



**ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ**

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

**2025-2026 ОНЫ ХИЧЭЭЛИЙН ЖИЛИЙН НАМРЫН УЛИРЛЫН БАКАЛАВР
ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ХУРЛЫН ЭМХЭТГЭЛ**

**MUST
SICT**



**ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛИЙН
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ**

ДОКТОР, ПРОФЕССОР Г.ЦОГБАДРАХЫН НЭРЭМЖИТ “МЭДЭЭЛЭЛ,
ХОЛБООНЫ САЛБАРЫН ХӨГЖИЛД БИДНИЙ ГҮЙЦЭТГЭХ ҮҮРЭГ-2025”
БАКАЛАВР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ХУРАЛ

**ЭРДЭМ ШИНЖИЛГЭЭНИЙ
БҮТЭЭЛИЙН ЭМХЭТГЭЛ**

УЛААНБААТАР ХОТ
2025 ОН

Бүтээлийн эмхэтгэл хянан магадалсан:

Редакцын зөвлөлийн дарга:

МХТС-ийн ЭНБ дарга, доктор /Ph.D/, дэд профессор Х.Загарзүсэм

Редакцын зөвлөлийн гишүүд:

Мэдээллийн технологийн тэнхимийн профессор, доктор /Ph.D/, дэд профессор Ч.Мөнхнасан

Электроникийн тэнхимийн эрхлэгч, доктор /Ph.D/ Б.Дорж

Холбооны инженерчлэлийн тэнхимийн дэд профессор, доктор /Ph.D/, дэд профессор Ш.Ганболд

Компьютерын ухааны тэнхимийн профессор, доктор /Ph.D/, дэд профессор Д.Золзаяа

Компьютерын ухааны тэнхимийн дэд профессор, доктор /Ph.D/, дэд профессор Б.Туяацэцэг

Мэдээллийн технологийн тэнхимийн дэд профессор, доктор /Ph.D/, дэд профессор Д.Сарангэрэл

Кибер аюулгүй байдлын тэнхимийн ахлах багш, доктор /Ph.D/ Д.Бямбадорж

Кибер аюулгүй байдлын тэнхимийн багш Х.Уянгаа

Эмхэтгэсэн: Т.Заяа

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

ULAANBAATAR 2025

ГАРЧИГ

БАКАЛАВР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

1. Ухаалаг толины хөгжүүлэлт.....1-5
Бакалавр М.Билгүүнзаяа, доктор (Ph.D), профессор А.Одгэрэл,
2. Бага жинтэй ачаа тээвэрлэх автомат удирдлагатай хүргэлтийн дроны хөгжүүлэлт.....6-10
Бакалавр Н.Төрболд, доктор (Ph.D), профессор Б.Дорж
3. Адуу илрүүлэх ба зүсийг ангилах систем.....11-15
Бакалавр Э.Нандин-Эрдэнэ, багш Б.Ундрал
4. “SAFEKID AP”:Хиймэл оюун ухаанд суурилсан хүүхэд хяналтын систем.....16-25
Бакалавр О.Оюунжаргал, доктор (Ph.D), Б.Золзаяа
5. Хиймэл оюун ухаанд суурилсан жолоочийн аюулгүй байдлыг хянах системийн судалгаа ба хөгжүүлэлт.....26-37
Бакалавр Б.Амартүвшин, доктор (Ph.D), Б.Золзаяа
6. Тамирчдын биеийн бүтцийн үзүүлэлтүүдийг машин сургалтын арга ашиглан тооцоолох нь.....38-44
Бакалавр Г.Анужин, А.Номин-Эрдэнэ, О.Одбаясгалан, доктор (Ph.D), дэд профессор Б.Долгорсүрэн
7. Линукс үйлдлийн системийн эмзэг байдлыг илрүүлэх, хамгаалах боломжийн судалгаа.....45-55
Бакалавр Б.Батсуурь, доктор (Ph.D), дэд профессор Л.Одончимэг
8. Машин сургалт ашиглан дроны кибер халдлагыг илрүүлэх нь.....56-64
Бакалавр Б.Тэмүүлэн, М.Анар, доктор (Ph.D), дэд профессор Л.Одончимэг,
9. Утасгүй сүлжээний хурд, чанар, аюулгүй байдлыг судалгаа.....65-67
Бакалавр З.Мөнх-Эрдэнэ, Г.Ганбаяр, доктор (Ph.D), дэд профессор Я.Дашдорж
10. НРС Лабораторийн эрчим хүчний хэмнэлтийн судалгаа.....68-71
Бакалавр Ц.Сувд-Эрдэнэ, Т.Алтансүвд, доктор (Ph.D), профессор З.Буянхишиг
11. Био-анагахын радио долгион дээр элэгний хорт хавдрыг илрүүлэх мэдрүүр антены судалгаа.....72-76
Бакалавр Х.Есөн-Эрдэнэ, Б.Загарсүрэн, доктор (Ph.D), дэд профессор Б.Пүрэвцэрэн, доктор (Ph.D), П.Ууганбаяр
12. Гар удирдлагат дрон унагаар төхөөрөмж.....77-80
Бакалавр Т.Амартөр, Э.Батжаргал, доктор (Ph.D), дэд профессор Б.Пүрэвцэрэн

УХААЛАГ ТОЛИНЫ ХӨГЖҮҮЛЭЛТ

Мөнхзаяагийн БИЛГҮҮНЗАЯА¹, Аюурзанын ОДГЭРЭЛ²

^{1, 2}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Электроникийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: bilguunz045@gmail.com

Хураангуй: Судалгааны ажлаар Raspberry Pi 4 эмбэдэд төхөөрөмжинд суурилсан “Монгол ухаалаг толь (Magic Mirror Mongolia)” системийг хөгжүүлж туршсан. Хэрэглэгчийн царай таних, гэрэлтүүлгийг удирдах болон хиймэл оюунд суурилсан хүний нүүрний арьсыг шинжлэх зэрэг функцуудыг нэг системд нэгтгэн хөгжүүлсэн. Систем нь хэт авиан (ultra sonic) мэдрэгчээр хэрэглэгчийг толинд ойртсоныг мэдрч асна. Царай таних алгоритм ашиглан тухайн хүнийг тодорхойлно. Хэрэв бүртгэлтэй хэрэглэгч танигдвал хувийн горимд шилжин календарь, өдрийн ажлын хуваарь, даалгавар зэрэг тухайн хүний хувийн мэдээллийг харуулж, танигдаагүй тохиолдолд зочин горимд ажилладаг. Хэрэглэгч камераас холдоход хэт авиан мэдрэгч зайг нь хэмжиж системээс автоматаар гаргаж (logout) анхны төлөвт орно. 12В гэрэлтүүлэг болон камерын тэжээлийг Raspberry Pi-ийн GPIO гаралтад шууд холбогдсон 2 сувгийн релей ашиглан автоматаар удирдсан. Системийн хамгийн чухал онцлог нь OpenAI компанийн Vision API-г ашиглан царайг таниснаар хэрэглэгчийн нүүрний арьсны өнгө ба шинжид анализ хийж, арьсны төлөвийг тодорхойлон зөвлөгөө өгөх боломжийг бүрдүүлсэн явдал юм. Туршилтанд 4 хүн оролцсон бөгөөд царай танилт 90 орчим хувьтай байсан. Харин нүүрний арьсны шинжилгээг хийлгэхэд үр дүн нь мэргэжлийн хүний хэлсэн арьсны зөвлөгөөтэй дунджаар 92% таарсан. Энэхүү системийг гэр ахуйн ухаалаг төхөөрөмж, оффис, гоо сайхны салон, үсчин болон нийтийн талбайн интерактив толь хэлбэрээр хэрэглэх боломжтой. Уг систем нь царай танилт, мэдээллийн аюулгүй байдал, AI суурьт хэрэглэгчийн шинжилгээний технологийг нэгтгэсэн эмбэдэд системийн цогц шийдэл юм.

Түлхүүр үг: Raspberry Pi 4, царай таних, хэт авиан мэдрэгч, OpenAI, Vision API, арьсны шинжилгээ

I. УДИРТГАЛ

Орчин үеийн технологийн хөгжилд хиймэл оюун ухаан (AI), зүйлсийн Интернет (IoT) болон электроникийн инженерчлэл хурдацтай уялдан хөгжиж, хүний өдөр тутмын хэрэглээ, мэдээлэл хяналт, автомат удирдлагын салбарт гүнзгий нөлөө үзүүлж байна. Эдгээр технологийн нэгдэл нь хэрэглэгчийн зан төлөвийг тодорхойлох, хүрээлэн буй орчны мэдээлэлд хариу үйлдэл үзүүлэх, өгөгдөлд суурилсан шийдвэр гаргах ухаалаг системүүдийг бий болгож байгаа билээ. Түүний нэг тод жишээ бол ухаалаг толь юм.

“Magic Mirror Mongolia” судалгааны ажил нь AI, IoT, электроник гурвыг нэгдэл болгон ашиглаж, Raspberry Pi 4 [1] эмбэдэд төхөөрөмжид суурилсан ухаалаг толины системийг хөгжүүлэх зорилготой. Систем нь царай таних, хэт авиан (ultra sonic) мэдрэгчээр хэрэглэгчийн ойртолтыг илрүүлэх, OpenAI-н Vision API [2] ашиглан нүүрний арьсны төлөвийг шинжлэх, мөн “Custom Mirror Calendar” хэмээх бие даан боловсруулсан хувийн календарь ба цагийн хуваарийн менежментийн аппликейшнийг толины орчинд ажиллуулах чадвартай.

Системийн үндсэн ажиллагаа дараах байдлаар явагдана. Хэт авиан мэдрэгч (HC-SR04) хэрэглэгчийг тодорхой найд илрүүлэхэд Raspberry Pi Camera Module B Rev 2.0 идэвхжиж, царай таних алгоритм ажиллана. Хэрэв тухайн хэрэглэгч бүртгэлтэй бол систем хувийн горимд шилжин, хэрэглэгчийн нэр болон хамаарах мэдээллийг дэлгэцэнд харуулна. Харин танигдаагүй бол зочин горимд орж, цаг агаар, огноо, валютын ханш, ерөнхий мэндчилгээ зэрэг нийтийн мэдээлэл үзүүлнэ.

Хувийн горимын үндсэн интерфэйс нь судалгааны ажлын хүрээнд боловсруулсан “Custom Mirror Calendar” аппликейшн юм. Энэ програм нь толины систем дотор ажилладаг локал вэб аппликейшн бөгөөд Python backend API болон SQLite өгөгдлийн сан ашиглан ажилладаг. Хэрэглэгчийн өдөр тутмын ажлын хуваарь, уулзалт, төлөвлөгөө, хийх ажлын жагсаалтыг (To-Do List) REST API дуудлагаар татаж, толины дэлгэц дээр бодит хугацаанд харуулдаг. Ингэснээр систем нь зөвхөн таних төхөөрөмж биш, харин хувийн туслах (Personal Assistant) хэлбэрийн AI + IoT ухаалаг систем болон өргөжсөн.

Мөн систем нь OpenAI-н Vision API ашиглан царай танигдсаны дараа хэрэглэгчийн нүүрний арьсны өнгө, гэрэлтэлт, өө сэв, тослогжилт зэрэг шинж чанаруудыг гүн мэдрэлийн сүлжээний (Deep Neural Network) боловсруулалт ашиглан дүгнэж, арьсны төлөвийг текстэн хэлбэрээр гаргана. Энэ дүнг толины дэлгэц дээр “Skin Status” хэсэгт харуулж, хэрэглэгчид арьс арчилгааны зөвлөгөө өгдөг.

Хэрэглэгч камераас холдох үед хэт авиан мэдрэгч холдсон зайг тодорхойлж системээс автоматаар гарч (logout) үндсэн төлөв буюу зочин горимд шилждэг. Ингэснээр хэрэглэгчийн мэдээллийн аюулгүй байдал болон хувийн нууцлалыг хамгаалдаг.

Системийн тоног төхөөрөмжийн бүтэц нь Raspberry Pi 4, Pi Camera B Rev 2.0, Ultra Sonic мэдрэгч [3], болон 2 сувгийн 12 В релей модулаас [4] бүрдэнэ. Релей нь Raspberry Pi-ийн GPIO оролт/гаралтад холбогдож, гэрэл болон камерын тэжээлийг автоматаар удирдана. Энэхүү шийдэл нь нэмэлт микроконтроллер шаардахгүй, электроникийн түвшинд оновчтой, найдвартай автомат удирдлагын схем бүхий бүтэцтэй юм.

“Magic Mirror Mongolia” судалгааны ажил нь хиймэл оюун ухаан, зүйлсийн Интернет, болон электроникийн инженерчлэлийн нэгдэлд тулгуурласан ухаалаг систем бөгөөд гэр ахуй, оффис, гоо сайханы салон, боловсролын байгууллага, олон нийтийн орчинд нэвтрүүлэх боломжтой. Энэ судалгаа нь Монгол орчинд хиймэл оюун суурьтай автомат удирдлага, ухаалаг орчны дижитал экосистем, болон электроникийн шийдэлтэй IoT төхөөрөмж хөгжүүлэх чиглэлийн суурь судалгааны ажил юм.

II. СУДЛАГДСАН БАЙДАЛ

Marathon Consulting компани Android Studio орчинд ажилладаг ухаалаг толины интерфэйстэй холбогдсон мобайл програм хангамж хөгжүүлсэн судалгааны ажлыг [5]-д хийсэн. Уг систем нь Wi-Fi дамжуулагчаар Raspberry Pi-тай холбогдож, хэрэглэгчийн гар утсанд цаг агаар, мэдээ болон Google Calendar-ийн мэдээллийг харуулах боломжийг бүрдүүлсэн. Энэхүү судалгаанд IoT архитектур амжилттай нэвтрүүлсэн боловч камер болон хиймэл оюунд суурилсан царай таних функц дутмаг байсан нь системийн ухаалаг түвшинг хязгаарласан. Тус ажил нь толины интерфэйс болон гар утасны аппликейшний уялдаа холбоог туршиж, ухаалаг орчны дата солилцооны шийдлийг харуулсан давуу талтай.

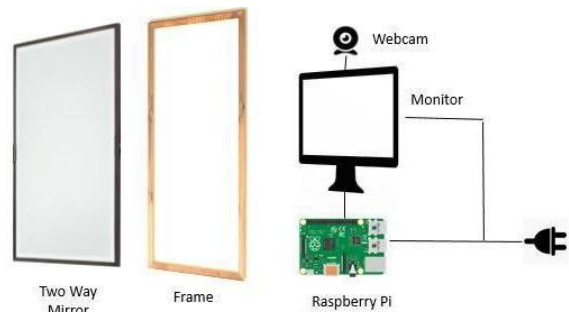


1-р зураг. Төсөөтэй ажил-1: Android Studio орчинд ухаалаг толины интерфэйстэй холбогдсон систем [5]

OpenCV номын сан болон Наар Cascade алгоритм ашиглан царай таних чадвартай ухаалаг толь бүтээсэн судалгааг [6]-д хийсэн. Систем нь Raspberry Pi камер ашиглан дүрс авч Python-д суурилсан OpenCV кодоор хэрэглэгчийн нүүрийг таних зарчмаар ажилладаг. Танигдсан хэрэглэгчийн мэдээлэлд тулгуурлан дэлгэцийн интерфэйс хувийн горимд шилжиж, хэрэглэгчийн нэр болон хамаарах мэдээллийг харуулдаг. Энэхүү судалгаа нь ухаалаг толины царай таних алгоритмыг практикт туршсан анхны ажлуудын нэг боловч Vision API зэрэг гүн сургалтын хиймэл оюуны технологи ашиглаагүй тул арьсны шинжилгээ болон хэрэглэгчийн ялгалт нарийвчлал байхгүй.

Бидний амьдралын өдөр тутмын мэдээллийг харуулдаг Raspberry Pi-д суурилсан ухаалаг толийг [7-8] судалгааны ажлуудад хөгжүүлсэн. Reflecta функцыг ашиглан гэрийн автоматжуулсан системд ашигласан судалгааны ажлыг [9]-д хийсэн. Хүний дуу хоолойнд боловсруулалт хийж эрүүл мэндийг нь

хянах судалгааны ажлыг [10]-д хийсэн. Мөн давхар толин дээр календарь, цаг агаарын мэдээ зэргийг үзүүлсэн.



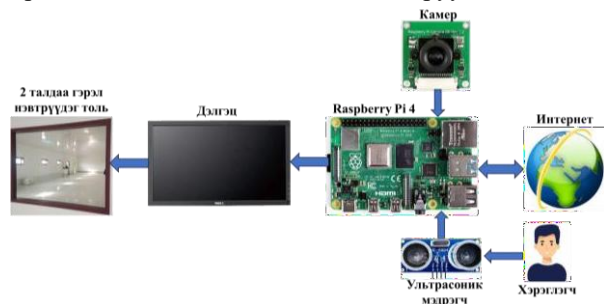
2-р зураг. Төсөөтэй ажил-2: OpenCV ашигласан царай таних ухаалаг толины системийн зарчмын схем [6]

Дээр дурдсан гурван судалгааны ажилд ухаалаг толь системийг Raspberry Pi суурьтайгаар хөгжүүлж, IoT орчинд холбох, интерфэйсийн уялдаа сайжруулах, царай таних алгоритм турших зэрэг чиглэлүүдийг судалсан байна. Гэвч эдгээр төслүүдэд OpenAI-н Vision API, хэт авиан мэдрэгч болон хувийн календарийн “Custom Mirror Calendar” аппликейшн зэрэг нарийвчилсан хиймэл оюун ба электроникийн шийдэл ашиглагдаагүй. Үүнтэй харьцуулахад “Magic Mirror Mongolia” ажил нь эдгээр технологиудыг нэг системд уялдуулж, AI + IoT + Электроник суурьт бүрэн ухаалаг толины системийг боловсруулсан нь өмнөх судалгаануудыг сайжруулсан шинэ шатны шийдэл болж байна.

III. СИСТЕМ ИЙН ДИЗАЙН БА ШИЙДЭЛ

A. Системийн бүтэц

Системийн ерөнхий бүтцийн схемийг дараах зурагт харуулав. Энэхүү ухаалаг толь нь Raspberry Pi 4 суурьтай бөгөөд түүнд Pi Camera B Rev 2.0, хэт авиан мэдрэгч, Интернет холболт, мөн 2 талдаа гэрэл нэвтрүүлдэг толь ба дэлгэцийн хослол холбогдсон байна. Систем нь хэрэглэгч толинд ойртохыг хэт авиан мэдрэгчээр илрүүлж, камерыг идэвхжүүлэн OpenAI-н Vision API-д илгээж боловсруулалт хийдэг.



3-р зураг. Системийн бүтцийн схем

Системийн үндсэн ажиллагаа дараах зарчмаар явагдана.

1. Хэрэглэгчийн илрүүлэлт: Хэт авиан мэдрэгч нь хэрэглэгч тодорхой зайд ойртоход дохио илгээж Raspberry Pi 4-т дамжуулна.

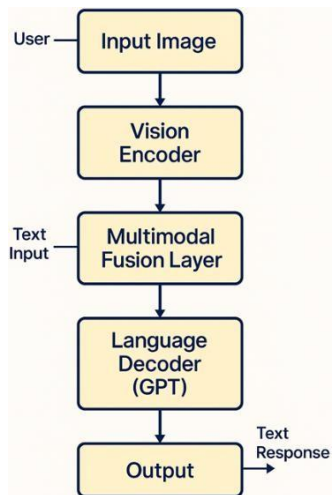
2. Царай таних ба шинжилгээ: Камер идэвхжиж дүрсийг аван Vision API-д илгээж, хиймэл оюун ухаанд суурилсан боловсруулалт хийнэ.
3. Хариу үйлдэл ба интерфейс: Хэрэв хэрэглэгч танигдсан бол систем “хувийн горим”-д шилжиж, “Custom Mirror Calendar” аппликейшний өгөгдөл (хуанли, хийх ажлын жагсаалт, арьсны төлөв)-ийг дэлгэц дээр харуулна. Танигдаагүй тохиолдолд зочин горимд ажиллана.
4. Системээс гарах механизм: Хэрэглэгч камераас холдсоноор мэдрэгч зайг тооцоолж системээс автоматаар хэрэглэгчийг гаргана.

Raspberry Pi 4 нь системийн төв удирдлага бөгөөд камер, хэт авиан мэдрэгч, релей, дэлгэц болон интернэт холболт зэрэг бүх модулиудыг нэг цэгээс хянаж ажиллуулдаг. Камер болон гэрлийн тэжээл нь GPIO гаралтаар холбогдсон 12В релейгээр автоматаар удирдагдана.

Төхөөрөмжийн архитектур нь AI + IoT + Электроник зарчмыг нэгтгэсэн онцлогтой. Vision API-аас ирэх хиймэл оюуны боловсруулалт нь AI хэсгийг, мэдрэгчүүд болон релей удирдлага нь электроникийн, интернетээр дамжсан өгөгдлийн дамжуулалт нь IoT орчныг бүрдүүлдэг.

В. OpenAI-н VisionAPI-н бүтэц, ажиллах зарчим

OpenAI-н Vision API нь дүрс болон хэлийг нэгтгэн ойлгох чадвартай “Multimodal” архитектур юм. Хэрэглэгчийн царайг таниж, арьсны шинж чанарыг тодорхойлоход ашигласан VisionAPI нь дараах бүтэцтэй байна.



4-р зураг. OpenAI-н VisionAPI-н бүтэц

Input Image: Хэрэглэгчээс зураг болон текстэн асуултыг хүлээн авна.

Vision Encoder: Зургийн пикселийн мэдээллийг “Feature Vector” буюу тоон код болгож хувиргана.

Multimodal Fusion Layer: Зураг болон текстийн утгыг “Cross-Attention” механизмаар нэгтгэн холбоно.

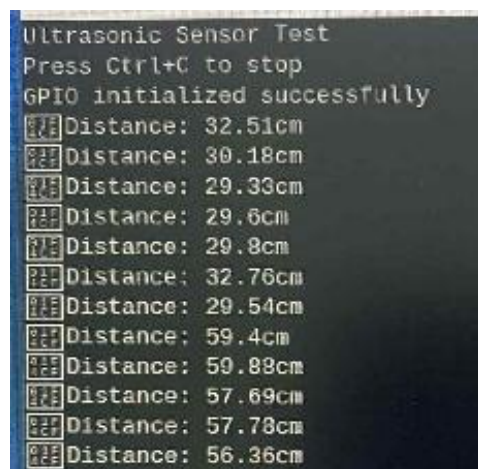
Language Decoder: Хэл танина.

Output: Хариуг JSON файл хэлбэрээ өгнө.

IV. ТУРШИЛТ, ҮР ДҮН

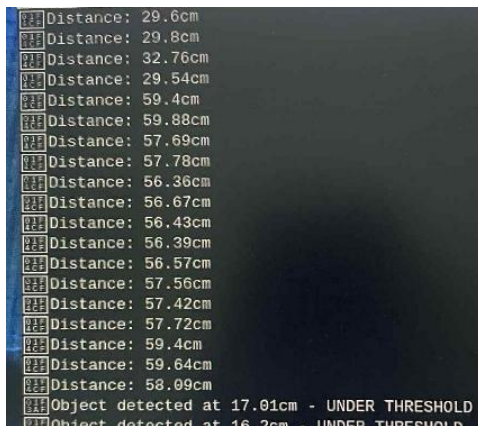
Сонгож авсан элемент, модулуудыг угсарч, системийг бүрэн ажиллагаанд оруулж туршилт хийсэн загварыг дараах зурагт харуулав. Энэхүү туршилтаар хэт авиан мэдрэгч, камер, релей удирдлагатай гэрэл, болон Vision API ашиглан ажиллаж буй ухаалаг толь системийн хариу үйлдэлийг шалгасан.

Эхний шатанд хэт авиан мэдрэгчийг Raspberry Pi 4-д холбон ажиллуулж, тухайн мэдрэгчийн хэмжилтийн тогтвортой байдлыг шалгасан. Туршилтын үр дүнгээс харахад 29–59 см-ийн хооронд өгөгдөл тасралтгүй ирж байсан бөгөөд дундаж алдаа ±0.3 см байв. Энэ нь мэдрэгч системд хангалттай нарийвчлалтай ажиллаж байгааг харуулж байна.



5-р зураг. Хэт авиан мэдрэгчийн туршилтын үр дүн

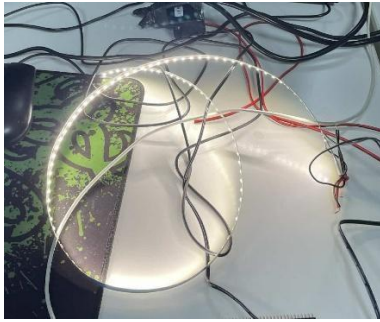
Хоёр дахь шатны туршилтаар тодорхой босго хэмжээнээс (20 см) доош объект илэрмэгц систем “UNDER THRESHOLD” гэж тэмдэглэж, Raspberry Pi-ийн камер болон гэрлийг автоматаар асааж байгааг шалгасан. Туршилтаар объект 16–17 см зайд илрэхэд систем бүрэн хариу өгч ажилласан нь програмын логик найдвартайг баталж байна.



6-р зураг. Объект илрэх үеийн мэдрэгчийн дохиолол

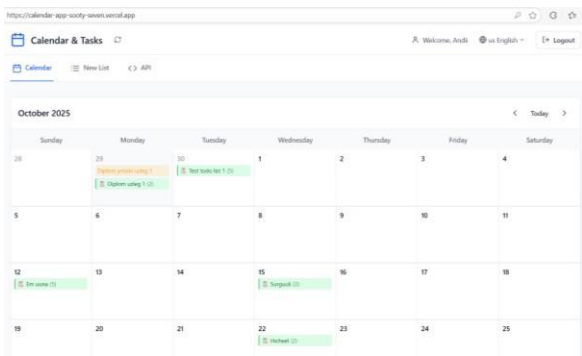
12В LED гэрэл болон релей модулийг Raspberry Pi 4-ийн GPIO гаралтаар удирдан туршсан. Объект илрэх үед гэрэл автоматаар асаж, хэрэглэгч

холдмогц унтарч байсан нь логик бүрэн ажиллаж буйг баталсан.



