөгдсөн бол, скрипт нь pandas сангийн функцуудаар (pd.read_csv эсвэл pd.read_excel форматад хамаарч) и-мэйл хаягуудыг уншдаг. И-мэйл хаягуудыг параллель боловсруулалтын хувьд жижиг хэсгүүдэд хуваадаг (ProcessPoolExecutor анги). Бүх хэсгийг process_chunk туслах функц руу дамжуулж, validator.py-д байрлах асинхрон функц (process_batch) ашиглана. process_batch нь chunk-д байгаа и-мэйл бүрийн хувьд email_validation_api функцийг дуудаг бөгөөд үр дүнг цуглуулдаг. Сукрег нь бүх хэсгийн үр дүнг нэгтгэн, сэжигтэй бус эрсдэлийн түвшинтэй и-мэйлүүдийг шүүнэ. Хэрвээ сэжигтэй и-мэйлүүд олдсон бол Openpyxl сангаар шинэ workbook үүсгэж, эдгээр и-мэйлүүдийн мэдээллийг агуулсан spreadsheet-ийг үүсгэнэ. Сукрег нь spreadsheet-ийг толгой, өгөгдөл, илүү сайхан харагдах байдлын төлөө тохируулж форматчилна. И-мэйл мэдэгдэл нь сэжигтэй и-мэйл хаягууд болон тэдгээрийн мэдээллийг агуулсан биеийг агуулж, spreadsheet-ийг хавсаргана. Эцэст нь, скрипт нь үүсгэсэн spreadsheet-ийг хэрэглэгчид татаж авах боломжийг олгоно.

B. Нэмэлт функционалиуд:

Энэхүү программ нь веб рамкийн функцүүдийг гүйцэтгэхийн тулд Flask-ыг, шаблончлалын тулд Jinja2-г ашигладаг. Алдааны удирдлага нь алдааг тэмдэглэж, хэрэглэгчдэд ээлтэй алдааны мессежийг үзүүлэх зориулалттай custom error handler (handle_exception) ашиглаж байна. Чухал үйл явдлуудыг болон боломжит асуудлуудыг тэмдэглэж авахад логгингийг эргэлдэгч файлын хандлагаар тохируулах боломжтой.