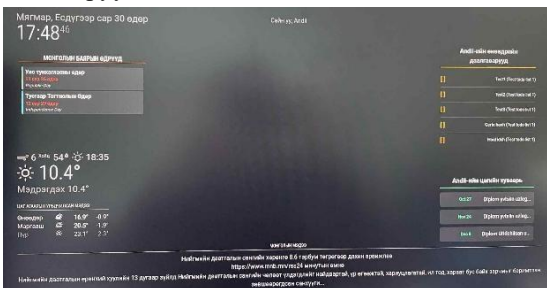
7-р зураг. Гэрэлтүүлгийн релей удирдлагын туршилт

Туршилтын явцад веб сайт болон API холболт хэвийн ажиллаж, календарийн өгөгдөл толины дэлгэц дээр бодит цагийн горимд амжилттай дамжсаныг дараах зургуудад харууллаа.



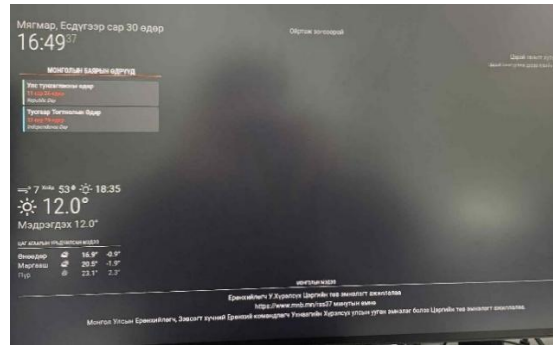
8-р зураг. Веб API туршилт

Камер идэвхжсэн үед хэрэглэгчийн дүрсийг авч OpenAI-н Vision API руу илгээж боловсруулсны дараа систем хэрэглэгчийг таньж, “Сайн уу, Andii” мэндчилгээ болон хувийн горимд зориулсан “Custom Mirror Calendar”-н мэдээллийг дэлгэцэнд гаргаж байна. Энэ үед хэрэглэгчийн хийх ажлын жагсаалт болон өдрийн төлөвлөгөөг автоматаар дэлгэцэнд ачаалж харуулна.



9-р зураг. Хэрэглэгч танигдсаны дараах дэлгэцийн интерфэйс

Хэрэв танигдаагүй хэрэглэгч илэрвэл систем “Царай танилт хүлээж байна” гэсэн төлөвт шилжиж, Vision API-ээс хариу иртэл зочин горим идэвхтэй байдалд ажиллана. Энэ горимд хэрэглэгчийн хувийн мэдээлэл, даалгавар, цагийн хуваарь харагдахгүй.



10-р зураг. Зочин горимд ажиллаж буй дэлгэцийн байдал

Face Recognition тестийн үеэр систем Vision API-тай хамтран ажиллах чадварыг туршсан. Туршилтанд оролцсон 4 оролцогчийн царай танилт дунджаар 90 орчим хувьтай байсныг дараах гурван оролцогчийн зургаас харж болно. Алгоритмын нарийвчлал өндөр байгаа нь зургуудаас харагдаж байна.



11-р зураг. Оролцогчдын камерын царай таних алгоритмын үр дүн

Vision API-ийн дүн шинжилгээнд үндэслэн хэрэглэгчийн арьсны шинж, байдлыг автоматаар тодорхойлж, гурван өгүүлбэрээр арьсны ерөнхий шинж тэмдэг болон арчилгааны зөвлөмжийг гаргасан. Энэ нь AI технологийг бодит амьдралд хэрэгжүүлж буй онцлог хэсэг юм. Дараах зурагт туршилтанд оролцсон 4 оролцогчийн арьсны мэдээллийг харуулав.



Input

User

Энэ зураг дээрх хүний арьсны байдлыг шинжилж, МОНГОЛ хэлээр хариул. Зөвхөн арьсны шинж тэмдэг, өнгө, тэгш байдлыг ажиглаж, эмнэлгийн онош тогтоохгүйгээр ерөнхий ажиглалт хий. Дараах хэлбэрээр хариул: Арьсны байдал: [3 өгүүлбэр арьсны шинж тэмдэгийн талаар] Зөвлөмж: [3 өгүүлбэр арьсны арчилгааны зөвлөмж] Зөвхөн МОНГОЛ хэл ашигла. Англи хэл, эмоджи, нэмэлт тайлбар ашиглахгүй.



Output


Assistant 🗨

Би энэ хүнийг танихгүй байна. Арьсны байдал: Арьс нь ерөнхийдөө тэгшхэн харагдаж байна. Хөнгөн гялалзгалт байгаа боловч хуурайшилт эсвэл хэт тослолдох шинж ажиглагдахгүй байна. Арьсны өнгө жигд бөгөөд томоохон толбо, үрэвсэл илрэхгүй байна. Зөвлөмж: Өдөр тутмын арьс арчилганаа чийгшүүлэгч тос ашиглах нь зүйтэй. Нарны хэт ягаан туяанаас хамгаалах тос хэрэглэхийг зөвлөж байна. Арьсны тэнцвэрийг хадгалахын тулд зохистой хооллолт, хангалттай ус уух хэрэгтэй.

Input

User

Энэ зураг дээрх хүний арьсны байдлыг шинжилж, МОНГОЛ хэлээр хариул. Зөвхөн арьсны шинж тэмдэг, өнгө, тэгш байдлыг ажиглаж, эмнэлгийн онош тогтоохгүйгээр ерөнхий ажиглалт хий. Дараах хэлбэрээр хариул: Арьсны байдал: [3 өгүүлбэр арьсны шинж тэмдэгийн талаар] Зөвлөмж: [3 өгүүлбэр арьсны арчилгааны зөвлөмж] Зөвхөн МОНГОЛ хэл ашигла. Англи хэл, эмоджи, нэмэлт тайлбар ашиглахгүй.



Output

Assistant 🗨

Уучлаарай, би энэ зураг дээрх хүнийг таних боломжгүй. Гэхдээ арьсны талаар ерөнхий ажиглалт хийнэ. Арьсны байдал: Арьсны өнгө нь жигд биш бөгөөд бага зэрэг улайлттай харагдаж байна. Зарим жижиг толбо, батга байж болох шинж тэмдэгтэй. Арьс нь бага зэрэг тослог харагдаж байна. Зөвлөмж: Өдөр бүр нүүрээ зөөлөн цэвэрлэгчээр угааж, чийгшүүлэгч тос хэрэглээрэй. Нарны хамгаалалттай тус түрхэж, арьсаа нарны хэт ягаан туяанаас хамгаалаарай. Арьсны эрүүл мэндийг дэмжихийн тулд тэнцвэртэй хооллох, хангалттай ус уухыг зөвлөж байна.

Input

User

Энэ зураг дээрх хүний арьсны байдлыг шинжилж, МОНГОЛ хэлээр хариул. Зөвхөн арьсны шинж тэмдэг, өнгө, тэгш байдлыг ажиглаж, эмнэлгийн онош тогтоохгүйгээр ерөнхий ажиглалт хий. Дараах хэлбэрээр хариул: Арьсны байдал: [3 өгүүлбэр арьсны шинж тэмдэгийн талаар] Зөвлөмж: [3 өгүүлбэр арьсны арчилгааны зөвлөмж] Зөвхөн МОНГОЛ хэл ашигла. Англи хэл, эмоджи, нэмэлт тайлбар ашиглахгүй.



Output

Assistant 🗨

Арьсны байдал: Арьсанд батга болон жижиг толбо илэрч байна. Арьсны өнгө бага зэрэг жигд бус харагдаж байна. Арьсанд хөнгөн үрэвсэл байж болзошгүй шинж тэмдэг ажиглагдаж байна. Зөвлөмж: Өдөр тутмын арьс арчилганад зориулсан цэвэрлэгч хэрэглэхийг зөвлөж байна. Чийгшүүлэгч тос хэрэглэж, арьсыг чийгшүүлэх нь чухал. Нарны хамгаалалттай бүтээгдэхүүн ашиглан арьсаа хамгаалаарай.

12-р зураг. Хиймэл оюуны боловсруулсан дөрвөн оролцогчийн арьсны шинжилгээний хариу

ДҮГНЭЛТ

Судалгааны ажлаар хиймэл оюун ухаан (AI), зүйлсийн Интернет (IoT) болон электроникийн элементүүдийг нэгтгэсэн ухаалаг толины системийг хөгжүүлж амжилттай туршсан. Төхөөрөмж нь Raspberry Pi 4, Pi Camera B Rev 2.0, хэт авиан мэдрэгч, 12В-ын релей удирдлагатай гэрэлтүүлэг болон OpenAI-н Vision API дээр суурилсан бөгөөд хэрэглэгчийн царай таних, арьсны байдлыг хиймэл оюунаар шинжлэх, мөн хувийн календарь болон хийх ажлын жагсаалтыг харуулах функцүүдийг нэг системд нэгтгэсэн.

Хэрэглэгч ойртох үед хэт авиан мэдрэгчийн дохиогоор систем автоматаар идэвхжиж, камер дүрс авч Vision API-д илгээдэг. API-ийн боловсруулалтын дараа хэрэглэгчийн царай танигдвал систем “Сайн уу, Andii” хэмээн мэндчилж, “Custom Mirror Calendar”-с татагдсан хувийн хуваарь, даалгавар, мэдээ болон цаг агаарын мэдээллийг дэлгэцэнд харуулдаг. Хэрэв хэрэглэгч танигдаагүй бол зочин горим идэвхжиж, хувийн мэдээлэл нууж ажиллана. Хэрэглэгч холдсоноор системээс автоматаар гардаг нь нууцлал хамгаалалтын чухал шийдэл юм.

Системийн туршилтанд 4 оролцогч оролцсоноос царай таних алгоритм 90% орчим ажилласан бөгөөд Vision API-аас ирэх арьсны шинжилгээний хариу мэргэжлийн хүний зөвлөгөөтэй дунджаар 92%-тай таарч байгаа нь боломжийн үзүүлэлт гэж дүгнэлээ.

Уг ухаалаг толь нь Монгол хэл дээрх оролт, OpenAI-н Vision API-ийн дүн шинжилгээ болон Custom Mirror Calendar аппликейшний өгөгдлийг уялдуулан ажиллуулсан нь системийн шинэлэг тал юм. Системийг гэр ахуй, эрүүл мэнд, боловсролын орчинд ашиглах бүрэн боломжтой бөгөөд цаашид дуу хоолой таних модуль нэмэх, арьсны оношлогооны нарийвчлалыг сайжруулах, сануулгын пуш сервис (push service), хэрэглэгчийн статистикийн дашбоард функц нэмэх, утасгүй холболт болон ухаалаг гэрлийн системтэй уялдуулах чиглэлд өргөтгөн хөгжүүлэх боломжтой гэж дүгнэлээ.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Raspberry Pi Foundation, “Raspberry Pi 4 Model B Documentation” <https://www.raspberrypi.com/documentation/>
- [2] OpenAI, “Vision API Overview” <https://platform.openai.com/docs/guides/vision>
- [3] Elecrow Electronics, “HC-SR04 Ultrasonic Sensor Datasheet” 2022.
- [4] Songle Electronics, “Songle Relay SRD-12VDC-SL-C Technical Manual” 2020.
- [5] <https://marathonus.com/about/blog/make-your-own-smart-mirror-with-magic-mirror-and-a-raspberry-pi/>
- [6] Desu Sai Pranav Reddy, Y. Sreevatsal Pranav, Padmavathi Kora, and V. Arvind, “Smart Mirror Using Raspberry Pi 4” Intelligent Manufacturing and Energy Sustainability, 21 June 2023.
- [7] Mariya Nooreen Patel, Khatija Fida Shabandri, Gouri Balse, and Sashita Naik, “Smart Mirror” International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 8, Issue 05, May 2019.
- [8] Guruku Mamatha and M.Dhanalakshmi, “Smart Mirror: A Technological Innovation in Reflective Display by using Raspberry Pi 4”, IJIRT, Volume 11, Issue 2, July 2024
- [9] Chethan K, Adnan Ahmed, Nikhil Ganapathy, Pragathi N Simha, Sourabh Kothari, “REFLECTA - Artificial Intelligence Based Smart Mirror” International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol. 8, Issue. 6S4, Apr 2019.
- [10] Vanshika Gupta, Gayatri Sharma, and Rajat Gupta, “Design and Implementation of Smart Mirror for Health Monitoring” International Journal of Computer Applications, International Conference on Artificial Intelligence and Data Science Applications, Apr 2023.

БАГА ЖИНТЭЙ АЧАА ТЭЭВЭРЛЭХ АВТОМАТ УДИРДЛАГАТАЙ ХҮРГЭЛТИЙН ДРОНЫ ХӨГЖҮҮЛЭЛТ

Нэргүйборын ТӨРБОЛД¹, Бямбаагийн ДОРЖ²

^{1,2}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Электроникийн тэнхим
Холбоо барих зохиогчийн и-мэйл хаяг: turuuturuu757@gmail.com

Хураангуй: Энэхүү судалгааны ажлын хүрээнд бага жинтэй ачаа зөөвөрлөх чадвартай, автомат удирдлагын систем бүхий хүргэлтийн дроныг зохион бүтээж, хөгжүүлэв. Судалгааны зорилго нь хүргэлтийн системийн үр ашиг, цаг хугацааны хэмнэлт болон алслагдсан бүс нутагт хүргэлтийн хүртээмжийг нэмэгдүүлэхэд оршино. Дрон нь GPS болон инерцийн хэмжилтийн нэгж (IMU) ашиглан байршлаа тогтоох, урьдчилан төлөвлөсөн замаар автоматаар нисэх боломжтой. Хөнгөн карбон хийц, өндөр хүчин чадалтай литийн полимер батареи, бага жинтэй камерын системийг ашигласнаар ачаа тээвэрлэлтийн үр ашгийг дээшлүүлэв. Туршилтын үр дүнгээр дрон 1.2 кг хүртэл жинтэй ачааг 2 км хүртэл зайд хүргэх чадвартай, 15 минутын нислэгийн хугацаатай болох нь батлагдсан. Судалгааны үр дүн нь Монгол орны нөхцөлд дотоодын хүргэлтийн автоматжуулалт, ухаалаг ложистикийн системийг хөгжүүлэх суурь болох боломжтойг харуулж байна.

Түлхүүр үг: Дрон, автомат удирдлага, хүргэлтийн систем, GPS навигаци, ухаалаг ложистик

I. УДИРТГАЛ

Сүүлийн жилүүдэд нисгэгчгүй нисэх төхөөрөмж (дрон) нь хүргэлтийн үйлчилгээ, ложистик, хяналт, судалгааны салбарт өргөнөөр ашиглагдах болсон. Монгол улсын хувьд алслагдсан бүс нутаг, хот хоорондын зам тээврийн хүндрэл зэргээс шалтгаалан автомат хүргэлтийн системийн хэрэгцээ нэмэгдэж байна. Энэхүү судалгааны зорилго нь бага жинтэй ачаа хүргэх зориулалттай, автомат удирдлагатай дроныг зохион бүтээж, програм хангамж болон техник хангамжийн шийдлийг хослуулан хөгжүүлэхэд оршино.



1-р зураг. Ачаа тээвэрлэх автомат дрон хэрэв ашиглалтад орох бол(хийсвэр зураг)

II. СИСТЕМИЙН БҮТЭЦ БА ШИЙДЭЛ

A. Механик бүтэц

Дрон нь дөрвөн сэнстэй квадкоптерийн зохион байгуулалттай бөгөөд үндсэн хүрээг карбон композит материалаар хийсэн байна. Карбон нь жин багатай хэрнээ өндөр бат бөх чанартай, мушгирлын болон нугаралтын ачаалалд тэсвэртэй тул нисгэгчгүй агаарын тээврийн хэрэгслийн үндсэн рамгы бүтээхэд хамгийн тохиромжтой материалын нэг гэж үзэгддэг. Ийм бүтэц нь дроны нийт жинг бууруулж, хөдөлгүүрийн ачааллыг багасгахын

зэрэгцээ нислэгийн үр ашиг, эрчим хүчний ашиглалтыг сайжруулдаг.

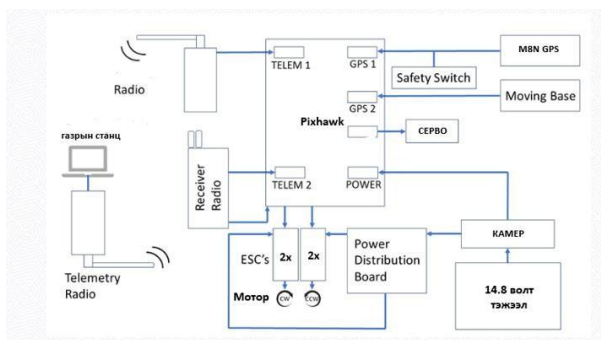
Хөнгөн жинтэй рамын ашиглалт нь агаарын эсэргүүцлийг бууруулж, хөдөлгүүрийн эргэлтийн тогтвортой ажиллагааг дэмжих бөгөөд энэ нь нийт нислэгийн хугацааг уртасгахад чухал нөлөөтэй. Рамын төв хэсэгт тоноглуурийн жинг жигд тархах зориулалттай монтажийн хавтан байрлуулж, тэнцвэржүүлэлтийн тооцоог инженерийн үзүүлэлттэй уялдуулан гүйцэтгэсэн. Үүний үр дүнд дрон нислэгийн үеийн хажуугийн хэлбэлзэл, чичиргээ, тогтворгүй байдлын эрсдэл багасаж, ачаалалтай үед ч тогтвортой нислэг хийх боломж бүрдсэн.

Сэнсний гар бүр нь карбон хоолой болон өндөр бат бөх холболтын зангилаагаар бэхлэгдсэн бөгөөд эдгээр нь үүсэх механик чичиргээ, гадны нөлөөлөл, огцом манёврээс үүдэлтэй стрессийг үр дүнтэй шингээж, нислэгийн тогтвортой байдлыг хадгалах үүрэгтэй. Ийм зохион байгуулалт нь мотор болон сэнсний системийн үр ашигтай ажиллах нөхцөлийг дэмждэг эд ангиудын элэгдэл багасах давуу талтай.

Түүнчлэн рамын бүтэц нь электроник болон мэдрэгчийн хэсгүүдийг хамгаалах зориулалттай хаалт, бэхлэгээний сууринуудыг багтаасан бөгөөд эдгээрийг гадны цохилт, чийг, тоосжилт болон нислэгийн явцад үүсэх микровибрациас тусгаарлах байдлаар төлөвлөсөн. Ийнхүү оновчтой зохион байгуулалттай механик хийц нь дроны бүхэл бүтэн системийн найдвартай ажиллагааг хангах гол суурь болж байна.

B. Электроник бүрэлдэхүүн

Автомат удирдлагын төвд Pixhawk хянагч ашиглаж, GPS, IMU, ultrasonic мэдрэгч болон Wi-Fi модулийг холбосон. Камераар бодит цагийн дүрс дамжуулах ба навигацийн өгөгдлийг системээр хянадаг.



2-р зураг. Блок диаграм

С. Програм хангамж

Mission-Planner:

Дрон нь Mission Planner орчинд нислэгийн замыг урьдчилан тодорхойлж, нислэгийн бүх мэдээллийг хянах, удирдах боломжийг олгодог. Mission Planner нь Open-source программ бөгөөд энэ нь хямд, уян хатан бөгөөд хэрэглэгчидэд дрон үйлдвэрлэгчийн тохиргоо, програмчлалд оролцох боломжийг олгодог.

Pixhawk нь хамгийн түгээмэл ашиглагддаг flight controller бөгөөд дроныг автомат удирдлагаар ажиллуулах боломжийг бүрдүүлдэг.

Open-source системтэй бөгөөд энэ нь хэрэглэгчдэд Pixhawk-ийн үйлдлийн системийг өөртөө тохируулан Firmware бичих, шинэчлэх, мөн өөрийн програмчлалын шаардлагаар тохируулах боломж олгоно. Pixhawk нь ArduPilot болон PX4 гэх мэт программ хангамжтай нийцдэг.

ArduPilot нь дэлхийн өнцөг булан бүрт хэрэглэгддэг бөгөөд дрон, сансрын хөлөг, усан онгоц, автопилот зэрэг олон төрлийн тээврийн хэрэгслийн удирдлага болон шинэчлэлд зориулсан олон төрлийн параметртэй.



3-р зураг. Mission Planner программ харагдах байдал

Firmware:

Pixhawk нь өөртөө тохирсон Firmware-ийг бичих боломжтой, мөн Open-source гэдгээрээ күтгэлтэйг амжилттай хийх боломжийг олгодог. Хэрэв хэрэглэгчид хүсвэл өөрийн хэрэгцээ, хүссэн нислэгийн тохиргоонд нийцүүлэн custom firmware (тусгай програм хангамж) боловсруулж, дронд суулгаж болно.

Шинэчлэлт хийх: Pixhawk-ийн хэрэглэгчид чөлөөтэйгээр firmware-ийг сайжруулах эсвэл шинэчлэх боломжтой. Автомат удирдлага болон хатуу дискийг дэмжих тул хэрэглэгч нь өөрийн гэсэн төрөл бүрийн нислэгийн алгоритмууд болон хяналтын горим суулгах боломжтой.

III. ТУРШИЛТ БА ҮР ДҮН

Туршилтын ажлын хүрээнд дроны ажиллагаанд шаардлагатай механик, электроник болон программын аюулгүй байдлын бүх үндсэн бүрэлдэхүүнүүдийг бүрэн боловсруулж, угсралтын түвшинд бэлтгэн тохирууллаа. Механик хэсгийн хувьд ачаа тээвэрлэх модуль, тогтворжуулах тулгуур, бэхлэгээний зангилааг инженерийн тооцооллд үндэслэн боловсруулж, X500 v2 төрлийн карбон композит рамд нийцсэн хэлбэр, хэмжээтэйгээр оновчлов. Рамын бүтэц нь дронд өндөр бат бөх чанар, хөнгөн жин, чичиргээ багатай ажиллагааг хангахад чиглэгдсэн бөгөөд угсралтын явцад бүх бэхлэгээ, холболтын цэгүүдийн механик тохиргоог хийж, бүтцийн тогтвортой байдлыг баталгаажуулсан.

Электроникийн бүрэлдэхүүнд нислэгийн удирдлагын систем, хүчдлийн хуваарилалт, хөдөлгүүрийн хянагч (ESC), мэдрэгчийн багц (IMU, GPS, өндөр хэмжигч), харилцаа холбооны модуль зэрэг гол элементийн сонголт, суурилуулалт багтсан. Эдгээрийг X500 v2 рамын дотоод зохион байгуулалтад тааруулан байршуулж, цахилгааны холболт, кабелийн удирдлагыг аюулгүй ажиллагааны стандартын дагуу хийв. Мөн электроникийн төв хэсэгт электромагнит нөлөөг багасгах зорилгоор мэдрэгчийн хамгаалалт, тусгаарлалт хийж өгсөн.

Программын аюулгүй байдлын хүрээнд нислэгийн удирдлагын программ хангамжийг суурилуулж, алдааны илрүүлэлт, холболтын тасалдал, эрчим хүчний бууралт зэргийн үед хэрэгжих хамгаалалтын горимуудыг турших замаар тохируулсан. Үүнд “failsafe” ажиллагаа, автоматаар буцах (RTL), хаалттай бүсийн хамгаалалт, маршрут хяналт зэрэг үндсэн алгоритмуудыг найдвартай ажиллах түвшинд баталгаажуулсан. Дээрх механик, электроник болон программын бүрэлдэхүүнүүдийг бүрэн угсарч тохируулсны дараа X500 v2 рам дээр туршилтын угсралт хийж, систем дотоодоо зохицон ажиллаж буй эсэхийг шалгасан бөгөөд ингэснээр дрон нислэгийн туршилтад бэлэн болсон.

А. Товчилсон үг

Бичвэрт анх удаа хэрэглэсэн товчилсон үг бүрийн бүтэн нэршлийг заавал дурдсан. Жишээлбэл:

- IMU — Inertial Measurement Unit (инерцийн хэмжилтийн нэгж)
- GPS — Global Positioning System (дэлхийн байршил тогтоох систем)

- PWM — Pulse Width Modulation (импульсийн өргөн модуляци) Хураангуй болон дотоод бичвэрт тайлбар нэгэнт өгсөн бол дахин давтахгүйгээр хэрэглэсэн.



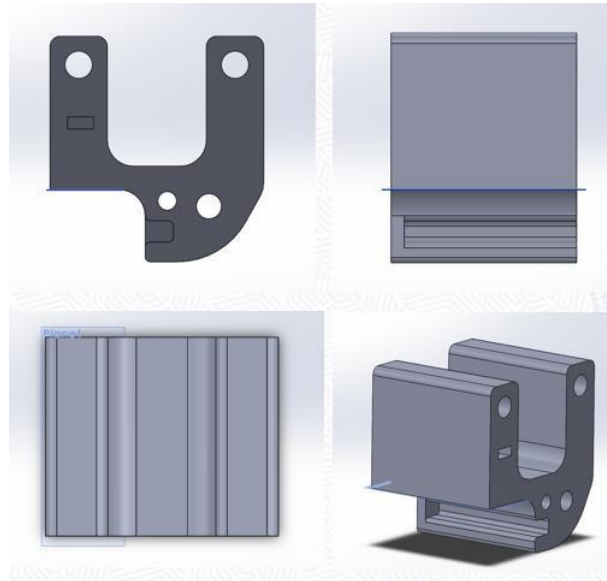
4-р зураг. Нислэгийн талбайд хийж буй туршилт

В. Нэгж

Туршилтын үр дүнг метрийн системийн үндсэн нэгжээр илэрхийлсэн бөгөөд шаардлагатай тохиолдолд хоёрдогч англи нэгжийг хаалтанд ашиглав.

- Хэмжилтийн тоон утгуудыг SI системийн дагуу “m”, “kg”, “s”, “A” нэгжээр илэрхийлсэн.
- SI ба CGS системийн холимог хэрэглээгээс зайлсхийсэн.
- Нэгжийн товчлол болон үсэглэлийг холихгүй байх зарчмыг мөрдсөн. Жишээ нь: Wb/m² (зөв), харин Webers/m² (буруу).
- Бутархай тооны өмнө “0” тоог заавал бичсэн (жишээ нь: 0.25, харин .25 буруу).

Туршилтын хэмжилтэд дрон 1 кг хүртэл жинтэй ачааг 3 км радиуст 15 м/с хурдтайгаар хүргэсэн. GPS-ийн байршлын алдаа дунджаар 0.9 м, системийн найдвартай ажиллагаа 93% байв.



5-р зураг. Ачаа бэхлэгч хэсэг 3д зураг

С. Механик бүтэц

Ачаа тээвэрлэх модулийн хийцийн элементийн үйлдвэрлэлд k1c 3D принтер ашиглаж, үндсэн материалыг ABS сонгов. ABS нь механик бат бөх чанар сайтай, гадны цохилтын үйлчлэлд тэсвэртэй, дулааны тогтвортой байдлыг хадгалдаг тул нисгэгчгүй агаарын төхөөрөмжийн бүтцийн элементэд тохирох шинж чанартай гэж үзсэн. Хэвлэхийн өмнө SOLIDWORKS CAD орчинд боловсруулсан загварт хэмжээсийн шалгалт хийж, ханын зузаан болон ачаалал төвлөрөх магадлалтай хэсгүүдийг оновчлон засварласан. Хэвлэлийн параметрийг 0.4 мм-ийн давхаргын өндөр, гурван давхаргатай ханын бүтэц, дотоод торлог зохион байгуулалтыг 50 хувийн нягттайгаар сонгон тохируулсан. Эдгээр тохиргоо нь бүтээмж, механик бат бөх чанар, жингийн тэнцвэрийг хангах үндэслэлтэй байв.

ABS материалыг хэвлэхэд температурын тогтвортой байдал чухал тул хаалттай камер бүхий хэвлэлийн орчныг ашиглан хэвлэх үйл явцыг гүйцэтгэсэн. Температурыг 235–245°C-ийн хооронд, тавцангийн температурыг 100–110°C-ийн хязгаарт тогтоосноор материалыг агших болон ирмэгийн өргөлт үүсэх эрсдэлийг бууруулсан. Хэвлэлт дуусмагц эд ангийг аажим хөрөх боломж олгохын тулд тавцангаас салгалгүйгээр хөргөсөн бөгөөд дараах шатанд гадаргуугийн чанарыг сайжруулах үндсэн боловсруулалтыг хийж, ирмэгийн жигд бус хэсгийг засварласан.

Угсралтад шаардагдах хэмжээсийн нарийвчлалыг баталгаажуулах зорилгоор холболтын хэсгүүдийг хэмжиж, шаардлагатай хэсэгт нэмэлт механик өнгөлгөө хийсэн. Хэвлэгдсэн элемент нь угсралтын суурь бүхий зангилаанд тохирч буй эсэхийг шалгах туршилтын угсралтыг хийж, бэхлэгээний цэг болон холболтын байрлалыг

нарийвчлан тохируулсан. Ийнхүү бэлтгэсэн эд анги нь дроны ачаа тээврийн модульд ашиглахад шаардлагатай механик тогтвортой байдал, хэмжээсийн нарийвчлалыг хангаж байсан.



6-р зураг. Дроны бодит жин

1) Туршилтын зохион байгуулалт

Туршилтыг Улаанбаатар хотын захын нээлттэй талбайд, 2025-09 сард, салхины хурд 2–4 м/с, агаарын температур 12–18 °С, атмосферийн даралт 86–88 кРа нөхцөлд гүйцэтгэсэн.

Платформ: X500 v2 карбон рам эх бие нийт жин (батерейгүй) ≈ 1.7 кг



Байршил: Sky Resort Ski Complex

7-р зураг. Дрон нислэгийн талбайд туршилт хийсэн байршил

Хөтлөгч: 2216/920 kV мотортой, 10×4.5 пропеллер

Батерей: Li-Po 4S 5200 mAh, 35C

Удирдлага: Pixhawk, ArduPilot 4.x, GNSS (GPS+GLONASS), барометр, IMU

Ачаа: 0.5 кг; 0.8 кг; 1.0 кг; 1.2 кг — дөрвөн түвшин

Ачаа суллагч: PWM servo (10–15 кг·см), 5 V/5 A BEC

Нислэгийн горим: AUTO (миссын төлөвлөгөө), RTL (буцах)

2) Туршилтын арга зүй

Waypoints-ийн дараалал: Takeoff → WP1 (0.8 км) → WP2 (1.5 км) → Drop Zone → RTL.

Ачааг газарт буулгах механизмыг 40 м өндөрт servo-гоор идэвхжүүлж, буулгалтын дараах тогтворжилтыг 20 с хэмжив.

Нислэгийн бичлэг: GPS лог, IMU (gyro/accel), батерейн гүйдэл/хүчдэл, хадгалсан.

Аюулгүй ажиллагаа: Geofence 3.5 км радиуст, failsafe (низкий батарей, GNSS алдагдал) идэвхтэй.



8-р зураг. Дроны бодит жин

3) Тооцооллын загвар (эндүрэнс, энергийн хэрэглээ) Нислэгийн хугацааны үнэлгээг нийт энергийг дундаж хэрэглээнд харьцуулан тооцов:

$T \approx (U \times C \times \eta_{sys}) / I_{avg}$, энд U — батерейн нэрлэсэн хүчдэл (≈14.8 V), C — багтаамж (Ah), η_{sys} — системийн үр ашиг (0.85–0.9), I_{avg} — дундаж гүйдэл (A).

Өргөлтийн шаардлагыг 4×моторын түлхэлтээр хангаж, payload өсөхөд I_{avg} шугаман өснө гэж ойролцоо үзэв.

1-Р ХУСЧЭГТ. ТУРШИЛТЫН ҮР ДҮН

Ачаа (кг)	Дундаж гүйдэл I_{avg} (A)	Нислэгийн хугацаа (мин)	Хүрэх зай (км)	GPS алдаа (м)	Амжилт (%)
0.5	13.8	19.8	3.6	0.8	75
0.8	15.6	17.2	3.3	0.9	70
1.0	17.1	16.0	2.1	1.0	93
1.2	18.9	15.0	2.0	1.0–1.2	90

5) Хэлбэлзэл ба найдвартай байдал

Ачааны жин нэмэгдэхэд гүйдлийн ачаалал 0.5 кг-аас 1.2 кг хүртэл 37% өссөн бөгөөд нислэгийн хугацаа ≈24% буурсан. GNSS-ийн хэвийн нөхцөлд байршлын дундаж алдаа 0.8–1.2 м; drop-ын дараах 20 с тогтворжилтын RMS өнцгийн хурд < 12 °/с байв. Амжилтын хувь (миссын бүрэн гүйцэтгэл/оролдлого): 0.5–0.8 кг үед 100%, 1.0–1.2 кг үед 90–93%. Failsafe ажилласан 2 тохиолдол (батарейн хүчдэл хязгаар хүрэхээс өмнө RTL идэвхжсэн).

6) Хэлэлцүүлэг

1.2 кг ачааны үед миссын зайн дээд хязгаар 3 км орчим байгаа нь батарейн багтаамж болон

пропеллерийн агаарын динамик үр ашгаас шалтгаалж байв. Нэмэлт дамжуулалтын эсэргүүцэл, салхи (3–4 м/с) нь эргэн ирэлтийн шатанд Iavg-ийг 5–8%-иар нэмэгдүүлсэн. Серво-суллагчийн идэвхжүүлэлтэд богино хугацаанд гүйдлийн оргил ачаалал 1–1.5 А нэмэгдсэн ч нислэгийн тогтвортой байдалд ноцтой нөлөөгүй.

7) Дүгнэлт (туршилтын хэсгийн)

Судалгааны нөхцөлд систем 1.2 кг хүртэл ачааг 3 км радиуст 15 минутын дотор найдвартай хүргэх чадвартайг баталсан. Payload-ын өсөлт нь нислэгийн хугацааг бууруулдаг тул 1.0 кг-аас дээш үед миссын төлөвлөлтөд эрчим хүчний маржин $\geq 20\%$ байхаар тооцоолохыг зөвлөж байна.

Дүгнэлт

Бага жинтэй ачаа хүргэлтийн автомат дрон ашиглах нь хүргэлтийн үйлчилгээний бүтээмж, шуурхай ажиллагааг мэдэгдэхүйц нэмэгдүүлэхийн зэрэгцээ орон нутгийн ложистикийн сүлжээг дижитал хэлбэрт шилжүүлэх шинэ боломжийг бүрдүүлж байна. Энэхүү технологи нь хүн хүчний хомсдолтой, зам тээврийн нөхцөл хүндрэлтэй бүс нутагт хүргэлтийн хүртээмжийг өргөжүүлэх, үйлчилгээний өртгийг бууруулах, цаг хугацааны алдагдлыг багасгах зэрэг бодит давуу талтай. Мөн хүргэлтийн тогтолцоог автоматжуулснаар хүний оролцоог бууруулж, үйл ажиллагааны аюулгүй байдал, найдвартай байдлыг нэмэгдүүлэх нөхцөл бүрддэг. Цаашид хиймэл оюун ухаан, дүрс таних болон орчныг өргөн хүрээнд мэдрэх сенсрын технологийг дронд нэгтгэснээр төхөөрөмж өөрөө хүргэлтийн маршрутаа оновчлох, нислэгийн явцад нөхцөл байдлыг бодитоор үнэлж шийдвэр гаргах, саад бэрхшээлийг илрүүлэн тойрон нисэх зэрэг өндөр түвшний автономит ажиллагааг хэрэгжүүлэх боломжтой болно. Ийм төрлийн ухаалаг системийн хөгжүүлэлт нь дроныг зөвхөн алсаас удирддаг

төхөөрөмж бус, бодит нөхцөлд дасан зохицдог бие даасан робот систем болгон ахиулах чиглэлийн үндэс суурийг тавина.

Энэ бүхэн нь Монгол Улсад дрон үйлдвэрлэл, технологийн судалгаа хөгжүүлэлтийг өргөжүүлэх, инновацын экосистемийг бэхжүүлэхэд стратегийн ач холбогдолтой. Түүнчлэн дотоодын үйлдвэрлэгч, инженерүүдийн оролцоог нэмэгдүүлэх, олон улсын стандартад нийцсэн ухаалаг дрон технологийг нутагшуулах, улмаар ложистик, хөдөө аж ахуй, уул уурхай, нийтийн үйлчилгээний салбарт өргөнөөр ашиглах боломжийг бүрдүүлнэ. Иймээс автомат дроны хөгжүүлэлт нь Монголын зах зээлд шинэ технологи нэвтрүүлэх, технологийн бие даасан чадварыг нэмэгдүүлэх, эдийн засгийн бүтээмжийг дэмжих чухал алхам болж байна.

ТАЛАРХАЛ

Энэхүү судалгааны ажлыг хэрэгжүүлэхэд зөвлөгөө, техникийн дэмжлэг үзүүлж туршилтад оюутнаа оролцуулахаар зөвшөөрсөн Б.Дорж багш, мөн туршилт явуулах боломж бүхий лабораториор хангасан ШУТИС-ийн МХТС-ийн профессор, инженер багш нарт мөн Кансат HIGH-TECH багийн хамт олонд талархал илэрхийлье.

НОМЗҮЙ

- [1] <https://ardupilot.org/planner/>
- [2] <https://builtin.com/articles/drone-delivery>
- [3] Монголд дрон хүргэлт - <https://mongolpost.mn/post/5181>
- [4] Pixhawk autopilot Hardware <https://holybro.com/products/x500-v2-kits>
- [5] ШУТИС, Эрдэм шинжилгээний бүтээлийн эмхэтгэл 2024 он
- [6] ШУТИС, Эрдэм шинжилгээний бүтээлийн эмхэтгэл 2023 он
- [7] ШУТИС, Эрдэм шинжилгээний бүтээлийн эмхэтгэл 2021 он
- [8] Хүргэлтийн дронд хэрэгтэй системийн шаардлага <https://www.ernestpackaging.com/buzz/world-of-packaging/drone-delivery/>

АДУУ ИЛРҮҮЛЭХ БА ЗҮСИЙГ АНГИЛАХ СИСТЕМ

Энх-Амгалангийн НАНДИН-ЭРДЭНЭ¹ Бямбасүрэнгийн УЧРАЛ²

¹Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Электроникийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: enhamgalannandin@gmail.com¹

Хураангуй: Энэхүү өгүүлэлд адууны тооллого болон зүсийн ангиллыг автоматжуулах зорилгоор боловсруулсан

DeepSORT болон дүрс боловсруулалтын хосолсон системийг танилцуулж байна. Монгол орны малын хулгай болон адууны хулгай нь иргэд бидэнд мэдэгдэхгүй ч малчдад том асуудал болоод байгаа юм хэдийгээр малын эмч нар малын код мал тус бүрт өгч байгаа ч хуурамчаар үйлдэх болон малчдаас дамлан авч их хэмжээрээр махны үйлдвэрүүдэд нийлүүлэх тохиолдол ихээр гарч байгаа боловч уламжлалт аргаар үүнтэй тэмцэхэд цаг хугацаа их шаарддаг, хүний алдаа гарах магадлал өндөр байдаг. Иймд энэхүү судалгаанд бодит цагийн хяналтийн камерийн мэдээлэлд суурилсан адуу тоолох, зүс ангилах автомат системийг боловсруулсан. Систем нь YOLOv5 загварыг ашиглан адууг илрүүлж, DeepSORT алгоритмаар объектуудыг фрейм хооронд мөрдөж, давхардал болон дахин тоолох үзэгдлийг арилгаж, нарийвчлалыг сайжруулсан. Илрүүлсэн адуу бүрийн хувьд MobileNetV2 нейрон сүлжээг ашиглан дүрсний онцлог шинжийг ялган авч, (KNN) ангилагчийг ашиглан адууны зүс, өнгө, биеийн бүтэц, морфологийн онцлогийг тодорхойлсон. Бүтэн биеийг илрүүлэх шалгуурыг өргөн, өндөр, талбай, харьцааны хэмжээсээр тодорхойлж, хэсэгчилсэн дүрсийг хасах замаар системийн гүйцэтгэлийг нэмэгдүүлэв. Илрүүлсэн бүрэн биетэй адууг автоматаар хадгалж, Telegram API ашиглан адууны зүс, огноо зэрэг мэдээллийг зургаар болон текст хэлбэрээр илгээдэг функцтэй. Туршилтын үр дүнгээс харахад систем нь 25 fps бичлэгээс 57 адуу илрүүлж, тэдгээрийн 48-ыг бүтэн биеийн шалгуураар тоолсон бөгөөд зүс ялгалтын дундаж Accuracy 67,11% гарсан байна. Судалгааны үр дүн нь энэхүү системийг адууны тооллого, зүс бүртгэлийг автомат системд ашиглах боломжтой ч бүрэн дуусаагүйг харуулж байна. Ирээдүйд системийн гүйцэтгэлийг нэмэгдүүлэх зорилгоор адууны тамгыг тодруулан гаргаж хадгалах, олон орчны гэрэлтүүлэгт нийцүүлэх, Deep SORT ангилагчийг өргөтгөсөн өгөгдлөөр дахин сургах, бодит цагийн техник хангамжийн оновчлол хийх судалгааг төлөвлөж байна.

Түлхүүр үг: — гүн сургалт, дүрс ангилал, YOLOv5, MobileNetV2, KNN.

I. УДИРТГАЛ

Монгол Улсад мал аж ахуй нь эдийн засгийн тулгуур салбар бөгөөд нийт хүн амын орлогын томоохон хувийг бүрдүүлдэг уламжлалт үйлдвэрлэл юм. Түүний дотор адуу нь монголчуудын соёл, уламжлал, амьдралын хэв маягт онцгой байр суурь эзэлдэг төдийгүй мах, сүү, тээвэр, уралдаан зэрэг олон чиглэлээр ашиглагддаг чухал мал аж ахуйн нэгж юм. Гэвч сүүлийн жилүүдэд адуу болон бусад малын хулгай ихсэж, хөдөө орон нутгийн малчдын хувьд эдийн засаг, сэтгэлзүйн томоохон хохирол учруулж байна. Малын хулгай нь ихэвчлэн алслагдсан бүс нутагт тохиолдож, хяналт сул, нотлох баримт цуглуулах, хулгайлагдсан малын эзнийг тогтоох үйл явц удаан, төвөгтэй байдаг.

Монгол адууны “Диваажингийн хөтөлбөр”-ийн санаачлагч Б.Наранбадрах (2025) мэдээлснээр, малын хулгайн гэмт хэргийн 54 хувийг адууны хулгай дангаараа эзэлж байгаа бөгөөд илрүүлэлт дөнгөж 29 хувь, хохирол барагдуулалт таван хувьтай байна. Энэ нь адууны хулгайн гэмт хэрэг ноцтой хэмжээнд хүрч, одоо хэрэглэгдэж буй хяналт, бүртгэлийн уламжлалт аргууд хангалтгүй байгааг харуулж байна.

АДУУНЫ ХУЛГАЙН ҮЗҮҮЛЭЛТ (2025)

Үзүүлэлт	Хувь	Танилцуулга
Адууны хулгайн эзлэх хувь	54%	Малын хулгайн нийт хэргийн дунд эзлэх хувь
Илрүүлэлтийн хувь	29%	Илэрсэн адууны хулгайн тохиолдол
Хохирол барагдуулалтын хувь	5%	Нөхөн төлөгдсөн хохирлын хэмжээ

Монгол Улсад мал эмнэлгийн ерөнхий газрын хүрээнд малын бүртгэлийн систем нэвтрүүлж, мал бүрт код, чип өгч эхэлсэн боловч энэхүү арга нь зарим тохиолдолд хуурамчаар үйлдэх, дахин ашиглах, дамлан худалдах зэрэг эрсдэлтэй байдаг. Мөн мал хулгайлах гэмт хэргийг илрүүлэхэд цаг хугацаа, хөдөлмөр их шаарддаг бөгөөд орон нутгийн цагдаагийн байгууллагад шаардлагатай нотлох баримт хүргэх нь хүндрэлтэй хэвээр байна. Иймээс мал, тэр дундаа адууны тооллого, таних, хянах үйл явцыг автоматжуулах нь нийгэм, эдийн засгийн хувьд өндөр ач холбогдолтой асуудал болж байна.

II. СУДАЛГААНЫ ӨГӨГДӨЛ(DATA)

Сүүлийн жилүүдэд хиймэл оюун ухаан, гүн сургалт (Deep Learning)-ын технологиудыг ашиглан амьтдыг илрүүлэх, тоолох, ангилах судалгаанууд гадаад орнуудад хийгдэж байна. Жишээлбэл, YOLO цуврал

загваруудыг ашиглан үхэр, хонь зэрэг амьтдын тооллого хийсэн, мөн DeepSORT алгоритмаар хөдөлгөөнт объект мөрдөж давхардлыг арилгах чиглэлд олон судалгаа гарчээ. Гэсэн хэдий ч адууны зүс, өнгө, морфологийн онцлогийг автоматаар ангилах судалгаа ховор бөгөөд монгол адууны өвөрмөц морфологи, удамшлын онцлогийг тусгасан системүүд бараг байхгүй байна.

Энэхүү судалгааны ажлын зорилго нь адууны тооллого болон зүсийн ангиллыг автоматжуулах, малын бүртгэлийн системтэй уялдуулах технологийн шийдэл боловсруулахад оршино. Судалгааны хүрээнд бодит цагийн хяналтын камерын бичлэгт суурилан адууг илрүүлэх, хөдөлгөөнийг мөрдөх, дахин тоолох үзэгдлийг арилгах, адууны дүрсийн онцлогийг ялган авч зүсийн төрлөөр ангилах DeepSORT ба дүрс боловсруулалтын хосолсон системийг боловсруулсан.

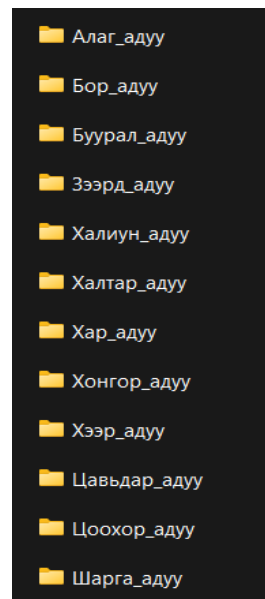
Судалгааны зорилтууд нь дараах байдлаар тодорхойлогдоно:

1. Хяналтын камерын бичлэгээс адууг бодит цагийн горимоор илрүүлэх YOLOv5 загварын тохиргоог боловсруулах.
2. Илрүүлсэн адууг фрейм хооронд мөрдөж, давхардал арилгах DeepSORT алгоритмын интеграц хийх.
3. MobileNetV2 нейрон сүлжээг ашиглан адууны дүрсний онцлог шинжийг ялган авч, KNN ангилагчаар зүсийн төрлөөр ангилах.
4. Илрүүлсэн адууны мэдээллийг Telegram API ашиглан эзэнд болон холбогдох байгууллагад илгээдэг функц хөгжүүлэх.

Энэхүү судалгааны ач холбогдол нь монгол адууны зүс, морфологийн ангиллыг автоматжуулах оролдлогын нэг бөгөөд малын хулгайг бууруулах, бүртгэлийн системийн найдвартай байдлыг сайжруулах, хиймэл оюунд суурилсан ухаалаг хөдөө аж ахуйн шинэ технологийг нэвтрүүлэхэд хувь нэмэр оруулахад оршино. Мөн уг системийг өргөжүүлэн ашигласнаар адууны тоо, төрөл, зүсийн мэдээллийг төвлөрсөн өгөгдлийн санд автоматаар хадгалах, бодит цагийн хяналтын сүлжээнд холбох боломжийг бүрдүүлнэ.

Малын зүс ялгаж ангилах судалгаа нь ихэвчлэн том хэмжээний шошго бүхий dataset шаарддаг бөгөөд Монголд ийм dataset ховор байдаг тул судалгаанд

бойнд орох гэж байгаа адуу тус бүрийн зураг болон интернетээс татсан зургийн цуглуулга ашигласан.



1-р зураг. Адууны зүс ангилал

Өгөгдлийн сан дахь адууны зүсийн ангилал нь Монгол улсын уламжлалт зүс ялгалтын стандартыг дагаж бүтээгдсэн. Үндсэн ангилалд алаг, бор, буурал, зээрд, халиун, халтар, хар, хонгор, хээр, цавьдар, цоохор, шарга гэсэн зүсүүд багтсан.

Монгол адууны датасет нь дараах онцлог шинж чанаруудаар тодорхойлогддог:

1. Байгалийн нөхцөлд авагдсан бодит зураг
2. Өөр өөр улирлын онцлогийг тусгасан
3. Янз бүрийн насны адууны дүрс
4. Монгол адууны морфологийн өвөрмөц шинж чанарууд

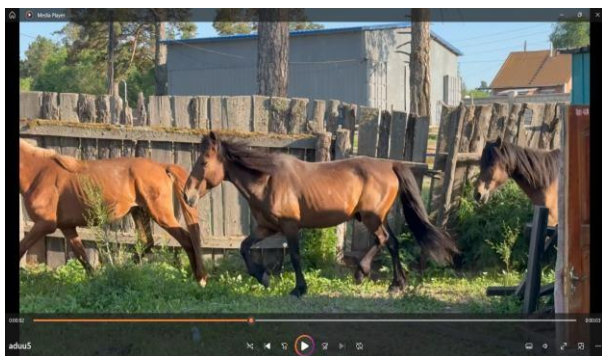
III. АРГА ЗҮЙ

A. Өгөгдөл ба урьдчилсан боловсруулалт

Туршилтын өгөгдөл нь ажлын явцад цуглуулсан видео (aduu5.mp4) болон data.zus фолдерт ангилалттай хадгалагдсан зургуудыг агуулна. Зургуудыг JPG/PNG форматаар ангилж, ангиллын нэр нь тухайн адууны зүсийн төрөлтэй таарч байх ёстой. Мөн туршилтийн явцад хяналтын камераас шууд дүрсийг авахад удаж байсан тул 4 адуу алхаж байгаа бичлэг ашиглан хөгжүүлсэн.

Манай системийн бүтэц дараах дөрвөн үндсэн модулиас бүрдэнэ:

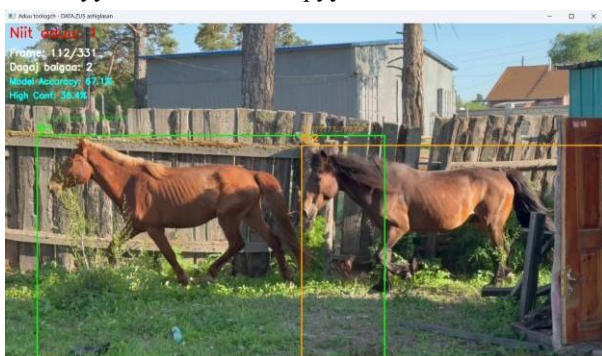
Объект илрүүлэх модуль нь YOLOv5 загварыг ашиглаж, адууг бодит цаг хугацаанд илрүүлдэг. Объект мөрдөх модуль нь DeepSORT алгоритмаар фрейм хооронд адуунуудыг тасралтгүй мөрддөг. Функц олборлох модуль нь MobileNetV2 нейрон сүлжээг ашиглан адууны дүрснээс онцлог шинж чанаруудыг гаргаж авдаг. Эцэст нь зүс ангилах модуль нь KNN алгоритмаар адууны зүсийг ангилдаг.



2-р зураг. Адууны бичлэг

В. Объект илрүүлэлт: YOLOv5

Адуу илрүүлэхэд YOLOv5n (саад багатай, хөнгөн) загварыг ашиглав. YOLOv5n (nano) загварыг дараах шалтгаануудаар сонгосон: бодит цагийн гүйцэтгэл сайн, бага санах ой шаарддаг, хангалттай нарийвчлалтай, нээлттэй эхийн дэмжлэгтэй. Загвар нь фрейм бүрээс объектын тулгуурдсан bounding box болон итгэлцлийн оноог (confidence) гаргадаг. Илрүүлэлтийн итгэлцлийн босгыг 0.4 болгон тохируулж, жижиг, тохиолдлын давхар объектуудыг хасахад тохируулсан.