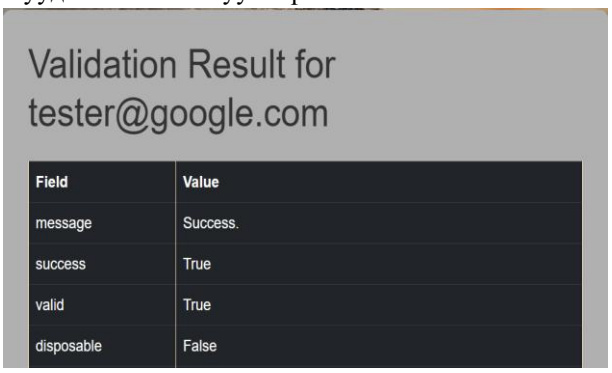
VI. ТУРШИЛТ БОЛОН ҮР ДҮН

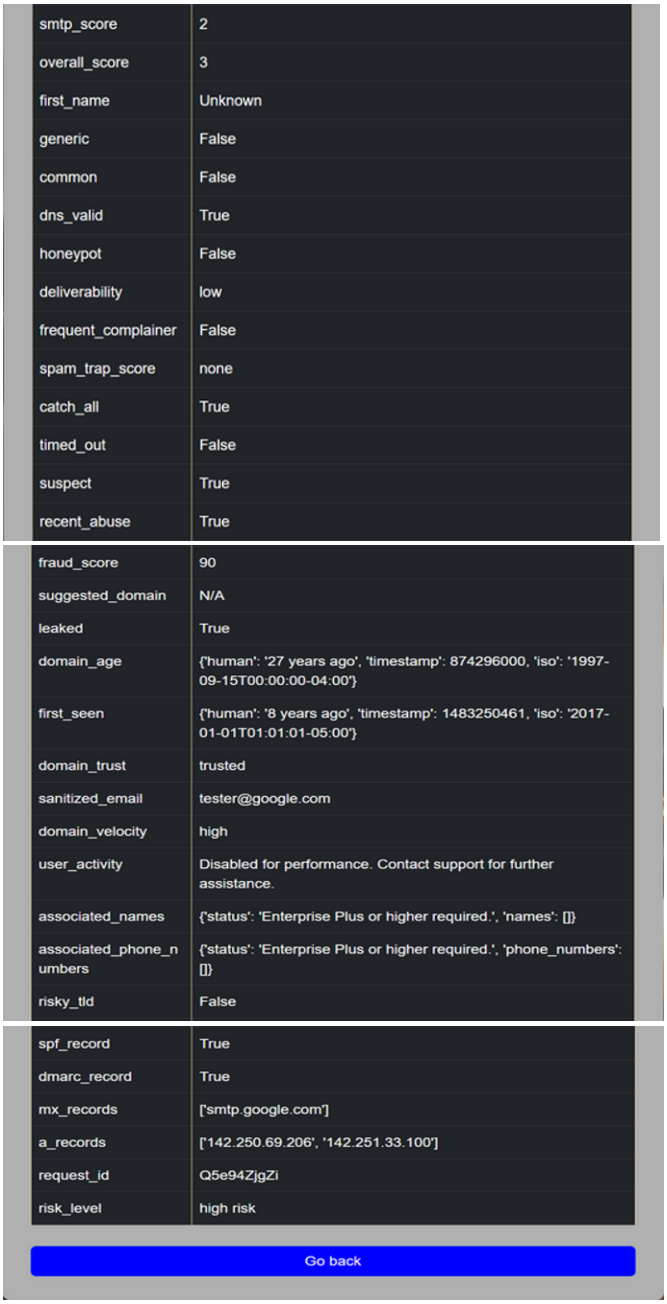
A. Single болон Bulk процессээр баталгаажуулах сонголтууд гарч ирж байна. Single баталгаажуулалтыг туршиж үзэцгээе.



6-р зураг. Э-мэйл баталгаажуулалтын ангилал

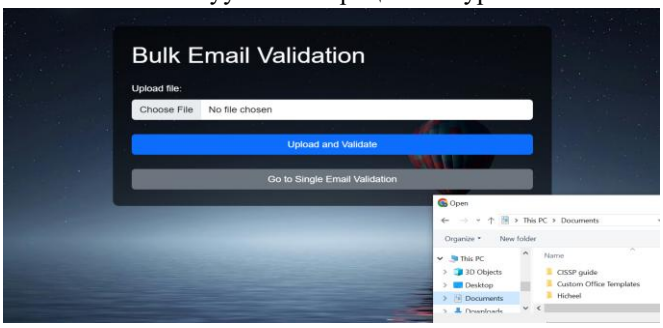
Жишээ болгож tester@google.com гэсэн цахим шууданг баталгаажуулж үзэв.