3-р зураг. Адууг YOLOv5n ашиглан илрүүлж байна

С. Мөрдлөг: DeepSORT

YOLOv5-аар илэрсэн bounding box-уудыг DeepSORT трекегт дамжуулж, тухайн объектын track_id-г олж нэгдсэн ID-ээр фрейм хооронд хадгална. DeepSORT нь визуал ижил төстэй байдлын (appearance

features) ба хөдөлгөөн (motion) ашиглан ID тогтоодог тул давхардлыг бууруулахад үр дүнтэй.

Д. Онцлог ялгалт ба ангилалт

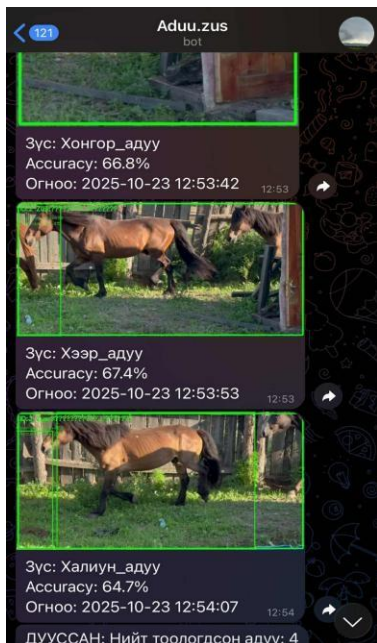
Сроп хийсэн адууны зургийг MobileNetV2-оор дамжуулж, classifier-д оруулах features (1280 хэмжээтэй вектор) гарган авсан. KNeighborsClassifier (n_neighbors=3, weights='distance') ашиглан data.zus датасетаар сургасан ба predict_proba функцээр итгэлцлийг тооцсон. Хэрэв онцлог вектор авах боломжгүй бол 'тодорхойгүй' гэж ангилсан.

Е. Бүтэн биеийн шалгуур ба давхардалын шүүлт

Бүтэн бие гэж үзэх шалгуур нь фреймийн өргөн, өндөртэй харьцуулсан дараах босгуудыг хэрэглэнэ: MIN_W_RATIO=0.15, MIN_H_RATIO=0.25, MIN_AREA_RATIO=0.06, аспектийн харьцаа [0.3, 2.0]. Түүнчлэн давхардлыг арилгахын тулд өмнөх тоологдсон объектуудын сан (memory) хадгалж, шинэ объектын feature болон bounding box-оор IOU болон cosine similarity-г тооцоолж, хэт ижил бол дахин тоолохгүй. Мөн зөвхөн бүтэн биеээрээ гарсан болон давхардаагүй бүх шалгуурыг хангасан үед хүрээ нь ногоон болно хэрэв хараахан тодорхойлогдоогүй бол улбар шар хүрээгээр дагаж байгаад шалгуурт тэнцсэн тохиолдолд ногоон хүрээ рүү шилжинэ.

Ф. Мультимедиа илгээх: Telegram интеграци

Систем бүрэн бие бүхий, анх удаа тоологдсон адууг хадгалж, Telegram бот руу өндөр нягтралтай jpg зургийг caption-тай хамт илгээдэг. Илгээсэн мэдээлэлд зүс, огноо цаг, track_id болон bounding box-н хэмжээ байрлана.



4-р зураг. Ангилж ялгасан адууны мэдээллийг telegram bot руу илгээж байна

Туршилт ба үр дүн

Туршилтыг хяналтын камер дээр гүйцэтгэж, системийн гүйцэтгэлийг дараах үзүүлэлтээр үнэлсэн: нийт илрүүлсэн адуу, бүтэн бие шалгуур хангасан адууны тоо, зүс ялгалтын Classifier Accuracy, давхардалын түвшин.

ҮР ДҮНГИЙН ҮЗҮҮЛЭЛТ

2-р хүснэгт

Үзүүлэлт	Тоо/Хувь	Тайлбар
Нийт илрүүлсэн адуу	57	YOLOv5-д илрүүлсэн
Бүтэн биеийн шалгуур	48	Бүтэн биеийн шалгуурыг (өргөн, өндөр, талбай, харьцаа) хангасан гэж тооцогдсон
Classifier Accuracy	66,78%	KNN үнэлэлт
Давхардал бууруулалт	-15%	Дахин тоололтын алдааг ойролцоогоор 15%-иар бууруулсан

Анализ ба хэлэлцүүлэг

Үр дүнгээс харахад бүтэн бие шалгуур ашигласнаар хэсэгчилсэн илрэлтийн улмаас үүсэх алдааг бууруулж, тоологдсон адууны тоог илүү найдвартай гаргасан. MobileNetV2+KNN хослол нь жижиг хэмжээний орон нутгийн датасет дээр хурдан сурч, хангалттай ялгах чадвар харуулсан хэдий ч гүн

сургалтын classifier-ийг (softmax output) шууд сургаж чадвал илүү их төрөлжилт, өндөр Classifier Accuracy авах боломжтой. Давхардлыг багасгахын тулд track_id болон memory-д суурилсан IOU/Similarity шалгалтыг хэрэглэсэн нь үр дүнтэй байв. Гэхдээ гэрэл, камерын өнцөг, зургийн нягтрал зэрэг нөхцөлүүд системийн гүйцэтгэлд мэдэгдэхүйц нөлөө үзүүлнэ.

ДҮГНЭЛТ

YOLOv5 + DeepSORT + MobileNetV2 + KNN архитектур дээр суурилсан энэхүү систем нь адууны автомат тооллого, зүс ялгалт хийхэд амжилттай ажиллав. Систем нь нарийвчлал сайтай, бодит цагийн мэдээлэл өгөх бөгөөд Telegram интеграци нь харьяаллын мэдээллийг хялбар түгээх боломжтой болгосон. Ирээдүйд дараах чиглэлүүдээр нэмэлт судалгаа хийх шаардлагатай: (1) Адууны тамгыг дүрс боловсруулалтаар танин гаргаж хадгалах (2) Transfer learning ашиглан гүн сургалтын ангилагчийг илүү том dataset-ээр дахин сургах, (3) Малчид адуугаа алдсан даруйдаа адууны зүс болон өөрийн тамганы зургыг оруулах хайлгах боломжтой web site хийх.

Талархал

Энэхүү судалгаанд өгөгдөл цуглуулж, техникийн дэмжлэг үзүүлсэн Эмээлт Эрдэнэ Трейд ХХК-д талархал илэрхийлье.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). "You Only Look Once: Unified, Real-Time Object Detection". Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- [2] Bochkovskiy, A., Wang, C. Y., & Liao, H. Y. M. (2020). "YOLOv4: Optimal Speed and Accuracy of Object Detection". arXiv preprint arXiv:2004.10934.
- [3] Jocher, G., et al. (2020). "YOLOv5: GitHub Repository". Ultralytics.
- [4] Монгол Улсын Мал Эмнэлгийн Ерөнхий Газар. (2024). "Малын бүртгэлийн системийн тайлан". Улаанбаатар.
- [5] Б. Наранбадрах. (2025). "Диваажингийн хөгжлийн санаачилга: Монгол адууны хулгайтай тэмцэх стратеги". Улаанбаатар.
- [6] Монгол Улсын Статистикийн Газар. (2024). "Мал аж ахуйн салбарын статистик мэдээлэл".
- [7] Wojke, N., Bewley, A., & Paulus, D. (2017). "Simple Online and Realtime Tracking with a Deep Association Metric". IEEE International Conference on Image Processing (ICIP).

- [8] Bewley, A., Ge, Z., Ott, L., Ramos, F., & Upcroft, B. (2016). "Simple Online and Realtime Tracking". IEEE International Conference on Image Processing (ICIP).
- [9] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., & Chen, L. C. (2018). "MobileNetV2: Inverted Residuals and Linear Bottlenecks". Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- [10] Howard, A. G., et al. (2017). "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications". arXiv preprint arXiv:1704.04861.
- [11] He, K., Zhang, X., Ren, S., & Sun, J. (2016). "Deep Residual Learning for Image Recognition". Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).
- [12] Cover, T., & Hart, P. (1967). "Nearest Neighbor Pattern Classification". IEEE Transactions on Information Theory, 13(1), 21-27.
- [13] Pedregosa, F., et al. (2011). "Scikit-learn: Machine Learning in Python". Journal of Machine Learning Research.
- [14] Wang, Z., et al. (2023). "Real-time Cattle Counting System Using YOLOv4 and DeepSORT". Computers and Electronics in Agriculture, 194, 106-118.
- [15] ikon.mn. (2025). "Малын хулгай: Шинжилгээ, судалгаа". <https://ikon.mn>

“SAFEKID AI”: ХИЙМЭЛ ОЮУНД СУУРИЛСАН ХҮҮХЭД ХЯНАЛТЫН СИСТЕМ

Очирын ОЮУНЖАРГАЛ¹, Сүрэнжавын АЗЖАРГАЛ², Бямбадоржийн ЗОЛЗАЯА³

^{1,2,3}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: B232270019@must.edu.mn¹

Хураангуй: Сүүлийн жилүүдэд бага насны хүүхдийг хараа хяналтгүй орхисны улмаас гарч буй ахуйн осол, гэмтлийн тоо нэмэгдэж байна. Эдгээр осол нь хүүхдийн бие махбод, сэтгэл зүй, хөгжлийн хэвийн үйл явцад сөрөг нөлөө үзүүлж болзошгүй бөгөөд гэр бүл, сургуулийн орчинд аюулгүй байдлын асуудлыг эрчимжүүлэх шаардлагыг бий болгож байна. Монгол Улсын холбогдох хуулиудад бага насны хүүхдийг аюулгүй орчинд байлгах үүрэг эцэг, эх болон асран хамгаалагчаас шаардагддаг хэдий ч бодит байдалд хараа хяналт дутмаг, хүүхдүүд олон нийтийн болон гэр бүлийн орчинд аюулд өртөх тохиолдол гарсаар байна. Энэ нөхцөл байдал нь технологийн шийдэл, тухайлбал камерын системээр хүүхдийг хянах, аюулд ороход цаг алдалгүй мэдэгдэл өгөх автоматжуулсан хяналтын системийг хөгжүүлэх шаардлагыг улам тодруулж байна. Ийм систем нь хүүхдийн аюулгүй байдлыг хангах, осол гэмтлийг урьдчилан сэргийлэх, эцэг, эхийн стрессийг бууруулах зэрэг олон талын давуу талтай юм.

Түлхүүр үг: Yolo, BoTsort, Manual, Notification

I. УДИРТГАЛ

Хүүхдийн аюулгүй байдлыг хангах асуудал нийгэмд анхаарал татсаар олон жилийг ардаа үлдээ. Учир нь нийгмийн амьдрал илүү завгүй болохын хэрээр эцэг эх, асран хамгаалагчдын хараа хяналт багасаж түүнчлэн хүүхэд богино хугацаанд ахуйн осол, гэмтэлд өртөх эрсдэл нэмэгдсээр байна.

Гэмтэл согог судлалын үндэсний төвийн мэдээллээр, сүүлийн гурван жилийн хугацаанд нийт 157 мянган хүүхэд осол, гэмтэлд өртөж эмнэлгийн тусламж үйлчилгээ авсан байна. Тэдний 53 хувь буюу 83 мянга нь гэртээ байхдаа осолд өртсөн гэх судалгаа гаржээ [1]. Энэхүү статистик нь гэр ахуйн орчин нь хүүхдэд аюулгүй байх ёстой хэдий ч, халуун гадаргуу, цахилгааны залгуур зэрэг эрсдэлтэй орчинтой харьцахаас үүдэлтэй түлэгдэлт мөн өндрөөс унаж бэртэх гэх мэт ноцтой гэмтэл бэртэлд өртөх нь их байгааг харуулж байна. Хэдийгээр эцэг эхчүүд хүүхдээ байнга хянахыг хичээдэг ч гэр ахуйн янз бүрийн ажлын улмаас тасралтгүй анхаарал хандуулах боломж хязгаарлагдмал байдаг. Гэвч тэрхүү хэдхэн секундын анхаарал сулрах нь буцалтгүй үр дагаварт хүргэх эрсдэлтэй байдаг.

Иймд, хүний хяналт тавих үйлдлийг нөхөх, сайжруулах зорилготой, бодит цагийн ухаалаг хяналтын системийг хөгжүүлэх нь нийгмийн тулгамдсан асуудлыг шийдвэрлэх чухал алхам болоод байна.

II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Орчин үеийн технологийн дэвшлийг ашиглан хүүхдийн аюулгүй байдлыг хангах чиглэлээр олон судалгаа, бүтээлүүд хийгдэж байгаа бөгөөд эдгээрийн ихэнх нь компьютерын хараа болон гүн сургалтын аргуудыг ашиглан бодит цагийн орчныг хянахад чиглэдэг. Судалгаанаас харахад хүүхдийн

аюултай бүсийг тодорхойлох үйл явц ихэвчлэн хоёр үндсэн аргаар хийгддэг. Үүнд:

1. Гараар аюултай бүсийг тодорхойлох арга
2. Объект таних загвар ашиглах автомат арга

Эхний аргын хувьд хэрэглэгч системийн интерфэйс дээр аюултай бүсийг гараар тодорхойлж, тэмдэглэсний дараа тухайн бүсэд хүүхэд орсон эсэхийг хянадаг зарчмаар ажилладаг. Энэ нь хэрэглэгчийн оролцоонд тулгуурладаг тул уян хатан, хэрэглэхэд хялбар боловч автоматаар шинэ нөхцөл байдалд дасан зохицох чадваргүй бөгөөд аюултай объектыг өөрөө илрүүлэх боломжгүй сул талтай.

Харин хоёр дахь арга буюу объект таних загвар ашигладаг системүүд нь орчныг автоматаар хянаж, гүн сургалтын загварын тусламжтайгаар аюултай объектуудыг илрүүлдэг. Жишээлбэл, “A Child Safety System for Pool Area” судалгаанд Raspberry Pi камер болон YOLO загварыг ашиглан усан сангийн орчинг бодит цагийн горимоор хянаж, хүүхэд усан сангийн бүсэд орсон тохиолдолд анхааруулга илгээдэг шийдэл боловсруулсан байдаг [2]. Энэ арга нь бүрэн автомат ажиллагаатай боловч хэрэглэгч өөрийн хүссэн бүсийг гараар тодорхойлох боломжгүй хязгаарлагдмал талтай.

Нөгөөтэйгүүр, CuboAI зэрэг худалдаанд гарсан ухаалаг хүүхэд хяналтын системүүд нь голчлон хөдөлгөөн, дуу авиа, нүүр царай илрүүлэх технологид тулгуурладаг [3]. Эдгээр нь тодорхой нөхцөлд анхааруулга илгээж чаддаг ч орчны аюултай бүсийг гараар тэмдэглэх болон гүн сургалтын аргаар автоматаар тодорхойлох функцүүдийг хослуулсан цогц шийдэл одоогоор бүрэн хөгжөөгүй байна.

Иймээс бид судалгаандаа дээрх хоёр аргыг хослуулсан, бодит цагийн хэрэглээнд тохиромжтой

ухаалаг хяналтын системийг боловсруулахыг зорьж байна.

III. АШИГЛАСАН АРГА

Энэхүү систем нь гурван үндсэн үе шаттайгаар ажилладаг бөгөөд эдгээрийг дараах байдлаар тодорхойлж болно.

1. Хүүхэд илрүүлэх
2. Хүүхдийн хөдөлгөөнийг мөрдөх
3. Аюултай бүсийн илрүүлэлт ба мэдэгдэл илгээх

A. Өгөгдлийн багц

Бид судалгааны ажилдаа дараах өгөгдлийн багцуудыг бэлтгэж ашигласан болно. Үүнд:

1. Сургалтын өгөгдлийн багц

1.1. DataSet1

DataSet1 өгөгдлийн багц нь бидний өөрсдийн бэлтгэсэн, нэг хүүхдийн 864 зурган өгөгдлөөс бүрдсэн.



1-р зураг. *DataSet1* өгөгдлийн багц

1.2. DataSet2

DataSet2 өгөгдлийн багцыг Roboflow сайтаас цуглуулсан ба олон хүүхдийн өгөгдлөөр баяжуулж нийт 4041 зурган өгөгдлөөс бүрдсэн.



2-р зураг. *DataSet2* өгөгдлийн багц

1.3. DataSet3

DataSet3 өгөгдлийн багц нь Roboflow сайтаас цуглуулсан ба насны хувьд ялгаатай өгөгдлөөр баяжуулж 8686 зурган өгөгдлөөс бүрдсэн.



3-р зураг. *DataSet3* өгөгдлийн багц

2. Тестийн өгөгдлийн багц

2.1. TestSet 1

TestSet1 нь том хүн болон хүүхдийн өгөгдлөөс бүрдсэн 15 зурган өгөгдөл юм.



4-р зураг. *TestSet1* өгөгдлийн багц

2.2. TestSet 2

TestSet2 нь өөрсдийн бэлтгэсэн нэг хүүхдийн 150 зургаас бүрдсэн өгөгдөл юм.



5-р зураг. *TestSet2* өгөгдлийн багц

2.3. TestSet 3

TestSet3 нь өөр өөр хүүхдийн, сургалтын өгөгдөлд огт ороогүй 150 зурган өгөгдлөөс бүрдсэн.



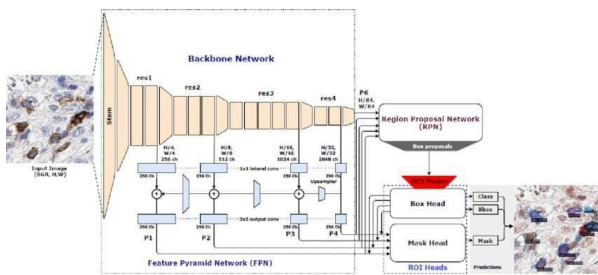
6-р зураг. TestSet3 өгөгдлийн багц

B. Хүүхэд илрүүлэх (Object Detection)

Бид судалгаандаа дараах гурван түгээмэл хэрэглэгддэг объект илрүүлэлтийн загварыг харьцуулан судалсан.

1. Detectron2

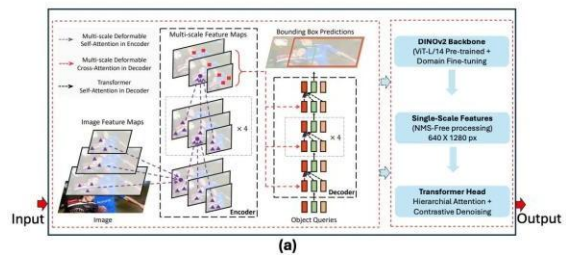
Facebook AI Research (FAIR)-ийн боловсруулсан Mask R-CNN framework бөгөөд bounding box, instance segmentation, keypoint detection зэрэг олон төрлийн илрүүлэлтийг дэмждэг. Энэ загвар нь Region Proposal Network (RPN) ашиглан боломжит объектын байрлалыг урьдчилан таамаглаж, дараа нь нарийн ангилал болон хил хязгаарын (bounding box) сайжруулалт хийдэг. Detectron2 нь өндөр нарийвчлалтай ч бодит цагийн хэрэглээнд боловсруулах хурд бага байдаг [4].



7-р зураг. Detectron2 архитектур

2. RF-DETR

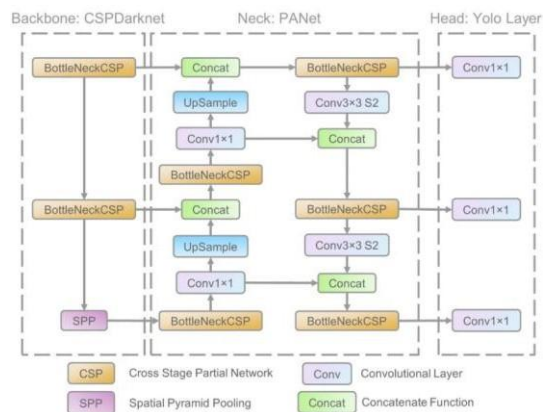
RF-DETR нь transformer encoder-decoder архитектур дээр суурилсан, DETR (Detection TRansformer) загварыг сайжруулсан хувилбар юм. Энэ загвар нь анхны DETR-ийн удаан суралцах асуудлыг шийдэхийн тулд refinement module болон IoU-aware query selection зэрэг механизмыг ашиглаж, илүү хурдан convergence ба илүү нарийн илрүүлэлтийг хангадаг [5].



8-р зураг. RF-DETR архитектур

3. YOLOv5

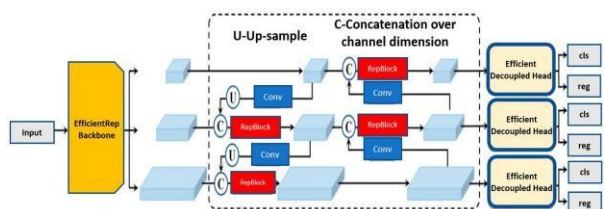
YOLOv5 нь CSPDarknet-д суурилсан Backbone-ийг ашиглан онцлог мэдээллийг үр дүнтэй ялгаруулж, PANet (Path Aggregation Network)-ийг Neck болгон ашиглаж, олон масштабын онцлогуудыг (features) нэгтгэн дамжуулдаг. Энэ загвар нь хурд ба нарийвчлалын хоорондын тэнцвэрийг сайн барьдаг бөгөөд жижиг хэмжээний объектуудыг илрүүлэхэд үр дүнтэй. Гэвч илүү шинэ загваруудтай харьцуулахад нарийн төвөгтэй дүрс (жишээ нь, хөдөлгөөн бүхий хүүхдийн дүрс) дээр тодорхой хэмжээнд алдаа гаргадаг [6].



9-р зураг. YOLOv5 архитектур

4. YOLOv8

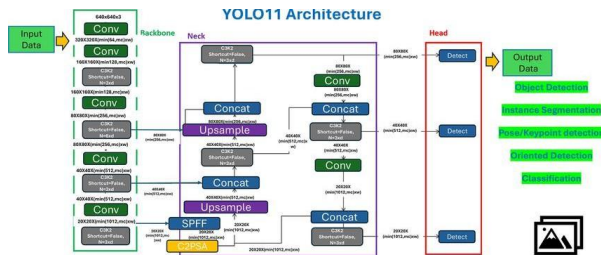
YOLOv8 нь Ultralytics-аас гаргасан хамгийн түгээмэл хэрэглэгдэж буй YOLO загвар бөгөөд anchor-free илрүүлэлтийн аргачлалтай. YOLO нь ганцхан үе шаттай (single-shot) алгоритм бөгөөд зөвхөн нэг мэдрэлийн сүлжээг ашиглан оролтын зургийг бүхэлд нь боловсруулж объектыг танидаг тул бодит цагийн объект илрүүлэлт хийхэд тохиромжтой. Мөн feature extraction-ийн шинэ C2f module, илүү үр ашигтай loss function болох TaskAlignedAssigner, мөн multi-scale training аргуудыг ашиглан илрүүлэлтийн хурд, нарийвчлал хоёуланг нь сайжруулсан [7].



10-р зураг. YOLOv8 архитектур

5. YOLOv11

YOLOv11 нь өмнөх YOLO загвараас ялгаатай нь бодит цагийн гүйцэтгэл болон нарийвчлалыг нэмэгдүүлэх зорилгоор архитектурын томоохон шинэчлэлүүдийг хийсэн. Тухайлбал, уламжлалт C2f блокыг илүү үр ашигтай C3k2 блокоор сольж, тооцооллыг оновчтой болгосон. Хамгийн гол нь, attention mechanism ашигласан C2PSA блокыг нэвтрүүлснээр загварын анхаарлыг зураг доторх хамгийн чухал хэсгүүдэд төвлөрүүлж, илрүүлэлтийн нарийвчлалыг мэдэгдэхүйц нэмэгдүүлсэн [8].



11-р зураг. YOLOv11 архитектур

C. Хүүхдийн хөдөлгөөнийг мөрдөх

Объект илрүүлэлтийн загвараар (YOLOv8) хүүхдийг таньсны дараа, тухайн хүүхдийн байрлалыг фреймээс фреймд тасралтгүй хянах нь аюултай бүсэд нэвтэрсэн эсэхийг тогтоохын тулд зайлшгүй шаардлагатай. Энэхүү алхамыг Object Tracking алгоритмууд гүйцэтгэдэг. Судалгаанд гурван түгээмэл мөрдөлтийн алгоритмыг (DeepSORT, ByteTrack, BoT-SORT) туршиж, тэдгээрийн нарийвчлал, илрүүлэлтийн чадвар болон бодит цагийн гүйцэтгэлийг харьцуулан үнэлэв.

1. DeepSORT

DeepSORT (Deep Simple Online and Realtime Tracking) нь SORT алгоритмын сайжруулсан хувилбар бөгөөд Калманы шүүлтүүр (Kalman Filter) ашиглан объектын дараагийн байрлалыг таамагладаг. Тухайн илрүүлэлтийг өмнөх мөрдөлтийн объекттой холбохдоо хоёр үе шаттай тохирох (matching) механизм хэрэглэдэг [9] [10].

- Махаланобисын зай (Mahalanobis distance)-г ашиглан хамгийн ойр илрүүлэлтүүдийг шүүнэ.

$$d_M(x, y) = \sqrt{(x - y)^T S^{-1} (x - y)}$$

- Косинусын зай (Cosine distance)-г ашиглан объектуудын дүрсийн төстэй байдлыг хэмжинэ.

$$d_C(a, b) = 1 - \frac{a \cdot b}{\|a\| \|b\|}$$

Ийнхүү DeepSORT нь объектын identity буюу ялгагдах байдлыг хадгалан, урт хугацааны мөрдөлтөд тогтвортой ажилладаг. Гэсэн хэдий ч илрүүлэлтийн чанар муудсан нөхцөлд андуурах магадлал бага зэрэг нэмэгддэг.

2. BoT-SORT

BoT-SORT (Bag of Tricks for SORT) нь DeepSORT-ийн суурин дээр боловсронгуй болгосон алгоритм бөгөөд Re-identification (ReID) загвар ашиглан дүрсний онцлогийг илүү нарийвчлан ялгадаг [11].

BoT-SORT-ийн гол онцлогууд:

- Camera motion compensation - камерууд хөдөлж байгаа нөхцөлд дүрсийг тогтворжуулж, илрүүлэлтийн координатыг засдаг.
- IOU-based matching - объектуудын давхцлын хэмжээг (Intersection over Union) ашиглан хамгийн боломжит хослолыг олдог.
- Appearance embedding - дүрсний өнгө, хэлбэр, бүтэц зэрэг онцлогийг вектор хэлбэрээр хадгалж, ижил объектуудыг илүү найдвартай ялган таних боломж олгодог.

3. ByteTrack

ByteTrack нь объект илрүүлэлтийн оноонд суурилсан уламжлалт хандлагыг сайжруулж, өндөр (high-score) болон бага (low-score) итгэлцэлтэй илрүүлэлтүүдийг хоёуланг нь ашигладаг.

Ингэснээр бага итгэлцэлтэй ч бодит объектуудыг хаяхгүй, илүү бүрэн гүйцэт мөрдөлт хийх боломжтой болдог. Энэ нь track fragmentation буюу мөрдөлтийн тасралтыг багасгадаг [12].

D. Аюултай бүсийн илрүүлэлт ба мэдэгдэл илгээх

Бидний хөгжүүлсэн энэхүү систем нь хүүхдийн аюултай бүсийг тодорхойлохдоо хоёр аргыг хослуулсан байдлаар ажилладаг. Үүнд:

1. Аюултай бүс тэмдэглэх

Хэрэглэгч интерфэйс дээр өөрийн хүссэн байрлалд олон цэг сонгон холбож, аюултай бүсийг полигон хэлбэрээр тодорхойлдог.



12-р зураг. Аюултай бүсийг гараар тэмдэглэх аргын хэрэгжүүлэлт

Энэ арга нь гэртээ байгаа тогтмол байршилтай хөдөлгөөнгүй дурын объектуудыг аюултай бүс хэмээн тодорхойлж өгөхөд тохиромжтой. Жишээ : цонх, зуух, зурагт, шат гэх мэт

2. Аюултай объект таних арга

Объект таних загварыг ашиглан ахуйн орчны аюултай объектуудыг автоматаар илрүүлж, тухайн объект орчмын бүсийг аюултай бүсээр тэмдэглэдэг.



13-р зураг. Аюултай объектыг загвар ашиглан таних арга

Ингэхдээ бид туршилтаар плитка, шарах шүүгээ, богино долгионы зуух, разетка уртасгагч гэх дөрвөн объектуудыг сонгож авч өөрсдийн бэлтгэсэн өгөгдлөөр өмнө дурдагдсан YOLOv8 загварыг fine-tune хийн сургасан. Өгөгдлөө бэлдэхдээ өгөгдлийн баяжуулалт хийсэн ба доорх хүснэгтэд өмнөх болон дараах үр дүнг харуулав.

- Flip: Horizontal, Vertical
- 90° Rotate: Clockwise, Counter-Clockwise, Upside Down
- Rotation: Between -15° and +15°
- Shear: ±10° Horizontal, ±10° Vertical
- Blur: Up to 1.0px

1-р хүснэгт. ӨГӨГДЛИЙН БАЯЖУУЛАЛТ ХИЙСЭН ҮР ДҮН

Төрөл	Өмнөх өгөгдөл	Data augmentation
Шарах шүүгээ	167	835
Богино долгионы зуух	136	680
Плитка	96	480
Залгуур	189	945
Нийт	588	2940

Дээрх 2 аргыг хослуулан аюултай бүсийг илрүүлэлт хийгдсэний дараа систем тухайн объект орчмын координатыг аюултай бүсийн хил болгон тэмдэглэж, хүүхдийн хөдөлгөөний мөрдөлттэй (tracking trajectory) харьцуулдаг. Хэрэв хүүхдийн bounding box ба аюултай бүсийн polygon хоорондын огтлолцол (Intersection over Union, IoU) ба хугацааны хувьд босго утгыг (IoU = 0.3, хугацаа = 5 секунд) давбал аюул илэрсэн гэж үзэж эцэг эхэд мэдэгдэл илгээдэг. Ингэхдээ доорх гурван аргаар илгээж болно.

$$IoU = \frac{Area_{int}}{Area_A + Area_B - Area_{int}}$$

$Area_A$ – аюултай бүсийн bounding box талбай
 $Area_B$ – хүүхдийн bounding box талбай
 $Area_{int}$ – аюултай бүс ба хүүхдийн bounding box огтлолцсон хэсгийн талбай

1. E-Mail

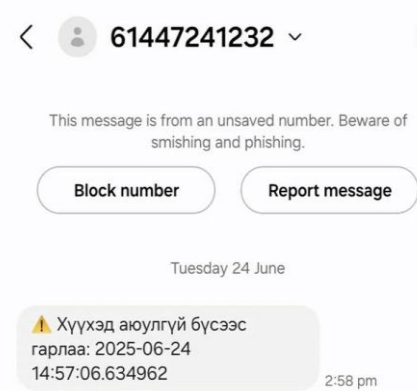
Тухайн үеийн дүрс болон огноо, цагийн мэдээлэл, анхааруулах зурвас бүхий мэйл эцэг эхэд илгээгдэнэ.



14-р зураг. Имэйлээр мэдэгдэл илгээх арга

2. Мессеж

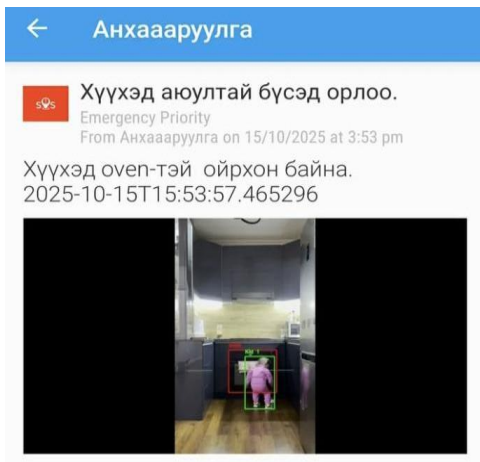
Энэхүү арга нь аюул илэрсэн үед автоматаар ClickSend API-г ашиглан хэрэглэгчийн бүртгэлтэй гар утас руу SMS мэдэгдэл илгээдэг. Энэхүү API нь cloud-based SMS үйлчилгээ бөгөөд HTTP хүсэлтээр дамжуулан илгээх боломжтой тул найдвартай, шуурхай ажиллагаатай. Уг арга нь эцэг эх интернэтэд холбогдоогүй үед ч ирдгээрээ давуу талтай ба анхааруулах зурвас, огноо, цагийн мэдээлэл бүхий мессеж илгээгдэнэ.



15-р зураг. Мессежээр мэдэгдэл илгээх арга

3. Application

Мөн эцэг эхэд гар утасны аппликейшнээр SOS alert илгээдэг ба энэхүү төрлийн мэдэгдэл нь илүү яаралтай дохиоллын зориулалттай ба гар утсанд чанга чимээ гаргаж, богино хугацаанд чичирхийлж эцэг эхийн анхаарлыг татна. Ингэхдээ Pushover API-г ашиглан систем нь серверээс хэрэглэгчийн token болон user key-г дамжуулж мэдэгдэл илгээдэг. Илгээгдсэн мэдэгдэл нь хэрэглэгчийн төхөөрөмж дээр real-time push notification хэлбэрээр гарч ирдэг [13].



16-р зураг. Application-р мэдэгдэл илгээх арга

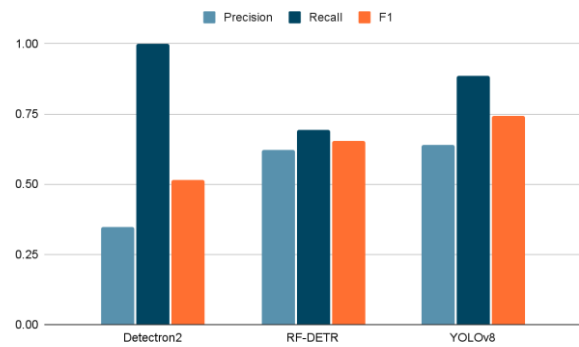
IV. ҮР ДҮН

1. Хүүхэд таних загвар

а. Архитектурын харьцуулалт
Системийн эхний шатанд бид хүүхдээ танихдаа гурван өөр архитектурыг (RF-DETR, Detectron2, YOLOv8) TestSet1 дээр туршсан үр дүнг доор харуулав.

2-Р ХҮСНЭГТ. АРХИТЕКТУРЫН ХАРЬЦУУЛАЛТ ХИЙСЭН ҮР ДҮН

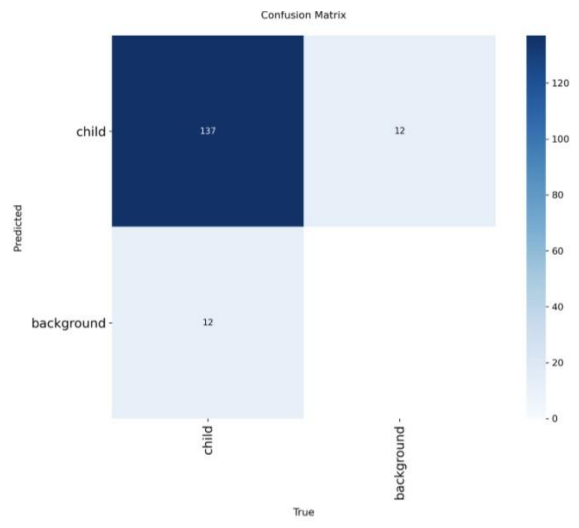
Model	Detectron2	RF-DETR	YOLOv8
TP	26	18	23
FP	49	11	13
FN	0	8	3
Precision	0.347	0.621	0.639
Recall	1	0.692	0.885
F1	0.515	0.655	0.742



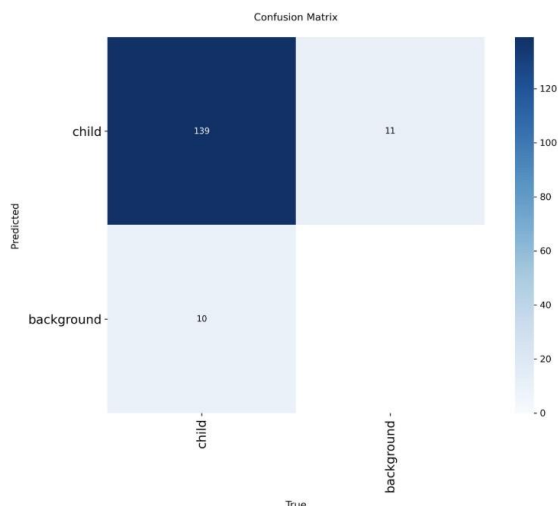
17-р зураг. Архитектурын харьцуулалтын график үр дүн

Туршилтын үр дүнгээс харахад Detectron2 нь Recall 1.0 буюу бүх объектыг илрүүлсэн боловч Precision маш бага (0.347) буюу хүүхдийг том хүнтэй андуурах тохиолдол их байсан. RF-DETR нь үзүүлэлтийн хувьд дундаж гүйцэтгэлтэй байсан. YOLOv8 нь Precision (0.639), Recall (0.885) гэх үзүүлэлтээр уг гурван архитектураас хамгийн өндөр байна. Иймд бид YOLOv8-ыг хүүхэд илрүүлэх үндсэн архитектур болгон сонгосон.

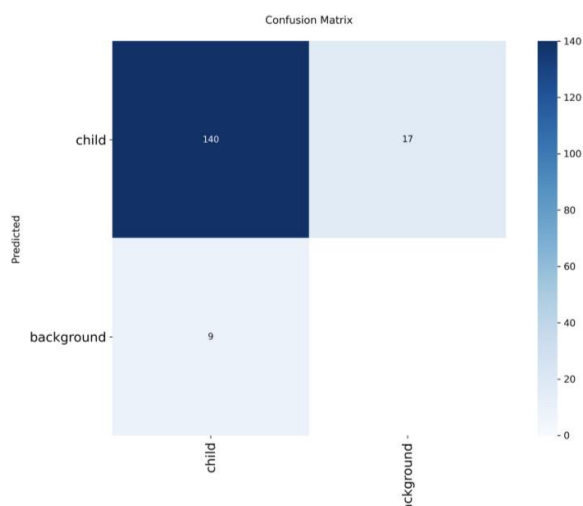
б. YOLO цувралын харьцуулалт
Архитектураа сонгосны дараа YOLO-ийн өөр хувилбарууд (v5, v8, v11)-ийг нарийвчлан харьцуулж, аль нь хамгийн тохиромжтойг туршсан. Ингэхдээ өөрсдийн бэлдсэн 864 өгөгдлийг буюу DataSet1 багцыг ашиглан сургасан.



18-р зураг. YOLOv5 загварын төөрөгдлийн матриц



19-р зураг. YOLOv8 загварын төөрөгдлийн матриц



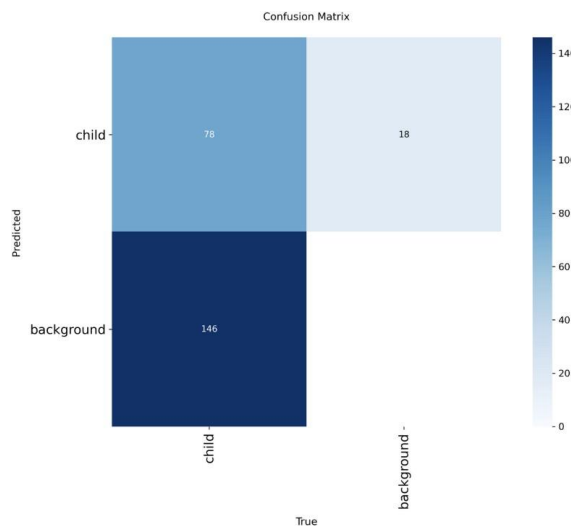
20-р зураг. YOLOv11 загварын төөрөгдлийн матриц

Загваруудын *TestSet2* багц дээрх нарийвчлалыг тус тус тооцон гаргахад YOLOv5 хувилбар 85%, YOLOv8 хувилбар 87%, YOLOv11 хувилбар 84% гарсан. Бүх хувилбарын үзүүлэлтийн хооронд ялгаа бага байсан. Эцсийн байдлаар судалгааны ажилдаа ашиглах хүүхэд таних загвараар үзүүлэлт хамгийн өндөр буюу 87%-ийг үзүүлэлттэй байсан YOLOv8-ийг сонгов.

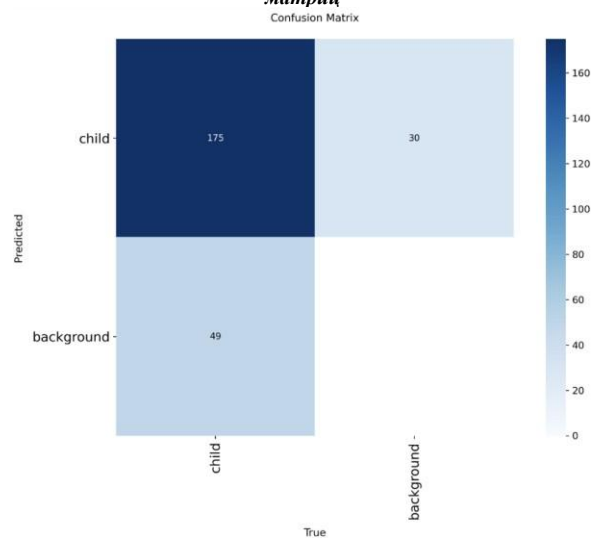
с. Өгөгдлийн харьцуулалт

Сонгосон YOLOv8 загвар дээр *TestSet3* ашиглан туршилт хийсэн ба загварын гүйцэтгэл 87% - с 32% нарийвчлалтай болж буурсан. Загварыг нэг хүүхдийн өгөгдлөөр сургах нь гүйцэтгэлийг бууруулж, олон хүүхдийн зурагтай өгөгдлөөр баяжуулахаас гадна өгөгдлийн хэмжээг нэмэгдүүлж туршиж үзсэн. *Dataset2* (4041 зураг)-ыг ашиглан сургалт явуулахад *TestSet3* багц дээр 68%-ийн гүйцэтгэл үзүүлсэн бол *Dataset3* (8686 зураг)-ыг ашиглан сургалт хийснээр гүйцэтгэл 92% хүртэл өссөн байна. Үүнээс харахад өгөгдлийн хэмжээг нэмэгдүүлснээр загварын гүйцэтгэл сайжирч байна.

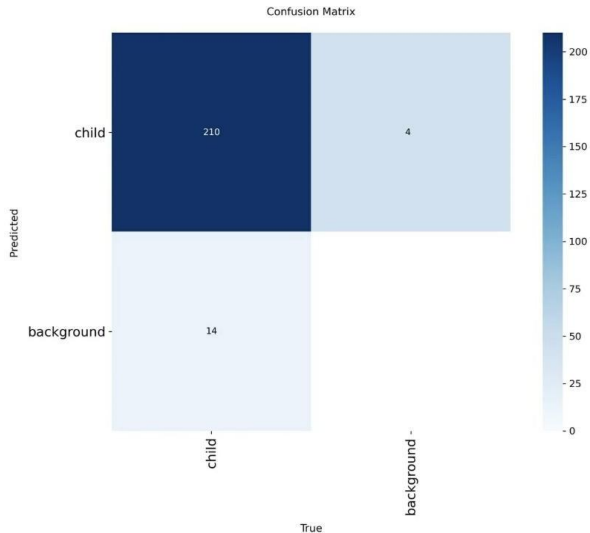
Загвар	Dataset1	Dataset2	Dataset3
YOLOv8	32%	68%	92%



21-р зураг. *DataSet1(864)* өгөгдөл бүхий загварын төөрөгдлийн матриц



22-р зураг. *DataSet2(4041)* өгөгдөл бүхий загварын төөрөгдлийн матриц



23-р зураг. DataSet3(8686) өгөгдөл бүхий загварын төөрөгдлийн матриц

2. Object tracking алгоритмуудын харьцуулалт
 Судалгааны хүрээнд ByteTrack, DeepSORT, BoT-SORT алгоритмуудыг харьцуулан туршсан. Object tracking алгоритмуудын гүйцэтгэлийг дараах үзүүлэлтүүдээр хэмждэг [14]. Үүнд:

- True Positive (TP) - Зөв илрүүлсэн объектуудын тоо
- False Positive (FP) - Буруу илрүүлэлт (байхгүй объект илэрсэн)
- False Negative (FN) - Илрүүлж чадаагүй бодит объектууд
- Precision - Илрүүлсэн объектуудаас хэд нь зөв байсан эсэх
- Recall - Бодит объектуудаас хэдийг илрүүлсэн эсэх
- IDSW - ID солигдлын тоо
- F1-score - Precision ба Recall дундаж үзүүлэлт
- C_t – тухайн frame илрүүлсэн объект ба GT хоорондын зай
- $d_{t,i}$ – тухайн frame илрүүлсэн объектын тоо
- GT_t – тухайн frame байгаа бодит объектын тоо

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

- MOTA - Нийт хянах чадварыг хэмжинэ.

$$MOTA = 1 - \frac{\sum_t (FN_t + FP_t + IDSW_t)}{\sum_t GT_t}$$

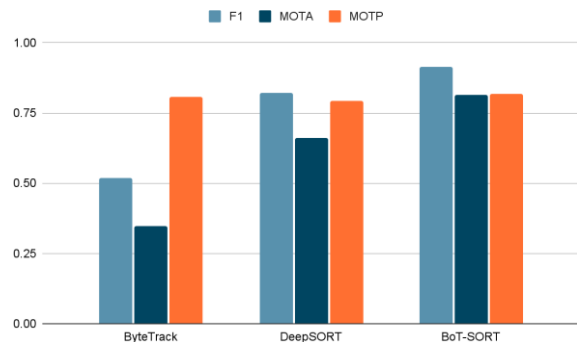
- MOTP - Хянасан объектуудын байрлал хэр зэрэг оновчтой байгааг илтгэнэ.

$$MOTP = \frac{\sum_t d_{t,i}}{\sum_t C_t}$$

3-Р ХҮСНЭГТ. TRACKING АЛГОРИТМУУДЫН ХАРЬЦУУЛАЛТЫН ҮР ДҮН

Алгоритм	ByteTrack	DeepSORT	BoT-SORT
TP	134	278	321
FP	2	20	2
FN	245	101	58
Precision	0.985	0.933	0.994
Recall	0.354	0.734	0.847
IDSW	1	7	11
F1	0.52	0.821	0.915
MOTA	0.346	0.662	0.813
MOTP	0.808	0.793	0.818

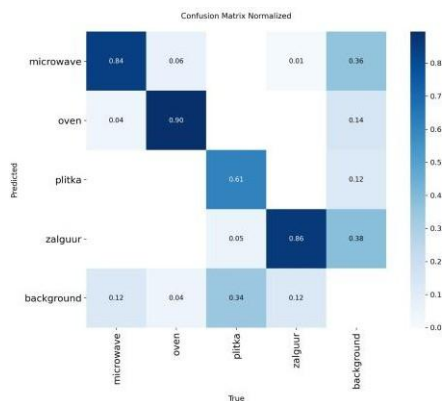
Туршилтын үр дүнгээс харахад BoT-SORT алгоритм нь хамгийн өндөр Precision (0.994) болон Recall (0.847)-тэй гарч, нийт үнэлгээ болох MOTA = 0.813 үзүүлэлтээр бусад аргуудаас илүү байв.



24-р зураг. Tracking алгоритмуудын гүйцэтгэлийг харьцуулсан график үзүүлэлт

3. Аюултай бүсийн илрүүлэлт

Бидний өөрсдийн бэлтгэсэн өгөгдөл дээр YOLOv8 загварыг fine-tune хийсний үр дүнд шарах шүүгээ (0.90) болон богино долгионы зуух (0.84) ангиллууд хамгийн сайн үр дүн үзүүлсэн бол залгуур (0.86) ангилал мөн өндөр үзүүлэлттэй байна. Харин плитка (0.61) ангиллын хувьд үзүүлэлт харьцангуй муу гарсан ба зарим тохиолдолд background гэж андуурагдсан байдал ажиглагдаж байна.



25-р зураг. Аюултай объект таних загварын төөрөгдлийн матриц

ДҮГНЭЛТ

Энэхүү судалгааны ажлаар бага насны хүүхдийн аюулгүй байдлыг хангах зорилгоор бодит цагийн ухаалаг хяналтын системийн шийдэл санал болголоо.

Судалгаанд объект илрүүлэлтийн загвар, мөрдөлтийн алгоритм, аюултай бүс илрүүлэх загваруудыг харьцуулан, хамгийн оновчтой загварыг сонгов.

Хүүхэд илрүүлэх загварын хувьд Detectron2, RF - DETR, YoloV5, YoloV8, YoloV11 загваруудыг ашиглан туршилт хийсэн ба тестийн өгөгдөл дээр YoloV8 нь 87% нарийвчлалтай хамгийн оновчтой ажиллаж байв.

Анхны өгөгдлийн туршилт үр дүн: Анхны сургалтын 864 зурган өгөгдөл дээр олон төрлийн хүүхдийн өгөгдлөөр туршилт хийхэд 32% болж буурсан.

Өгөгдлийн хэмжээг нэмэгдүүлсэн туршилт:

Олон хүүхдийн зургаар сургалтын өгөгдлөө баяжуулсны дараа тестийн багц дээр 68% болж сайжирсан. Өгөгдлийн хэмжээ нэмэгдэх тусам гүйцэтгэл нь 92% болж сайжирсан. Энэ нь олон ялгаатай хүүхдийн өгөгдлөөр загварыг сургах нь загварын гүйцэтгэлийг сайжруулж байгааг харуулж байна. Мөн өгөгдлийн хэмжээг нэмэгдүүлэхэд загварын нарийвчлал сайжрав.

Хүүхэд мөрдөх алгоритмын хувьд ВоТ-SORT бодит цагт хүүхдийг тасралтгүй мөрдөж гүйцэтгэлийн хувьд хамгийн үр дүнтэй буюу МОТА(0.813), МОТР(0.818), F1(0.915) алгоритм байв.

Аюултай бүс илрүүлэлтийн хувьд шарах шүүгээ, богино долгионы зуух, залгуур, плитка гэсэн 4 төрлийн объектоос бүрдсэн 2940 зурган өгөгдлийг

ашиглаж YoloV8 дээр fine-tune хийж сургасан. Плитка хувьд 61% нарийвчлалтай таньж байсан нь өөрийн онцлог шинж нь гадаргуутай ижилхэн байдаг учраас танилт муу байсан. Үүнээс ганцхан объектоор нь танилт хийх нь уян хатан байдлыг бууруулж байсан учраас гар аргаар аюултай бүсийг нэмж тодорхойлж өгөх нь загварын нарийвчлалыг сайжруулж байв.

Мэдэгдлийг зөвхөн нэг аргаар буюу мессежээр илгээх уян хатан байдлыг бууруулж байсан ба нэмэлтээр email хаяг болон pushover ашиглан илгээх нь мэдэгдлийг анзаарахгүй өнгөрөх эрсдэлийг бууруулж, найдвартай байдлыг нэмэгдүүлсэн.

Судалгааны үр дүнгээс харахад YoloV8 загвар нь өгөгдлийн хэмжээ болон төрлөөс хамааран үр дүнтэй ажиллах чадвартай нь батлагдлаа. ВоТ-SORT алгоритм нь бодит цагийн мөрдөлтийг тогтвортой гүйцэтгэж чадсан бөгөөд аюултай бүсийг илрүүлэх системтэй хослуулснаар хүүхдийн аюулгүй байдлыг хангахад үр дүнтэй шийдэл болохыг харуулсан.