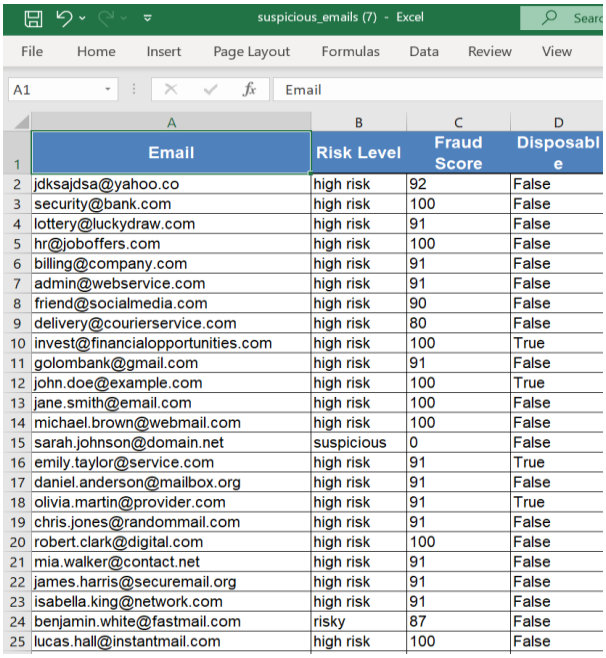
7-р зураг. Single email validation

1. Bulk баталгаажуулалтын процессыг туршсан.



8-р зураг. Bulk file uploading process

2. Random 25н ширхэг цахим шууданг баталгаажуулахад үр дүн ингэж харагдаж байна.



suspicious_emails (7) - Excel

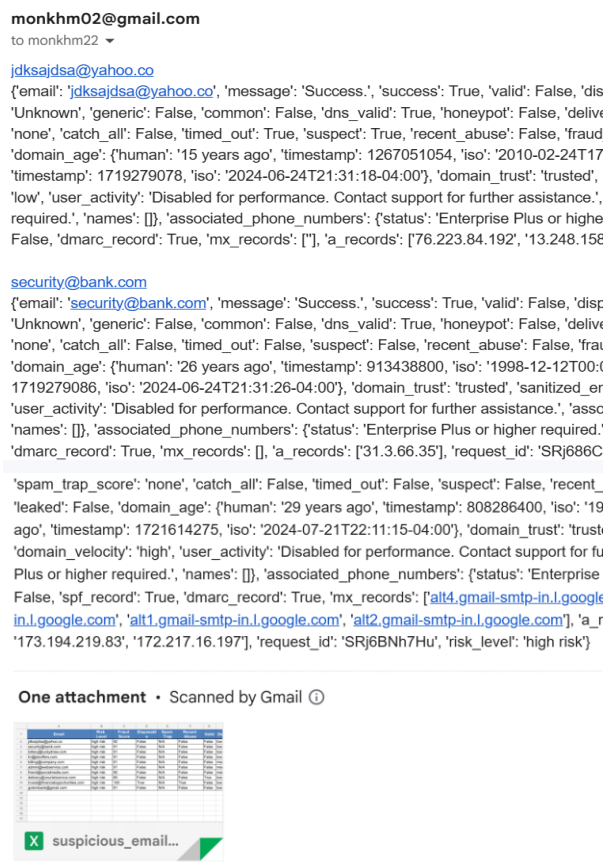
File Home Insert Page Layout Formulas Data Review View

A1 Email

	A	B	C	D
1	Email	Risk Level	Fraud Score	Disposable
2	jdksajdsa@yahoo.co	high risk	92	False
3	security@bank.com	high risk	100	False
4	lottery@luckydraw.com	high risk	91	False
5	hr@joboffers.com	high risk	100	False
6	billing@company.com	high risk	91	False
7	admin@webservice.com	high risk	91	False
8	friend@socialmedia.com	high risk	90	False
9	delivery@courierservice.com	high risk	80	False
10	invest@financialopportunities.com	high risk	100	True
11	golombank@gmail.com	high risk	91	False
12	john.doe@example.com	high risk	100	True
13	jane.smith@email.com	high risk	100	False
14	michael.brown@webmail.com	high risk	100	False
15	sarah.johnson@domain.net	suspicious	0	False
16	emily.taylor@service.com	high risk	91	True
17	daniel.anderson@mailbox.org	high risk	91	False
18	olivia.martin@provider.com	high risk	91	True
19	chris.jones@randommail.com	high risk	91	False
20	robert.clark@digital.com	high risk	100	False
21	mia.walker@contact.net	high risk	91	False
22	james.harris@securemail.org	high risk	91	False
23	isabella.king@network.com	high risk	91	False
24	benjamin.white@fastmail.com	risky	87	False
25	lucas.hall@instantmail.com	high risk	100	False

9-р зураг. Олноор баталгаажуулалтын үр дүн

3. Bulk процессоор баталгаажуулсан үр дүнг цахим хаягаар автоматаар файлаар илгээгдсэн байна.



monkhm02@gmail.com
to monkhm22

jdksajdsa@yahoo.co
{'email': 'jdksajdsa@yahoo.co', 'message': 'Success.', 'success': True, 'valid': False, 'dis
'Unknown', 'generic': False, 'common': False, 'dns_valid': True, 'honeypot': False, 'delive
'none', 'catch_all': False, 'timed_out': True, 'suspect': True, 'recent_abuse': False, 'fraud
'domain_age': {'human': '15 years ago', 'timestamp': 1267051054, 'iso': '2010-02-24T17
'timestamp': 1719279078, 'iso': '2024-06-24T21:31:18-04:00'}, 'domain_trust': 'trusted',
'low', 'user_activity': 'Disabled for performance. Contact support for further assistance.',
required.', 'names': []}, 'associated_phone_numbers': {'status': 'Enterprise Plus or highe
False, 'dmarc_record': True, 'mx_records': ['"], 'a_records': ['76.223.84.192', '13.248.158