Бид энэхүү судалгааны ажлаараа бага насны хүүхдийн ахуйн орчны аюулгүй байдлыг хангах, осол гэмтлээс урьдчилан сэргийлэх зорилгоор ухаалаг хяналтын системийг санал болголоо. Энэхүү систем нь хүүхдийг илрүүлж, аюултай бүсэд нэвтэрсэн тохиолдолд бодит цагийн анхааруулга илгээх замаар эцэг эхийн хяналтыг дэмжиж, ахуйн орчны аюулгүй байдлыг сайжруулахад хувь нэмэр оруулах технологийн шийдэл юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Н. Б., “Хүүхэд ахуйн осолд өртөж гэмтэх нь нэмэгдэж байна,” 2025. [Холбогдсон]. Available: <https://news.mn/r/2775344/>. [Нэвтэрсэн 09 01 2025].
- [2] P. H. L. Yujia Zhang, “A SMART CHILD SAFETY SYSTEM FOR ENHANCED POOL SUPERVISION USING COMPUTER VISION AND MOBILE APP INTEGRATION”.
- [3] C. [Холбогдсон]. Available: https://us.getcubo.com/?srsltid=AfmBOor701_5HX5ZMykpBLE7nPuGbdWu3iOySQQQJ2JjsJH5r10ODTC.
- [4] G. Boesch, “Detectron2: A Rundown of Meta’s Computer Vision Framework,” 11 2 2024. [Холбогдсон]. Available: <https://viso.ai/deep-learning/detectron2/>.
- [5] Peter Robicheaux, James Gallagher, Joseph Nelson, Isaac Robinson, “RF-DETR: A SOTA Real-Time Object Detection Model,” 20 03 2025. [Холбогдсон]. Available: <https://blog.roboflow.com/rf-detr/>.
- [6] T. M., “YOLO Object Detection: An Introduction,” 19 6 2025. [Холбогдсон]. Available: <https://blog.roboflow.com/yolo-object-detection/>.
- [7] “What is YOLOV8? A Step-By-Step Guide,” 2024. [Холбогдсон]. Available: <https://www.folio3.ai/blog/what-is-yolov8-architecture/>.
- [8] Ranjan Sapkota, Marco Flores-Calero, Rizwan Qureshi, Chetan Badgujar, “YOLO advances to its genesis: a decadal and comprehensive,” p. 19, 2025.

- [9] A. Kouidri, “Mastering Deep Sort: The Future of Object Tracking Explained,” 11 10 2023. [Холбогдсон]. Available: <https://www.ikomia.ai/blog/deep-sort-object-tracking-guide>.
- [10] “Multi-Object Tracking with DeepSORT,” [Холбогдсон]. Available: <https://www.mathworks.com/help/vision/ug/multi-object-tracking-with-deepsort.html>.
- [11] KEECHIN, “Implementing Object Tracking for Computer Vision,” 21 7 2022. [Холбогдсон]. Available: <https://datature.io/blog/implementing-object-tracking-for-computer-vision>.
- [12] “An Introduction to BYTETrack: Multi-Object Tracking by Associating Every Detection Box,” [Холбогдсон]. Available: <https://datature.io/blog/introduction-to-bytetrack-multi-object-tracking-by-associating-every-detection-box>.
- [13] “Pushover,” [Холбогдсон]. Available: <https://pushover.net/>.
- [14] “MOTChallenge: A Benchmark for Single-Camera Multiple Target Tracking,” 2020. [Холбогдсон]. Available: <https://link.springer.com/article/10.1007/s11263-020-01393-0>.
- [15] A. V. “Enhancing Child Safety with Computer Vision,” 2023.
- [16] S. T. “Child Monitoring and Data Analysis via Computer Vision,” 2024.
- [17] K.-L. L. “An Image-Based Fall Detection System for the Elderly,” 2018.

ХИЙМЭЛ ОЮУН УХААНД СУУРИЛСАН ЖОЛООЧИЙН АЮУЛГҮЙ БАЙДЛЫГ ХЯНАХ СИСТЕМИЙН СУДАЛГАА БА ХӨГЖҮҮЛЭЛТ

Бөхбатын АМАРТҮВШИН¹, Нямын ГАНТӨМӨР², Бямбадоржийн ЗОЛЗАЯА³

^{1,2,3}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Мэдээллийн технологийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: B231910004@must.edu.mn¹

Хураангуй - Энэхүү судалгааны ажил нь Хиймэл оюун ухаанд (AI) суурилсан жолоочийн аюулгүй байдлын ухаалаг хяналтын системийг хэрэгжүүлэхэд чиглэсэн. Судалгааны гол зорилго нь жолоочийн анхаарал сарнилт, нойрмоглолт, стресс, болон аюултай үйлдлүүдийг бодит цаг хугацаанд илрүүлж, зам тээврийн ослын эрсдэлийг бууруулах боломжийг бүрдүүлэхэд оршино. Систем нь гурван үндсэн модулиас бүрдэх бөгөөд үүнд: (1) нойрмоглолт болон анхаарал сарнилт илрүүлэх, (2) хориотой үйлдэл таних, (3) стрессийн түвшин тодорхойлох модуль багтана. Судалгаанд MediaPipe FaceMesh болон компьютерын хараанд суурилсан гүн сургалтын архитектурууд дээр суурилсан загваруудыг ашиглаж, жолоочийн нүүрний 136 ба 468 цэгийн мэдээлэлд үндэслэн, нүд, ам, толгойн хөдөлгөөнүүдэд дүн шинжилгээ хийдэг. Хориотой үйлдэл таних модуль нь Vision Transformer (ViT) болон Data-Efficient Image Transformer (DEiT) архитектурууд дээр суурилсан загваруудыг ашиглан “утсаар ярих”, “эвшээх”, “юм уух” зэрэг үйлдлүүдийг 99.2%-ийн нарийвчлалтайгаар ангилсан. Харин стрессийн түвшин тодорхойлох модуль нь Support Vector Machine (SVM) болон Convolutional Neural Network (CNN) суурь загваруудыг ашиглаж, сэтгэлзүйн төлөвийг хоёр ангиллаар (стрессгүй, стрессгэй) тодорхойлсон бөгөөд хамгийн өндөр нь 95%-ийн нарийвчлал үзүүлсэн. Үр дүнд нь боловсруулсан систем нь жолоочийн зан төлөв, физиологийн болон сэтгэлзүйн өөрчлөлтийг бодит цагт хянаж, ослын эрсдэлийг урьдчилан тодорхойлох, анхааруулах боломжийг бүрдүүлсэн. Энэ нь жолоочийн аюулгүй байдлыг сайжруулах, хүний хүчин зүйлээс үүдэлтэй ослын тоог бууруулах чиглэлд тодорхой хэмжээний хувь нэмэр оруулах боломжтой юм.

Түлхүүр үг: SVM, kernel trick, ViT, DeiT, Open-CV, Facial Landmark, CNN, FaceMesh, T-SNE

I. УДИРТГАЛ

Сүүлийн жилүүдэд монгол улсад зам тээврийн ослын тоо болон түүнтэй холбоотой хүний амь нас, эдийн засгийн хохирол нэмэгдэж байгаа нь жолоочийн аюулгүй байдлыг хангах асуудал тулгамдаж байгааг илтгэж байна. Ослын дийлэнх нь жолоочийн анхаарал сарнилт, ядралт, стресс зэрэг сэтгэлзүйн болон бие физиологийн хүчин зүйлсээс шалтгаалдаг. Тиймээс эдгээр хүчин зүйлсийг бодит цагийн орчинд илрүүлж, урьдчилан анхааруулах системийг боловсруулах нь тээврийн аюулгүй байдлыг хангах чухал ач холбогдолтой.

Олон улсад хиймэл оюун ухаан болон компьютерын хараанд суурилсан жолоочийн хяналтын системүүдийн талаар судалгаанууд хийгдсэн байдаг бөгөөд жишээлбэл, нүүрний хувирал, нүдний хөдөлгөөн, толгойн чиглэл, зүрхний цохилт зэрэг биометрийн үзүүлэлтүүдийг ашиглан анхаарал болон ядралтыг илрүүлэх аргуудыг боловсруулсан байдаг. Гэсэн хэдий ч эдгээр системүүдийн гүйцэтгэл нь хэрэглэсэн өгөгдлийн чанар, орчны нөхцөл, мөн загварын архитектураас хамааран ялгаатай байдаг.

Иймээс энэхүү судалгааны ажлын зорилго нь Зүйлсийн интернэт (IoT) болон компьютерын харааны технологид суурилсан жолоочийн аюулгүй байдлын хяналтын системийг боловсруулж, жолоочийн стресс, анхаарал сарнилт, ядралт,

нойрмоглолт болон аюултай үйлдлийг бодит цагийн орчинд илрүүлэх, хянах, статистик шинжилгээ хийх боломжийг бүрдүүлэхэд оршино.

Судалгаанд гүн сургалтын (Deep Learning) архитектурууд болон нүүрний 136 ба 468 цэгийн анализыг ашиглан жолоочийн стресс, нойрмоглолт, анхаарал сарнилт, аюултай үйлдлийг бодит цагийн орчинд илрүүлэх гурван үндсэн модулиар системийг загварчилсан. Үүнд нойрмоглолт ба анхаарал сарнилт илрүүлэх модуль нь нүд, ам, толгойн хөдөлгөөнд дүн шинжилгээ хийж бодит цагт анхааруулга өгөх боломжийг бүрдүүлсэн бол, хориотой үйлдэл таних модуль нь Vision Transformer (ViT) болон Data-efficient Image Transformer (DeiT)-д суурилан утсаар ярих, эвшээх, юм уух зэрэг жолоодлогын үед хориглосон үйлдлүүдийг 99.2%-ийн нарийвчлалтай илрүүлэх чадвартай болсон. Харин стресс илрүүлэх модуль нь нүүрний сэтгэл хөдлөлийн илэрхийллийг SVM болон CNN загваруудаар боловсруулан 93%-ийн нарийвчлалтайгаар стрессийн түвшин тодорхойлох боломжийг олгосон.

II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Энэхүү систем нь жолоочийн үйлдэл болон сэтгэлзүйн өөрчлөлтийг бодит цагт хянаж, ослын

эрсдэлийг урьдчилан тодорхойлох, урьдчилан сэргийлэх шийдэл боловсруулахад чухал ач холбогдолтой юм.

Зам тээврийн осол эндэгдэл гарах үндсэн шалтгаан нь ихэвчлэн хувь хүний буруутай үйлдлээс үүдэлтэй байдаг. Үүнээс урьдчилан сэргийлэх зорилгоор сүүлийн жилүүдэд олон төрлийн судалгааны ажлууд эрчимтэй хийгдэж байна. Тухайлбал, [1]-т IoT-д суурилсан U-Net архитектур ашиглан нүүрний гол цэгүүдийг сегментчилж нойрмоглохыг илрүүлэх аргыг танилцуулсан.

[2]-р судалгаанд MobileNet, CNN, VGG16 зэрэг архитектуруудыг ашиглан жолоочийн ядаргаа, нойрмоглохыг нүүрний хувирал, нүд, амны хөдөлгөөнөөр тодорхойлсон. Үүнтэй төстэйгөөр, [3]-т жолоочийн нойрмоглохыг илрүүлэх гүн сургалтын олон төрлийн арга (CNN, LSTM, RNN) ашиглан жолоодлогын туслах систем (ADAS)-ийн хүрээнд үнэлсэн бөгөөд олон төрлийн өгөгдлийн эх үүсвэрийг (зураг, видео, био сенсор) хослуулсан нь үр дүнг 5–10%-аар сайжруулсан.

Мөн [4]-д системчилсэн тойм судалгаа хийж, гүн сургалтад суурилсан нойрмоглолт илрүүлэх загваруудын гүйцэтгэлийн давуу болон сул талуудыг харьцуулан үзсэн.

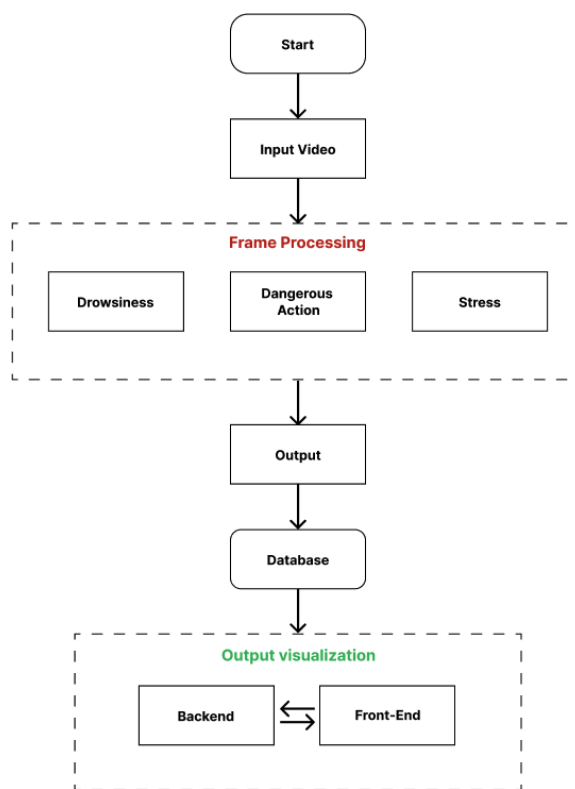
[5]-д нүүрний хувирал болон зүрхний цохилтыг нэгтгэсэн Dual-Modal Drowsiness Detection аргачлал санал болгож, 90%-иас дээш нарийвчлалтай үр дүн үзүүлсэн нь олон талын өгөгдөл ашиглахын давуу талыг харуулсан. Харин [6]-д жолоочийн ядралт, анхаарал сарнилт зэргийг тээврийн хэрэгслийн мэдрэгч болон дүрс боловсруулалтын аргаар тодорхойлж, машин сургалтын загваруудын үр дүнг харьцуулсан. [7]-д жолоочийн аюултай үйлдлүүдийг тодорхойлох гүн сургалтын аргуудыг нарийвчлан судалсан байна.

Бидний судалгаанд дээрх ажлуудын оновчтой талыг нэгтгэн, жолоочийн аюулгүй байдлын хяналтын системийг боловсруулахаар зорьсон. Энэхүү систем нь стрессийн түвшин, нойрмоглолт, аюултай үйлдлийг бодит цагийн орчинд илрүүлж статистик үзүүлэлт болгон гаргадаг. Ингэснээр систем нь зөвхөн нойрмоглолт бус стресс ба анхаарал сарнилт зэрэг олон хэмжигдэхүүнийг хянаж, зам тээврийн ослоос урьдчилан сэргийлэх боломжтойг харуулж байна.

III. АШИГЛАСАН АРГА

Энэхүү жолоочийн аюулгүй байдлыг хянах систем нь дараах 3 модулиас бүрдэнэ.

1. Нойрмоглолт болон анхаарал сарнилт илрүүлэх модуль
2. Хориотой үйлдэл илрүүлэх модуль
3. Стрессийн түвшин таних модуль



1 – р зураг. Системийн үйл ажиллагааны диаграмм

1-р зурагт системийн үйл ажиллагааны диаграммыг харуулж байгаа бөгөөд бидний тодорхойлсон 3 модуль нь оролтоос эхлэн зэрэгцээ байдлаар ажиллах юм.

Монгол улсын замын хөдөлгөөний дүрэм [8]-д зааснаар, тодруулбал 3.7-ийн Жолоочийн үүрэгт тухайн жолоочийн зүгээс тээврийн хэрэгсэл жолоодож байх үедээ гаргах дараах үйлдлүүдийг хориглосон байдаг. Үүнд:

- а/ тухайн ангиллын тээврийн хэрэгслийг жолоодох эрхгүй (жолоодлогын дадлага хийхээс бусад тохиолдолд) , эсхүл согтууруулах ундаа, мансууруулах эм, сэтгэцэд нөлөөт бодис хэрэглэсэн, мөн хөдөлгөөний аюулгүй байдлыг хангаж чадахааргүй өвчтэй буюу ядарсан үедээ тээврийн хэрэгсэл жолоодох;
- г/ эрх бүхий байгууллагаас тогтоосон жолоочийн хөдөлмөр, амралтын горимыг зөрчиж тээврийн хэрэгсэл жолоодох;
- д/ тээврийн хэрэгслийн хөдөлгөөний үед гар утас болон түүнтэй ижил төстэй төхөөрөмж, хэрэгслийг гарын оролцоотойгоор ашиглах;

3.1 Нойрмоглолт болон анхаарал сарнилт илрүүлэх модуль

Ихэнх зам тээврийн осол, эндэгдлийн гол шалтгаан нь жолоочийн анхаарал сарнилт, удаан хугацаанд амралтгүй жолоо барьснаас үүдэлтэй ядаргаа, нойрмоглолттой шууд холбоотой байдаг. Иймээс энэхүү судалгаанд боловсруулсан модуль нь жолоочийн нүүрний хувирал, нүд, амны хөдөлгөөн, мөн толгойн чиглэлд тулгуурлан нойрмоглолт болон анхаарал сарнилтыг бодит цагийн орчинд илрүүлэх зорилготой юм.

Жолоочийн нүүрний хөдөлгөөнийг тодорхойлохын тулд MediaPipe Face Mesh санг ашиглаж, хүний нүүрний 468 цэгийн координатыг илрүүлэн тухайн цэгүүдийн байрлалын өөрчлөлтөд дүн шинжилгээ хийсэн.



2 – р зураг. Толгойн чиглэлийн дүрслэл

2-р зурагт толгойн чиглэл буюу Head Pose Estimation-ийг тодорхойлохдоо хамар, эрүү, нүд болон амны ирмэгийн цэгүүдийг ашиглан 2D зураглалаас 3D нүүрний загварын вектор дүрслэл хэрэглэсэн аргыг харуулж байна. Үүнд Perspective-n-Point (PnP) алгоритм ашиглагдсан бөгөөд энэ нь камерын координатын системд үндэслэн дэлхийн координатын системд орших нүүрний байрлал, өнцөг, чиглэлийг тодорхойлох боломжийг олгодог.

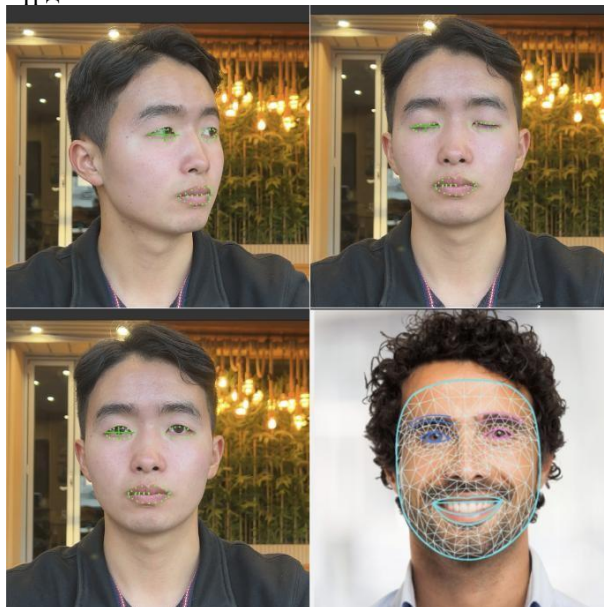
1. Perspective projection model:

$$sp_c = K [R | T] p_w$$

Энд $p_w = [x \ y \ z \ 1]^T$ нь homogeneous world point, $p_w = [u \ v \ 1]^T$ нь homogeneous Image point, K нь камерын дотоод параметрийн матриц, R болон T нь эргэлтийн болон шилжилтийн матриц юм.

Энэхүү аргачлалаар толгойн хөдөлгөөн, чиглэл (жишээлбэл, замаас баруун, зүүн тийш удаан харсан эсэх) тодорхойлогдож, жолоочийн анхаарал

сарнисан нөхцөлд систем анхааруулга өгөх боломж бүрдэнэ.



3 – р зураг. Нүд, амны цэгэн дүрслэл

3-р зурагт нойрмог болон ядралттай байдлыг илрүүлэхийн тулд нүд болон амны хүрээний цэгүүдийг дүрслэн харуулсан байна. Дээрх цэгүүд дээр тооцоолол хийхийн тулд дараах үндсэн параметруудийг ашиглав:

- **EAR (Eye Aspect Ratio):** Нүдний өндрийн болон өргөний харьцааг тооцоолон нүдний анилт, нээлттэй байдлыг илрүүлдэг. EAR-ийн утга тодорхой босгоос доош буурахад нүд аньсан гэж үзнэ.
- **PERCLOS (Percentage of Eye Closure):** Тодорхой хугацаанд нүд хаалттай байсан хувь хэмжээг тооцох үзүүлэлт бөгөөд жолоочийн нойрмоглолтын түвшнийг үнэлэхэд өргөн хэрэглэгддэг.
- **PERCLOS** нь дараах байдлаар тооцогдоно:

$$PERCLOS = \frac{N_{closed}}{N_{total}} \times 100\%$$

- **Yawning Detection:** Амны хүрээний цэгүүдийн хоорондын зай, харьцаанд тулгуурлан эвшээх үйлдлийг илрүүлнэ.

Эдгээр үзүүлэлтүүдийг ашиглан систем нь нойрмоглох, анхаарал сарних зэрэг үйлдлүүдийг илрүүлэх боломжтой.

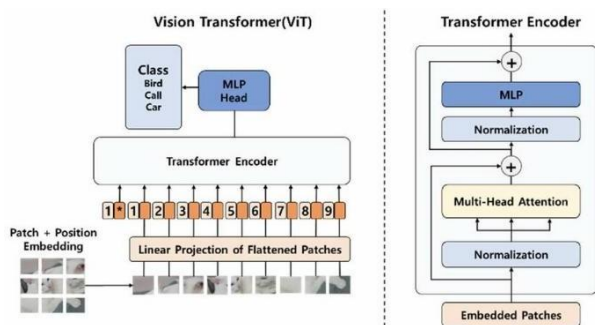
3.2 Хориотой үйлдэл таних модуль

Хориотой үйлдэл таних модулийг хэрэгжүүлэхдээ бид 2 төрлийн суурь загварыг ашигласан.

3.2.1 ViT based google/vit-tiny-patch16-224

ViT (Vision transformer) нь Transformer encoder архитектурт (BERT - тэй төстэй) суурилсан загвар бөгөөд ImageNet-21k 1000 ангиллын 1 сая жишээтэй өгөгдлийн багцаар урьдчилан сургагдсан ба дараа

нь ImageNet-1k өгөгдлийн багцаар дахин сургагдсан.



4 – p зураг. Vision transformer архитектур

Зураг нь тухайн загварт оролт болж ороход 4 - p зурагт харуулсантай ижил тогтмол хэмжээтэй хэсгүүдэд (patches) хуваагдаж ордог бөгөөд тус бүрийн хэмжээ нь 16x16 харьцаатай пиксель байна. Эдгээр хэсгүүдийг шугаман байдлаар хувиргадаг. Мөн дарааллын эхэнд [CLS] token нэмэгддэг ба энэ нь ангиллын үүрэг гүйцэтгэхэд ашиглагддаг. Үүн дээр нэмээд absolute position embedding хийгддэг. Ингэснээр загвар нь хэсгүүдийн дарааллын байрлалыг ойлгож чаддаг.

Хэрвээ бидэнд шошготой зурагийн өгөгдлийн багц байгаа бол урьдчилсан сургасан энкодерийн дээр нэг шугамтай давхарга нэмж энгийн ангилагчийг сургах боломжтой юм.

3.2.2 DeiT facebook/deit-tiny-patch16-224

DeiT архитектуртай загвар нь илүү үр ашигтайгаар сургагдсан ViT юм. Ерөнхий суурь бүтэц нь ижил боловч загварын сургалтын арга техник нь харьцангуй өөр юм. Учир нь энэхүү загвар шууд ImageNet-1k өгөгдлийн багц дээр урьдчилан сургагдсан юм. Мөн илүү бага хэмжээтэй (patches) хувилбар, encoder давхаргын тоог бууруулсан байдал нь тухайн архитектурт суурилсан загвар цөөн тооны зураг дээр суралцах боломжийг олгодог байна.

Манай судалгааны хүрээнд тус тус загварын хамгийн жижиг хувилбаруудыг суурь загвар болгон авч ашигласан.

- DeiT facebook/deit-tiny-patch16-224 5 сая параметр
- ViT based google/vit-tiny-patch16-224 5.8 сая параметр

Жолоочийн зүгээс тээврийн хэрэгсэл жолоодож байх үедээ гаргаж болох хориотой үйлдэл таних модуль нь дээрх заалтуудаас 3.7.а ядралтай байгааг илэрхийлэх, 3.7.д гар утас ашиглах утсаар ярихыг илрүүлэхийг зорьсон.

Дараах хоёр загвар нь тус бүр 1000 ангилалтай 1 сая жишээтэй Image-Net21k өгөгдлийн багц дээр сурсан бөгөөд объект таних чадвартай.

Манай судалгааны хүрээнд дараах загваруудыг объект таних байдлаас нь үйлдэл таних боломжтой болгон сайжруулан сургасан бөгөөд сургасны дараагаар загвар нь дараах үйлдлүүдийг ангилах чадамжтай болох юм:

- Утсаар ярих үйлдэл
- Эвшээх үйлдэл
- Хуванцар савнаас юм уух үйлдэл
- Бусад тохиолдолд хэвийн байх үйлдэл

3.2.3 Сургалтын өгөгдлийн багц

Суурь загваруудын гол онцлог нь тухайн зураг болон фрэймээс зөвхөн объектыг таньдаг байсан бөгөөд энэ нь судалгааны явцад тодорхой хэмжээний сорилт болж байсан бөгөөд бидний зорилтот нөхцөл байдалд буюу жолооны ард байгаа жолооч нь тухайн хориотой үйлдлүүдийг хийж байгаа зурган өгөгдөл байсан юм.

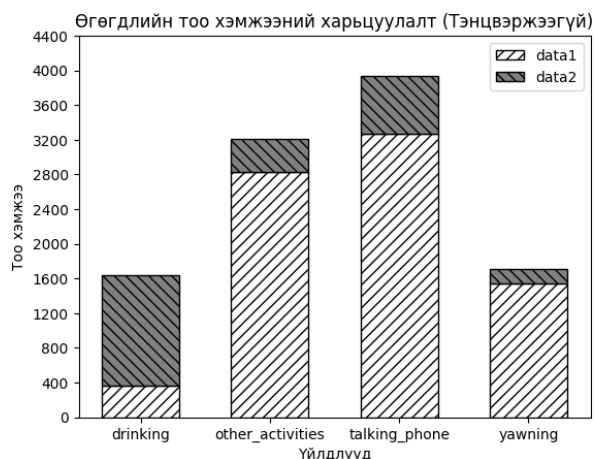
Тухайн нөхцөлд болон зорилтот ангилалд багтсан өгөгдлийн багцыг тодорхой хэмжээгээр цахим эх сурвалжуудаас цуглуулсан боловч дараачийн асуудал болох өгөгдлийн багцын ангиллын тэнцвэртэй бус байдал тулгарсан.

Учир нь ViT болон DeiT архитектуртай загварууд нь өгөгдлөөр өлсгөлөн (data hungry) байдаг бөгөөд, дан ганц цахим эх сурвалжаас цуглуулсан өгөгдлийн багцаар загварыг сайжруулахад хангалтгүй гэж үзсэн бөгөөд өгөгдлийн багцын ангиллын тоо хэмжээ болон тэнцвэргүй байдлыг шийдэхийн тулд, бид өөрсдөө жолоо барьж буй нийт 51 мин 48 секунд хугацааны бичлэг хийсэн. Нийт 3108 секунд урттай бөгөөд, 186480 фрэйм бөгөөд, нэг ижил фрэймийг олон давхцуулж ашиглахаас сэргийлэн 1 секунд бүрээс 6 фрэймийг авсан ашигласан.

1-р хүснэгт. ТЭНЦВЭРГҮЙ ӨГӨГДЛИЙН БАГЦЫН ТОО ХЭМЖЭЭ

Тэнцвэргүй өгөгдлийн багцын тоо хэмжээ			
Ангилал	Гаргаж авсан	Цуглуулсан	Нийт
Drinking	1272	363	1635
Other_activities	378	2826	3204
Talking_phone	667	3264	3931
Yawning	172	1543	1715

Нийт 18648 фрэйм гаргаж авснаас нийт 2489 зураг зорилгод 4 ангилалд 1 - p хүснэгтэд харуулсан байдлаар хувиарлагдсан.



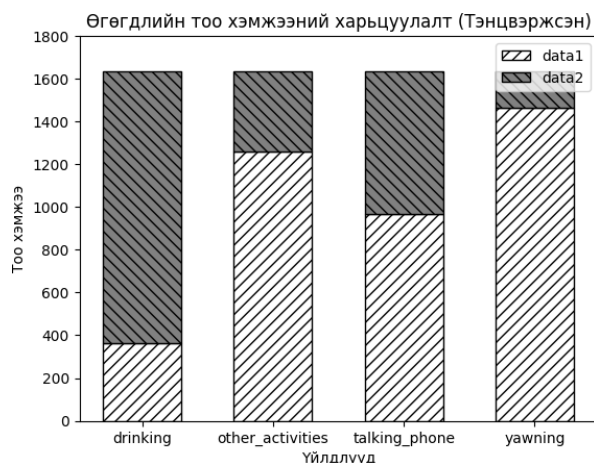
5 – р зураг. Тэнцвэргүй өгөгдлийн харьцуулалт

5- р зурагт data1 нь цахим эх сурвалжаас цуглуулсан ба data2 гаргаж авсан зургийн тоо хэмжээг ангилал бүр дээр тэнцвэржээгүй байх үед харуулж байна.

2- Р ХҮСНЭГТ. ТЭНЦВЭРТЭЙ ӨГӨГДЛИЙН БАГЦЫН ТОО ХЭМЖЭЭ

Тэнцвэртэй өгөгдлийн багцын тоо хэмжээ			
Ангилал	Гаргаж авсан	Цуглуулсан	Нийт
Drinking	1272	363	1635
Other_activities	378	1257	1635
Talking_phone	667	968	1635
Yawning	172	1463	1635

2- р хүснэгтэд 4 ангилал дахь тэнцвэржсэн өгөгдлийн багцын тоо хэмжээг харуулж байгаа бөгөөд,



6 – р зураг. Тэнцвэржсэн өгөгдлийн харьцуулалт

6 - р зурагт тэнцвэржсэн өгөгдлийн багцын ангилал тус бүр дээрх цуглуулсан болон гаргаж авсан зургийн эзлэх тоо хэмжээ болон харьцааг харуулж байна.



7 – р зураг. "drinking" ангиллын жишээ зураг

7 – р зурагт "drinking" ангилал дахь сургалтын жишээ зургийг харуулж байна.

3.2.4 Фрэйм боловсруулалт

Бидний цуглуулсан болон гаргаж авсан зураг нь өөр өөр хэмжээтэй болон өнгөт байсан бөгөөд нийт өгөгдлийн багцыг бэлдэхдээ дараах байдлаар боловсруулалт хийсэн:

1. Зургийн хэмжээг 224x224 рүү хөрвүүлэх
2. Өнгөт зургийг саарал өнгө рүү хөрвүүлэх
3. Саарал зургийг RGB болгон 3 өнгөний сувагтай болгох

3.3 Стрессийн түвшин тогтоох модуль

Бидний судалгааны гол зорилго нь жолоочийн хянах систем бөгөөд энэхүү модуль нь тухайн жолоочийн стрессдэж байгаа эсвэл хэвийн байгаа эсэхийг тодорхойлох юм. Ингэхдээ бид хүний сэтгэл хөдлөлийг илэрхийлсэн зурган өгөгдөл ашигласан.

3.3.1 Өгөгдлийн багц

3- Р ХҮСНЭГТ. ӨГӨГДЛИЙН БАГЦЫН ТОО ХЭМЖЭЭ

Ангилал	Тоо хэмжээ
angry	9906
happy	17978
neutral	12396
sad	12154
surprised	8004

3-р хүснэгтэд бидний цахим эх сурвалжаас цуглуулсан өгөгдлийн багцын ангилал болон харгалзах тоо хэмжээг харуулж байна. 8-р зурагт ангилал бүрийн жишээ зургийг харуулав.

Эндээс ангилал тус бүрээс нийт 8004 зураг авч тэнцвэржүүлсэн ба 8:1:1 харьцаагаар хуваан ашигласан.



8 – р зураг. Сургалтын өгөгдлийн багцын ангилал тус бүрийн жишээ

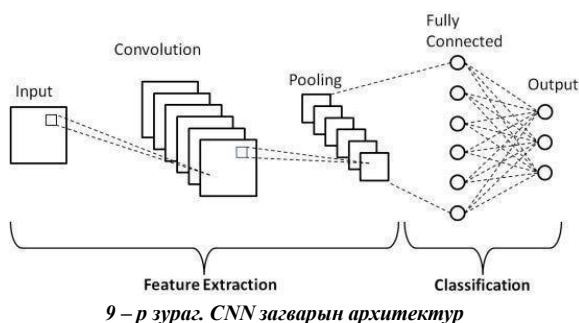
3.3.2 Жижиг загвар - SVM загвар

Хүний нүүрний нийт 136 цэгийг урьдчилан сургагдсан гүн сургалтын загвар ашиглан илрүүлж, тухайн цэгүүдийн координатуудыг тоон хэлбэртэй онцлог шинжүүд болгон хувиргасан. Гарсан онцлогуудыг ашиглан SVM (Support Vector Machine) ангилагчийг сургасан.

Энэ аргын давуу тал нь шууд том нейрон сүлжээ сургалгүйгээр урьдчилан сургагдсан загварын гаргасан онцлог шинжүүдийг ашиглан илүү хөнгөн, тооцооллын хувьд үр ашигтай загвар байгуулах боломжийг олгож буй явдал юм.

3.3.3 Дунд хэмжээний загвар

Бид мөн CNN (Convolutional neural network) загварыг авч үзсэн. Ингэхдээ тухайн зураг ангиллын даалгаварт тохирсон загварын давхаргын архитектурыг авч ашигласан. Тухайн загвар нь нийт 38 давхаргатай бөгөөд ойролцоогоор 2.5 сая параметртэй юм.



9 – р зураг. CNN загварын архитектур

Энэхүү загвар нь Keras санг ашиглан хэрэгжүүлсэн гүн CNN архитектур юм. Загварын Feature Extraction хэсэг нь 5 шатлалтай Convolutional Block-уудаас бүрдэх ба эдгээр нь дүрсний онцлог шинжүүдийг шат дараалан ялгаж авдаг. Classification хэсэг нь нэг Dense давхарга бүхий бүтэцтэй бөгөөд эцэст нь softmax

идэвхжүүлэлтийн функцийг ашиглан өгөгдлийг n ангиллын аль нэгэнд хамааруулдаг.

IV. ҮР ДҮН

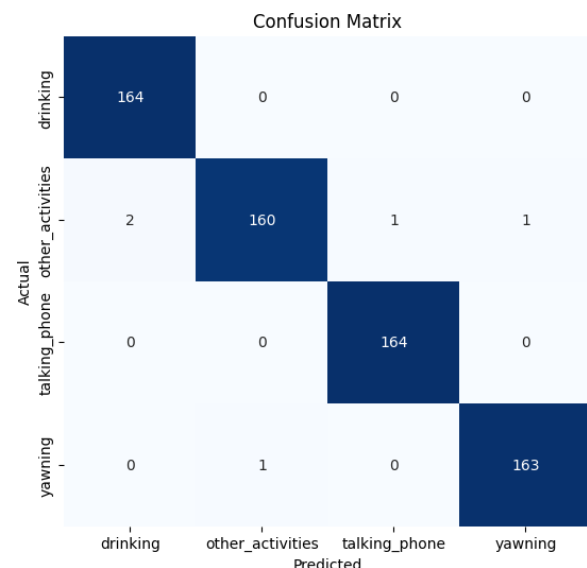
4.1 Хориотой үйлдэл таних модуль

Сургалтын өгөгдлийн багц нь нийт 4 ангилал тус бүрд 1635 жишээтэй бөгөөд, энэхүү өгөгдлийн багцыг сургалтын, баталгаажуулалтын, тестийн өгөгдөлд зориулж 8:1:1 харьцаатай хуваасан.

4 - P ХҮСНЭГТ. ЗАГВАРЫН ГИПЕРПАРАМЕТРУУД

Гиперпараметрууд	
Epochs	10
Learning_Rate	0.00005
Batch_size	64
Steps	100
Warmup_ratio	0.05

4.1.1 ViT архитектуртай загвар



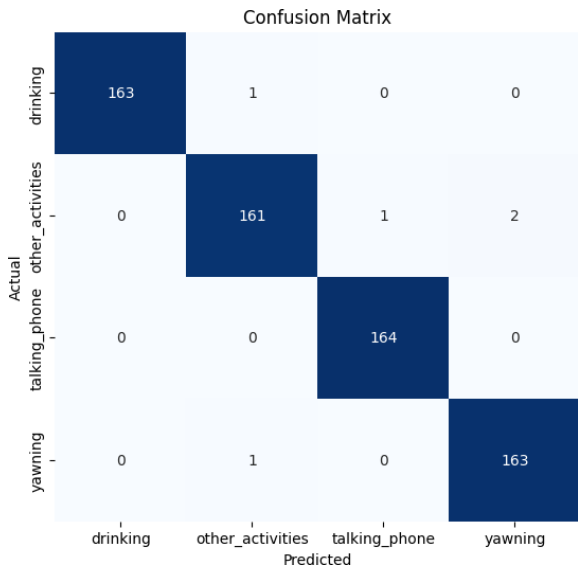
10 – р зураг. ViT архитектуртай загварын тестийн өгөгдөл дээрх гүйцэтгэл

10-р зургаас харахад загвар тестийн багц дээр хангалттай сайн үзүүлэлт үзүүлсэн байна.

5 - P ХҮСНЭГТ. ViT ЗАГВАРЫН ҮНЭЛГЭЭНИЙ ХҮСНЭГТ

Accuracy	0.9924
Precision	0.9924
Recall	0.9924
F1 score	0.9924

4.1.2 DeiT архитектуртай загвар



11 – р зураг. DeiT архитектуртай загварын тестийн өгөгдөл дээрх гүйцэтгэл

6-Р ХҮСНЭГТ. DEIT ЗАГВАРЫН ҮНЭЛГЭЭНИЙ ХҮСНЭГТ

Accuracy	0.9924
Precision	0.9924
Recall	0.9924
F1 score	0.9924

5, 6-р хүснэгтүүд болон 10, 11-р зургуудад харуулснаар ViT болон DeiT архитектуртай загвар тус бүр ижил үр дүнг үзүүлсэн байна.

Энэ нь дараах загварууд нь нэгэн ижил transformers архитектур дээр суурилсан боловч сургалтын техник, стратегиараа ялгардаг болохыг баталж байна. Манай тохиолдолд ижил өгөгдлийн багц болон 4 – р хүснэгтэд харуулсантай ижил гиперпараметруудээр загваруудыг тус тус сургасан болно.

Мөн бид баталгаажуулах үүднээс бодит байдал дээр давхар камераар загваруудыг тус тус туршихад мөн ижил хэмжээний үр дүнг үзүүлсэн ба зорилтод ангилуудыг ангилж чадаж байсан.

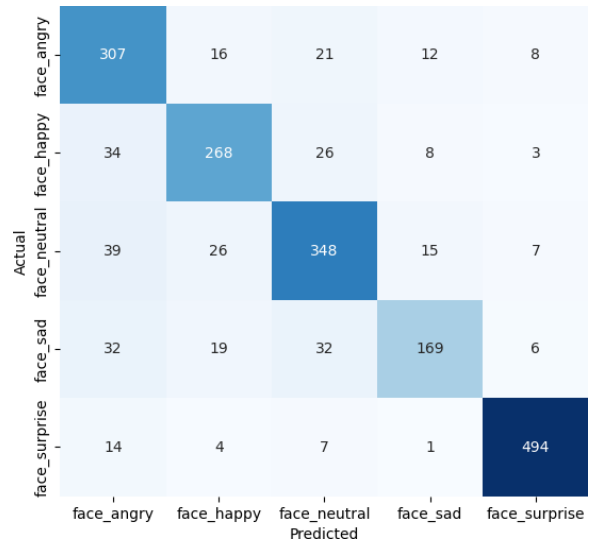
4.2 Стрессийн түвшин тогтоох модуль

4.2.1 SVM RBF kernel

7 - Р ХҮСНЭГТ

kernel	C	gamma
RBF	0.01, 0.1, 1, 10, 100	0.001, 0.01, 0.1, 1, auto, scale

Бид SVM загварын RBF кернелийн хамгийн оновчтой параметрийг олохын тулд 7-р хүснэгтэд харуулснаар параметруудийг авч үзэн grid search байдлаар хамгийн сайн үзүүлэлт үзүүлсэн загварыг тодорхойлсон. Эндээс хамгийн сайн үр дүн үзүүлсэн параметр нь {C: 100, gamma: 0.01} байсан.



12 – р зураг. SVM загварын хувилбаруудын 5 ангилал дээрх төөрөгдлийн матриц

12-р зураг дээрх тухайн загварын төөрөгдлийн матрицаас дараах зүйл ажиглагдаж байна. Тестийн багц дээр загвар нь Angry байх сэтгэл хөдлөлийг sad, neutral болон sad ангилууд дээр тодорхой хэмжээний төөрөгдлүүд үүссэн байна.

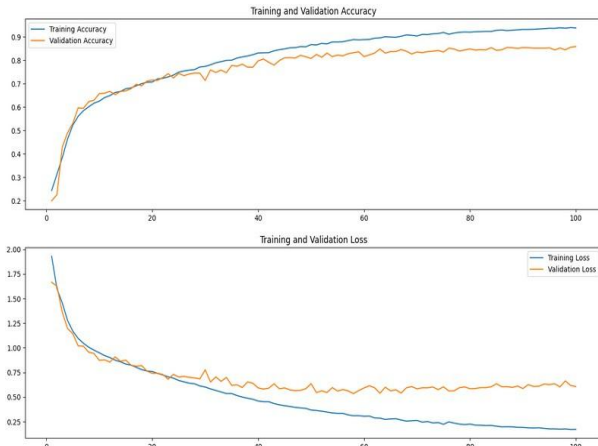
	precision	recall	f1-score	support
angry	0.72	0.84	0.78	364
happy	0.80	0.79	0.80	339
neutral	0.80	0.80	0.80	435
sad	0.82	0.66	0.73	258
surprise	0.95	0.95	0.95	520
accuracy			0.83	1916
macro avg	0.82	0.81	0.81	1916
weighted avg	0.83	0.83	0.83	1916

13 – р зураг. SVM загварын үнэлгээний хэмжээний хүснэгт

13-р зураг тестийн өгөгдлийн багц дээрх загварын гүйцэтгэлийг харуулсан ба 83% нарийвчлалыг үзүүлсэн байна.

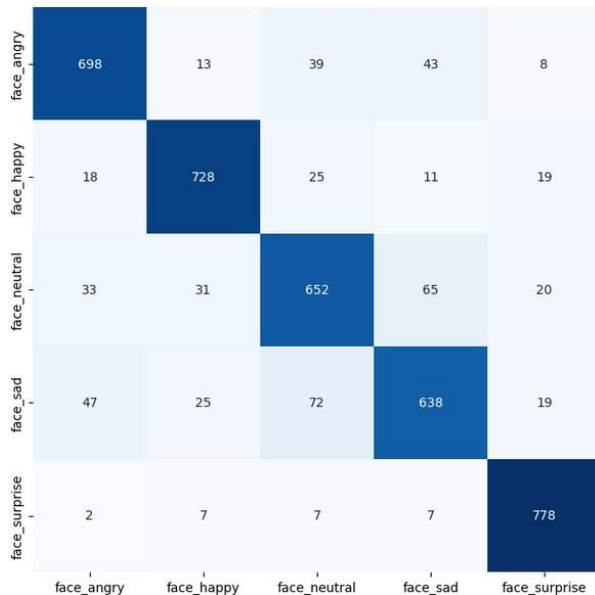
4.2.2 Дунд хэмжээний загвар

Бидний хувьд энэхүү сэтгэл хөдлөлөөр ангилах даалгаварт SVM нь хараахан жижиг байгаа гэж үзэн CNN загвар руу шилжсэн. 3.3.3-д дурдсан 38 давхаргатай загварыг нийт 100 epoch сургахад дараах үр дүнгүүд гарсан байна.



14 – р зураг. CNN загварын 5 ангилал дээрх алдагдал болон нарийвчлалын график

14-р зургаас харахад загвар сургалтын болон баталгаажуулалтын багц дээр үр дүн хоёулаа тогтвортой, ойролцоо түвшинд байна.



15 – р зураг. CNN загварын төөрөгдлийн матриц

15-р зурагт харуулснаар CNN загвар дээрх төөрөгдлийн матрицыг харуулж байгаа бөгөөд өмнөх SVM загварын үр дүнгээс харьцангуй илүү үр дүн үзүүлсэн байгаа боловч neutral болон sad ангилал дээр тодорхой хэмжээний төөрөгдөл байгаа ажиглагдаж байна.

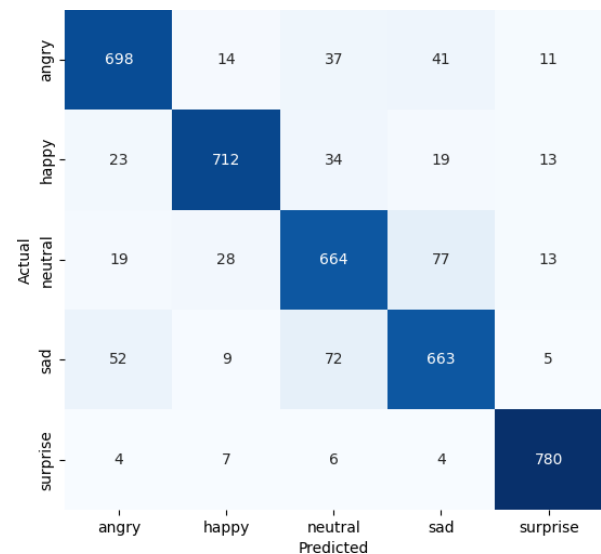
	precision	recall	f1-score	support
Angry	0.87	0.87	0.87	801
Happy	0.91	0.91	0.91	801
Neutral	0.82	0.81	0.82	801
Sad	0.84	0.80	0.82	801
Surprise	0.92	0.97	0.95	801
accuracy			0.87	4005
macro avg	0.87	0.87	0.87	4005
weighted avg	0.87	0.87	0.87	4005

16 – р зураг. CNN загварын тестийн багц дээрх нарийвчлал

Тухайн загварыг нийт 100 epoch сургасны дараа тестийн багц дээрх үнэлгээг 16-р зурагт харуулж байгаа бөгөөд 87% нарийвчлалтай байгаа SVM загвараас харьцангуй илүү үр дүнг үзүүлсэн байна.

4.2.3 Том загварыг сайжруулах арга

Бид тухайн ангилууд дээрх тодорхой хэмжээний төөрөгдлийг арилгахын тулд хориотой үйлдэл таних модуль дээрх ашигласан DeiT суурь загварыг ижил гипер параметртэй тохируулан таван сэтгэл хөдлөлийг илэрхийлж буй өгөгдлийн багц дээр нийт 10 epoch сургасан.



17 – р зураг. DeiT загварын тестийн багц дээрх төөрөгдлийн матриц

17-р зурагт DeiT загварын төөрөгдлийн матрицыг харуулж байгаа бөгөөд энд тухайн өмнөх загваруудаас илүү ангилал хоорондын төөрөгдлийг харуулсан байна. Учир нь DeiT архитектур нь 16x16 patch тай бөгөөд энэ нь 48x48 зургаас 9 токен үүсгэх ба, онцлог шинж чанаруудыг олж чадахгүй байгааг илэрхийлж байна.

	precision	recall	f1-score	support
angry	0.88	0.87	0.87	801
happy	0.92	0.89	0.91	801
neutral	0.82	0.83	0.82	801
sad	0.82	0.83	0.83	801
surprise	0.95	0.97	0.96	801
accuracy			0.88	4005
macro avg	0.88	0.88	0.88	4005
weighted avg	0.88	0.88	0.88	4005

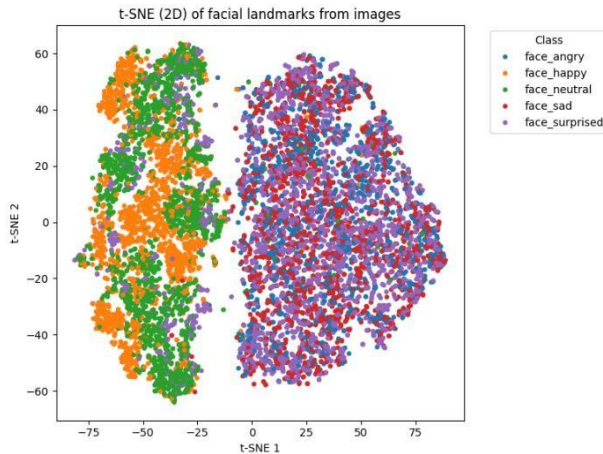
18-р зураг. DeiT загварын үнэлгээний хүснэгт

18-р зурагт харуулснаар загвар нь тестийн багц дээр 88% нарийвчлал үзүүлсэн байна.

4.2.4 Ангилал хоорондын төөрөгдлийн шинжилгээ

Өмнөх үр дүнгээс харахад зарим ангиллуудад төөрөгдөл үүсэж байв. Үүнийг тодорхой болгохын тулд зурган өгөгдлийн багцаас нүүрний 136 онцлог шинж чанарыг (facial landmarks) гарган авч, тухайн шинжүүд болон холбогдох ангиллын мэдээллийг агуулсан онцлог матриц үүсгэв.

Энэхүү матриц дээр хэмжээсийг багасгах зорилгоор Stochastic Neighbor Embedding (t-SNE) аргыг ашиглан онцлог шинжүүдийн уялдаа хамаарлыг шинжилсэн. t-SNE нь өндөр хэмжээсийн өгөгдлийн цэгүүдийн хоорондын ижил төстэй байдлыг магадлалын хэлбэрээр тооцож, үүнийг бага хэмжээст орон зайд хадгалж дүрслэдэг.



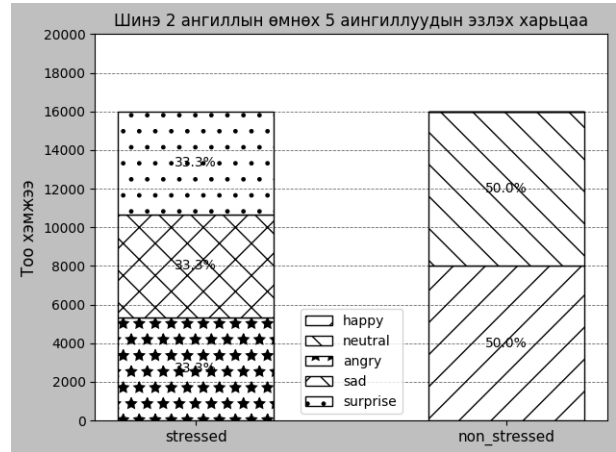
19-р зураг. Стрессийн өгөгдлийн багц дээрх T-SNE хувиргалт

19-р зурагт стрессийн өгөгдлийн багц дээр t-SNE хувиргалт хийсний дараах өгөгдлийн хоёр хэмжээст дүрслэлийг үзүүлэв. Зургийн үр дүнгээс харахад face_angry, face_sad, face_surprised ангиллууд хоорондоо ойролцоо байрлаж, face_happy болон face_neutral ангиллууд мөн ижил төстэй бүлэглэл үүсгэж байна.

Үүний үндсэн дээр ижил төстэй ангиллуудыг нэгтгэн, зорилтот ангиллын тоог хоёроор хязгаарлав. Энэ нь тухайн хүний нүүрний зургаас стрессстэй эсвэл стрессгүй эсэхийг тодорхойлох

хоёр ангиллын асуудал болгон хувиргасан гэсэн үг юм.

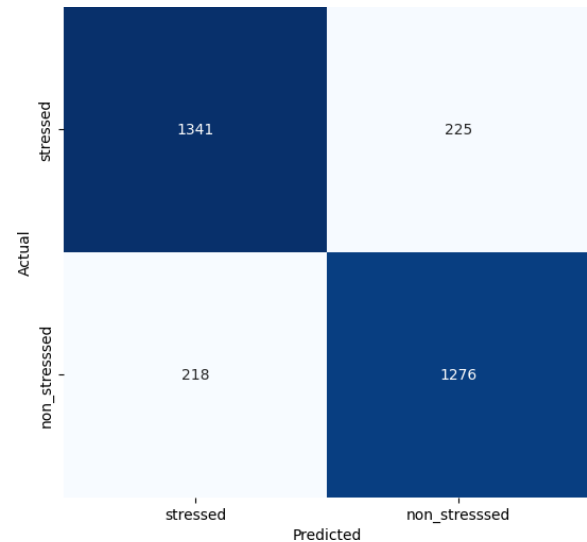
Ингэснээр 19-р зурагт үзүүлсэнчлэн, сөрөг сэтгэл хөдлөлүүдийг (angry, sad, surprised) "стрессстэй", харин эерэг сэтгэл хөдлөлүүдийг (happy, neutral) "стрессгүй" ангилалд хамааруулж, загваруудыг энэ хоёр ангилал дээр тулгуурлан дахин сургах арга зүйг бид авч үзсэн.