security@bank.com
{'email': 'security@bank.com', 'message': 'Success.', 'success': True, 'valid': False, 'disp
'Unknown', 'generic': False, 'common': False, 'dns_valid': True, 'honeypot': False, 'delive
'none', 'catch_all': False, 'timed_out': False, 'suspect': False, 'recent_abuse': False, 'frau
'domain_age': {'human': '26 years ago', 'timestamp': 913438800, 'iso': '1998-12-12T00:(
1719279086, 'iso': '2024-06-24T21:31:26-04:00'}, 'domain_trust': 'trusted', 'sanitized_er
'user_activity': 'Disabled for performance. Contact support for further assistance.', 'assc
'names': []}, 'associated_phone_numbers': {'status': 'Enterprise Plus or higher required.'
'dmarc_record': True, 'mx_records': [], 'a_records': ['31.3.66.35'], 'request_id': 'SRj686C

'spam_trap_score': 'none', 'catch_all': False, 'timed_out': False, 'suspect': False, 'recent_
'leaked': False, 'domain_age': {'human': '29 years ago', 'timestamp': 808286400, 'iso': '19
ago', 'timestamp': 1721614275, 'iso': '2024-07-21T22:11:15-04:00'}, 'domain_trust': 'trust
'domain_velocity': 'high', 'user_activity': 'Disabled for performance. Contact support for fu
Plus or higher required.', 'names': []}, 'associated_phone_numbers': {'status': 'Enterprise
False, 'spf_record': True, 'dmarc_record': True, 'mx_records': ['alt4.gmail-smtp-in.l.google
in.l.google.com', 'alt1.gmail-smtp-in.l.google.com', 'alt2.gmail-smtp-in.l.google.com'], 'a_r
'173.194.219.83', '172.217.16.197'], 'request_id': 'SRj6BNh7Hu', 'risk_level': 'high risk'}

One attachment • Scanned by Gmail

suspicious_email...

10-р зураг. Push mail processing

C. Хэдэн хувийн нарийвчлалтай баталгаажуулалт хийгдэж байгааг дараах хүснэгт (10) дээр харуулж байна.

2-Р ХҮСНЭГТ

Process	Шалгасан э-мэйл	Зөв э-мэйл	Буруу э-мэйл	(%)
Single process	50	48	2	96%
Bulk process	200	188	12	94%

Single Process: 50 и-мэйл хаягийн 48 нь зөв баталгаажсан, 2 нь буруу баталгаажсан (96% нарийвчлалтай).

Bulk Process: 200 и-мэйл хаягийн 188 нь зөв баталгаажсан, 12 нь буруу баталгаажсан (94% нарийвчлалтай).

ДҮГНЭЛТ

Техник, технологийн орчны хөгжлөөс шалтгаалж үүнийгээ даган эрсдэл хэрэглэгч хүн бүрийн дээр ирж байна. Хувийн мэдээллээ ашиглан нэвтрэх, итгэл үнэмшилдээ тулгуурлан санхүү, цаг хугацаа, хувийн мэдээллээ алдах магадлал маш ихээр байна. Тиймээс энэхүү Detection-ийг ашиглаад халдлагаас хамгаалах, урьдчилан сэргийлэх харьцуулан хувьчлан гаргана.

НОМ ЗҮЙ

[1] Statista. (2023). Email Verification Market Growth Statistics. Statista

[2] Mailgun. (2022). Email Verification Best Practices.

[3] 2022 International Conference on Computing, Communication and Automation (ICCCA)

[4] (2023). Market Guide for Email Verification Solutions

[5] K. Elissa, “Title of paper if known,” unpublished.

[6] Browser Extension based Hybrid Anti-Phishing Framework using Feature Selection

[7] Security and Privacy in Social Networks and Solutions

[8] Монгол банк. (2023). Банкны системийн аюулгүй байдал.

[9] Мэдээллийн технологийн стандарт. (2023). Мэдээллийн аюулгүй байдал.

[10]Судалгааны байгууллага. (2024). Санхүүгийн байгууллагуудын дотоод аудит.