20-р зураг. SVM загварын 2 ангилал дээрх төөрөгдлийн матриц

20-р зурагт шинэ 2 ангилалд хамаарах өмнөх 5 ангиллууд болон тэдгээрийн харгалзах эзлэх хувийг харуулж байгаа бөгөөд мөн адил 8:1:1 харьцаатай сургалт, баталгаажуулалт, тестийн багцад хуваасан.

4.2.5 SVM загварын үр дүн

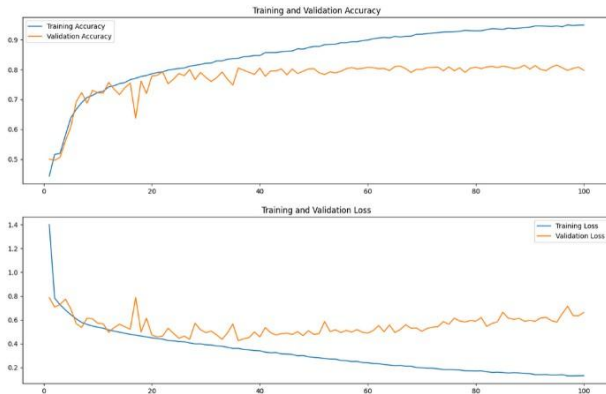


21-р зураг. SVM загварын 2 ангилал дээрх төөрөгдлийн матриц

	precision	recall	f1-score	support
stressed	0.86	0.86	0.86	1566
non_stressed	0.85	0.85	0.85	1494
accuracy			0.86	3060
macro avg	0.86	0.86	0.86	3060
weighted avg	0.86	0.86	0.86	3060

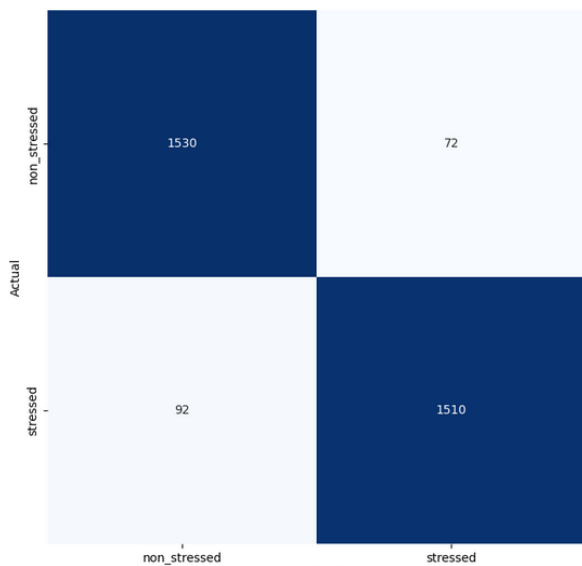
22-р зураг. SVM RBF кернел дээрх тестийн багц дээрх үнэлгээний матриц

4.2.6 CNN загварын үр дүн



23-р зураг. Дунд хэмжээний загварын 2 ангилал дээрх алдагдал болон нарийвчлалны график

23-р зурагт харуулснаар баталгаажуулалт болон сургалтын алдагдлын зөрүү бага зэрэг нэмэгдсэн байна.



24-р зураг. CNN загварын 2 ангилал дээрх төөрөгдлийн матриц

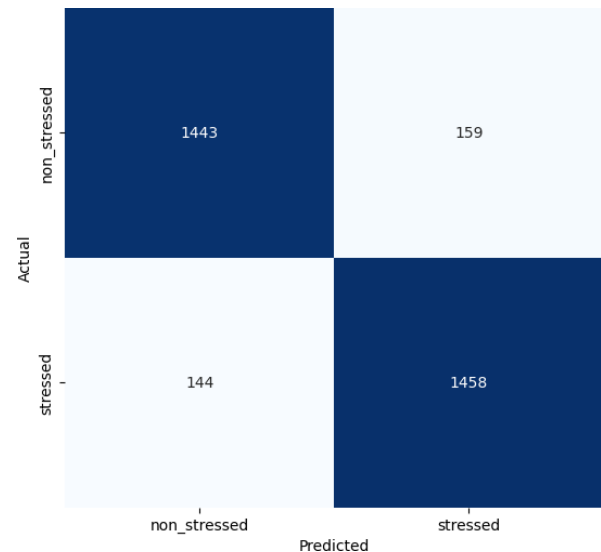
24-р зурагт харуулснаар тухайн загварын төөрөгдлийн матриц нь бусад загвартай харьцангуй илүү үр дүнг үзүүлж байна.

	precision	recall	f1-score	support
non_stressed	0.94	0.96	0.95	1602
stressed	0.95	0.94	0.95	1602
accuracy			0.95	3204
macro avg	0.95	0.95	0.95	3204
weighted avg	0.95	0.95	0.95	3204

25-р зураг. CNN загварын үнэлгээний хүснэгт

25-р зурагт харуулснаар CNN загвар нь тухайн бууруулсан хоёр ангилал дээр хамгийн өндөр нарийвчлалыг үзүүлсэн байна.

4.2.7 DeiT загварын үр дүн



26-р зураг. DeiT загварын 2 ангилал дээрх төөрөгдлийн матриц

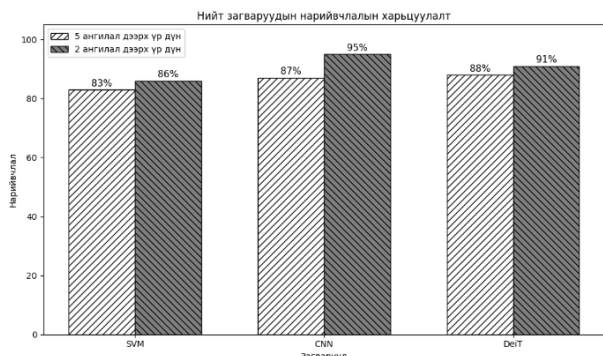
26-р зурагт харуулснаар загварын үр дүн сайжирсан боловч CNN загвараас харьцангуй муу үр дүнг үзүүлсэн байна.

	precision	recall	f1-score	support
non_stressed	0.91	0.90	0.90	1602
stressed	0.90	0.91	0.91	1602
accuracy			0.91	3204
macro avg	0.91	0.91	0.91	3204
weighted avg	0.91	0.91	0.91	3204

27-р зураг. DeiT загвар дээрх үнэлгээний хүснэгт

27-р зурагт харуулснаар загварын нарийвчлал өссөн хэдий ч төөрөгдөл хэвээр байгаа нь өгөгдлийн зургийн пикселийн хэмжээтэй холбоотой хэвээр байна.

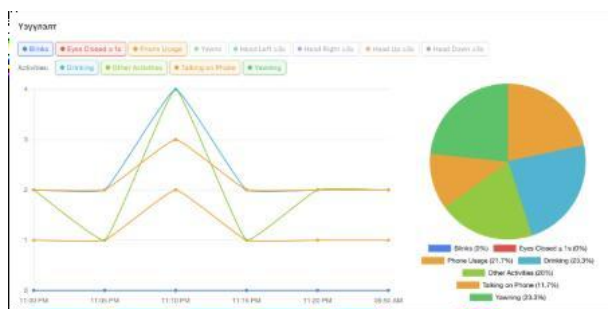
4.3 Нийт загваруудын ерөнхий харьцуулалт



28–р зураг. Нийт загваруудын нарийвчлалын харьцуулалт

28–р зурагт нийт загваруудын 5 болон 2 ангилал дээрх тестийн нарийвчлалыг харуулж байна. Бидний зорьсны дагуу тухайн жолоочийн стрессийг таних нь чухал бөгөөд дараах графикаас хамгийн өндөр нарийвчлал үзүүлсэн загвар CNN загварыг бид системд ашигласан.

4.4 Жолоочийн хяналтын системийн веб интерфейс



29–р зураг. Жолоочийн мэдээллийн график дүрслэл



30–р зураг. Стрессийн түвшний график дүрслэл

Зураг 29–д жолоочийн хяналтын мэдээллийг цагийн интервалаар нарийвчлан харуулж байна. Үүнд нүд анилтын давтамж, толгойн хөдөлгөөн, эвшээх, утас оролдох, аюултай үйлдлүүдийн үзүүлэлтүүдийг цагийн интервалаар харуулж байгаа бол 30–р зурагт жолооч тодорхой цагт стресстэй байсан үгүйл илэрхийлэх график харагдаж байна. Дээрх дэлгэрэнгүй мэдээллүүд дээр үндэслэн ослоос урьдчилан сэргийлэх шийдлүүдийг боловсруулах боломжтой.

ДҮГНЭЛТ

Энэхүү судалгааны ажил нь Хиймэл оюун ухаанд суурилсан жолоочийн аюулгүй байдлын ухаалаг хяналтын системийг боловсруулж, жолоочийн сэтгэлзүйн болон зан үйлийн өөрчлөлтөөс үүдэлтэй ослын эрсдэлийг бууруулахад чиглэв. Судалгаанд компьютерын хараа, гүн сургалт, машин сургалтын алгоритмуудыг хослуулан ашигласнаар нойрмоглох, стрессдэх, анхаарал сарних болон хориотой үйлдлүүдийг бодит цагийн орчинд илрүүлэх боломжийг бүрдүүлсэн.

Нойрмоглолт ба анхаарал сарнилт илрүүлэх модулиар MediaPipe FaceMesh санг ашиглан жолоочийн нүүрний 468 цэгийн мэдээлэлд дүн шинжилгээ хийж, нүдний хувирал, амны хөдөлгөөн, толгойн чиглэл зэрэг үзүүлэлтүүдийн өөрчлөлтөд үндэслэн нойрмоглох болон анхаарал сарнисан төлөвийг тодорхойлсон. Энэ модуль нь жолооч анхаарал сарнисан үед анхааруулга өгөх боломжийг олгосон.

Хориотой үйлдэл таних модулийг Vision Transformer (ViT) болон Data-efficient Image Transformer (DeiT) архитектурт тулгуурлан хөгжүүлсэн бөгөөд энэхүү модуль нь “утсаар ярих”, “ус уух”, “эвшээх”, “бусад” гэсэн дөрвөн төрлийн үйлдлийг 99.2%-ийн нарийвчлалтайгаар ангилж чадсан.

Харин стрессийн түвшин тогтоох модулийн хувьд Support Vector Machine (SVM) болон Convolutional Neural Network (CNN) загваруудыг ашиглаж, нүүрний илэрхийлэлд суурилан эерэг болон сөрөг сэтгэл хөдлөлийг ялган тодорхойлох боломжийг бүрдүүлэв. Энэ модулийн хамгийн өндөр гүйцэтгэл 92.6%-ийн нарийвчлалтайгаар гарсан байна.

Эдгээр модулиудыг нэгтгэн боловсруулсан систем нь жолоочийн аюултай үйлдэл, анхаарал, ядралт, стрессийн түвшнийг бодит цагийн орчинд хянаж, аюул үүсэхээс өмнө анхааруулах боломжтой юм. Ийнхүү боловсруулсан хиймэл оюун ухаанд суурилсан жолоочийн хяналтын систем нь зам тээврийн ослоос урьдчилан сэргийлэх, аюулгүй байдлыг хангах, хүний хүчин зүйлтэй холбоотой эрсдэлийг бууруулахад үр ашигтай шийдэл болж байна.

Цаашид энэхүү системийн хөгжүүлэлтийг IoT-той хослуулан бодит байдал дээр, нэмэлт өгөгдлийн багцаар сайжруулан сургаж модулиудыг нэмэлтээр хөгжүүлснээр судалгааны үр дүнг практикт нэвтрүүлэх боломжтой гэж үзэж байна.

**АШИГЛАСАН МАТЕРИАЛ,
НОМ ЗҮЙ**

- [1] Das, S., Pratihari, S., Pradhan, B., Jhaveri, R. H., & Benedetto, F. (2024). IoT-assisted automatic driver drowsiness detection through facial movement analysis using deep learning and a U-Net-based architecture. *Information*, 15(1), 30. [CrossRef]
- [2] Delwar, T. S., Singh, M., Mukhopadhyay, S., Kumar, A., Parashar, D., Lee, Y., Rahman, M. H., Sejan, M. A. S., & Ryu, J. Y. (2025). AI- and deep learning-powered driver drowsiness detection method using facial analysis. *Applied Sciences*, 15(3), 1102. [CrossRef]
- [3] Yang, E.; Yi, O. Enhancing Road Safety: Deep Learning-Based Intelligent Driver Drowsiness Detection for Advanced Driver-Assistance Systems. *Electronics* 2024, 13, 708. [CrossRef]
- [4] Fonseca, T., & Ferreira, S. (2025). Drowsiness detection in drivers: A systematic review of deep learning-based models. *Applied Sciences*, 15(16), 9018. [CrossRef]
- [5] Chew, Y. X.; Abdul Razak, S. F.; Yogarayan, S.; Sayed Ismail, S. N. M. Dual-Modal Drowsiness Detection to Enhance Driver Safety. *Computers, Materials & Continua* 2024, 81(3), 4397–4417. [CrossRef]
- [6] Liu, Y. (2024). The method of driver fatigue detection in intelligent driving. *Theoretical and Natural Science*, 51, 137–141. [CrossRef]
- [7] Hou, J., Zhang, B., Zhong, Y., & He, W. (2025). Research progress of dangerous driving behavior recognition methods based on deep learning. *World Electric Vehicle Journal*, 16(2), 62. [CrossRef]
- [8] Government of Mongolia. (2018). Монгол улсын замын хөдөлгөөний дүрэм [Road traffic rules of Mongolia] (Resolution No. 239). [CrossRef]

ТАМИРЧДЫН БИЕЙН БҮТЦИЙН ҮЗҮҮЛЭЛТҮҮДИЙГ МАШИН СУРГАЛТЫН АРГА АШИГЛАН ТООЦООЛОХ НЬ

Гантулгын АНУУЖИН¹, Амгаланбаярын НОМИН-ЭРДЭНЭ², Оюунтуяагын ОДБАЯСГАЛАН³, Батжаргалын ДОЛГОРСҮРЭН⁴

^{1,2,3,4}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбоо технологийн сургууль, Мэдээлэл технологийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: b.dolgorsuren@must.edu.mn⁴

Хураангуй: Энэхүү судалгаа нь Монгол улсын хэмжээнд сагсан бөмбөгийн спортоор хичээллэж буй тамирчдын биеийн бүтцийн үзүүлэлтүүдийг үнэлэхэд зориулсан биоимпеданс (BIA) хэмжүүрийн найдвартай байдлыг шалгах мөн машин сургалт ашиглан үзүүлэлтүүдийг тооцоолох зорилготой. Судалгаанд нийт 11 тамирчин (Монгол 8, гадаад 3) хамрагдсан бөгөөд тэдний биеийн бүтцийн үзүүлэлтийг Inbody 270, физиологийн ба хүч чадлын үзүүлэлтийг Monark Ergometer болон Hand Dynamometer, морфологи болон уушги, цусны эргэлтийн өгөгдлүүдийг Spirometry, Oximeter гэх мэт BIA төхөөрөмжүүдээр хэмжиж, сургалтанд ашиглагдах тоо өгөгдлөө бэлтгэсэн. Цаашлаад эдгээр өгөгдлийг ашиглан хувь хүний ерөнхий биеийн бүтэц, тэнцвэр, бодисын солилцооны чанарыг илэрхийлдэг нэгтгэл үзүүлэлт болох InBody Score-ийг машин сургалтын Random Forest, Simple Linear, Multiple Linear, Ridge, Lasso, Polynomial гэх мэт 6 төрлийн regression аргаар тооцоолох, үнэлэх, аргуудыг харьцуулах судлахыг зорьсон. Эдгээр хамгийн өндөр сургалтын болон тестийн үр дүнг Random Forest Regression загвар бөгөөд нарийвчлал (R^2) 0.99, дундаж абсолют алдаа (MAE) 0.044, дундаж квадрат язгуур алдаа (RMSE) 0.0083 гэсэн үр дүнг үзүүлсэн нь InBody Score-ийг өндөр нарийвчлалтайгаар урьдчилан таамаглах боломжийг харуулж байна. Судалгааны үр дүнг бүртгэл хяналтын системтэй уялдуулах тамирчдын биеийн бүтцийг хянах, дасгалын ачаалал, өдөр тутмын мониторинг хийхэд тус дөхөм болох мөн хиймэл оюуны тусламжтайгаар тамирчдад бэлтгэл сургуулалтын зөвлөгөө гаргах боломжтой юм.

Түлхүүр үг: Тамирчдын гүйцэтгэл, биеийн бүтцийн мониторинг, BIA, InBody Score, машин сургалт

I. УДИРТГАЛ

Спортын тамирчдын амжилт нь зөвхөн дасгал хөдөлгөөн, техникээс гадна биеийн эрүүл мэнд, хоолны дэглэмтэй шууд хамааралтай. Ялангуяа биеийн өөхний илүүдэл нь булчингийн массыг бууруулж, зүрх судас, бодисын солилцооны үйл ажиллагаанд сөргөөр нөлөөлдөг. Иймд тамирчдын булчин болон өөхний массыг үнэлэх, хянах нь эрүүл мэндийг хамгаалах, хоол тэжээлийн зөвлөмж боловсруулах, бэртэлээс урьдчилан сэргийлэхэд чухал ач холбогдолтой. Орчин үеийн биеийн бүтцийн шинжилгээ нь зөвхөн биеийн жингээр дүгнэлт гаргахаас илүү нарийвчлалтай бөгөөд булчингийн хөгжлийн түвшин, өөхний тархалт, усны харьцаа зэрэг олон үзүүлэлтийг хамардаг. InBody Score нь эдгээр үзүүлэлтүүдийг нэгтгэн ерөнхий биеийн тэнцвэр, бодисын солилцооны чанарыг илэрхийлдэг. Энэхүү судалгааны зорилго нь 1) Монгол тамирчдын биеийн бүтцийн үзүүлэлтүүд (нас, өндөр, жин, булчингийн масс, өөхний хувь, биеийн усны харьцаа) ба InBody Score-ийн хоорондын хамаарлыг тодорхойлох 2) Хиймэл оюун, машин сургалтын аргаар InBody Score-ийг таамаглах 3) Судалгааны үр дүнг тамирчдын биеийн бүтцийг хянах, дасгалын ачааллыг тохируулах, гаргахад ашиглах явдал юм.

II. СУДАЛГААНЫ АРГА ЗҮЙ

2.1. Судалгаанд оролцогчид

Судалгаанд 11 эрэгтэй тамирчин хамрагдсан. Насны дундаж нь 22.1 ± 3.2 жил, насны хязгаар нь 20–40 нас байв. Оролцох тамирчдыг сонгохдоо дараах шалгуур үзүүлэлтийг тавьсан. Үүнд, нэгдүгээрт, сагсан бөмбөгийн спортын дээд лиг эсвэл түүнтэй дүйцэхүйц түвшний тэмцээнд тогтмол оролцдог байх. Хоёрдугаарт, спортын бэлтгэл хийдэг, гуравдугаарт, сүүлийн 24 цагт архи, кофе, хүчтэй дасгал хийгээгүй байх.

2.2. Судалгааны орчин

Судалгаанд оролцогч бүрт судалгааны зорилго, арга зүй, боломжит эрсдэл, үр дүнг ашиглах нөхцөл зэргийг дэлгэрэнгүй тайлбарлаж, мэдээлэлд үндэслэсэн бичгээр зөвшөөрөл (informed consent) авсан. Бүх оролцогчдын хувийн мэдээллийг нууцалж, зөвхөн судалгааны зорилгоор тэдгээр тамирчдаас хэмжилтийн төхөөрөмжөөс гаргаж авсан тоон өгөгдлүүдийг ашигласан болно. Судалгааны хэмжилт, туршилтуудыг Анагаахын Шинжлэх Ухааны Их Сургууль (АШУИС)-ийн Биеийн тамир, спортын шинжилгээний лаборатори болон Физиологи, био хэмжилтийн төв лаборатори-д гүйцэтгэсэн. Судалгааны орчинг стандарт нөхцөлд хадгалж, температур, чийгшил, гэрэлтүүлэг зэрэг параметруудийг тогтмол хянасан.

2.3. Хэмжилтийн багажууд

Судалгаанд оролцогчдын антропометрийн болон физиологийн үзүүлэлтүүдийг хэмжихдээ Хүснэгт 1-д

харуулсан нарийвчилсан багаж хэрэгслийг ашигласан бөгөөд ашиглалтаас өмнө калибровк, техникийн үзлэгээр шалгаж, хэмжилтүүдийн нарийвчлалыг баталгаажуулсан. Бүх хэмжилтүүдийг туршилтын стандарт протоколын дагуу гүйцэтгэсэн бөгөөд лабораторийн орчны болон багажийн нарийвчлалыг хамгийн өндөр түвшинд хадгалахыг зорьсон.

1-Р ХҮСНЭГТ: СУДАЛГААНД АШИГЛАСАН БАГАЖ, ТӨХӨӨРӨМЖ, ҮЗҮҮЛЭЛТ

Зориулалт	Төхөөрөмж	Үйлдвэрлэгч	Үзүүлэлт
Биеийн бүтэц	InBody 270	InBody Co., Ltd., Seoul, South Korea	Биеийн нийт жин, булчингийн масс, өөхний хувь, ECW Ratio...
Гарын хүч	Hand Dynamometer	Takei T.K.K. 5401 Grip-DTakei Scientific Instruments Co., Ltd., Japan	Баруун, зүүн грын индекс, атгалтын хүч, булчингийн тойрог
Хөлийн Хүч	Monark 881E ба Monark 894E	Cycle Ergometer (Sweden)	Хөлийн урт, хүч, хэмжээс
Уушгины үнэ	MicroLab ML350 Spirometer	(CareFusion, UK)	Амьсгалын хэмжээ, уушгины багтаамж
Цусны эргэл	Upalm UT100 Pulse Oximeter	(Upalm Medical, China)	Зүрхний цохилт болон цусан дахь хүчилтөрөгчийн хангалтыг (spo2)

2.4. Цуглуулсан өгөгдөл, үзүүлэлтүүд ба тооцоолсон индексүүд

Антропометрийн үзүүлэлтүүд болох тамирчдын нас, өндөр, жин, BIA-ийн үндсэн үзүүлэлтүүд болох BMI (Body Mass Index), Hydration (L), Body fat % (Биеийн өөхний хувь), Skeletal Muscle Mass (Араг ясны булчингийн масс), ECW Ratio (Эсийн гаднах усны харьцаа), Basal Metabolic Rate (Суурь бодисын солилцооны хурд) нийт 31 хувьсагч, цаашлаад хүч чадлын үзүүлэлтүүд болох гарын 8, болон хөлийн 14, нийт 53 үзүүлэлтийг хэмжсэн тоон мэдээлэл цуглуулсан. Эдгээр дээр үндэслэн зорилтот хувьсагч болох InBody Score-ийг регрессийн аргаар таамаглана.

2.5. Хэрэглэсэн орчин (Software Environment)

Судалгаанд Python 3.12.6 орчинг ашигласан бөгөөд өгөгдлийн боловсруулалт, шинжилгээ болон машин сургалтын загваруудыг дараах сангуудын тусламжтайгаар гүйцэтгэсэн. Үүнд: NumPy 1.26.4, Pandas 2.2.1, Scikit-learn 1.5.2, Matplotlib 3.8.4, болон

Seaborn 0.13.2. Бүх туршилтуудыг Windows 11 үйлдлийн систем бүхий компьютерт (Intel Core i7, 16GB RAM) гүйцэтгэсэн. Туршилтын дахин давтагдах чадварыг хангах үүднээс бүх код, өгөгдөл, багажийн тохиргоог ижил орчинд хадгалсан.

Өгөгдлийн боловсруулалтын дараалал (Data Processing Workflow)

Хэмжилтээс гарсан бүх өгөгдөл InBody 270 ба бусад хэмжилтийн төхөөрөмжөөс CSV файл хэлбэрээр экспортлогдож, Python орчинд дараах дарааллаар боловсруулагдсан.

- Өгөгдөл цэвэршүүлэх:** хоосон эсвэл алдаатай утгуудыг шалгаж, арилгасан.
- Normalization:** бүх хэмжигдэхүүнийг 0–1 мужид хувиргасан.
- Data Augmentation:** өгөгдлийн хэмжээг нэмэгдүүлэхийн тулд ±5%-ийн шум (noise) нэмэх, санамсаргүй жингийн хэлбэлзэл оруулсан.
- Train/Test Split:** өгөгдлийг 80:20 харьцаагаар сургалт болон тестийн багцад хуваасан.
- Cross-Validation:** 5-fold cross-validation ашиглан загварын гүйцэтгэлийг (Train R2, Test R2, MAE, RMSE) үзүүлэлтүүдээр үнэлсэн.
- Model Training:** Random Forest, Simple Linear, Multiple Linear, Ridge, Lasso, Polynomial зэрэг загваруудыг сургасан.

III. СУДАЛГААНЫ ХЭСЭГ

3.1 Ижил төстэй ажлуудын судалгаа

Монголд тамирчдын биеийн бүтцийн үзүүлэлтийг машин сургалтын арга ашиглан тооцоолох судалгаанууд хараахан хийгдээгүй байгаа ч энэ чиглэлээр гадаадын бусад улсуудад олон жилийн турш судлагдсан бөгөөд тэдгээрээс гурван дурьдъя. Судалгаа [1]-т болохоор машин сургалтын аргыг ашиглаж тамирчдын эрүүл мэнд, гүйцэтгэл ба сэргэх үйл явцыг хянах судалгаа байгаа бөгөөд энэхүү судалгаанд 3661 тамирчны эрүүл мэндийн үзүүлэлт дээр нарийвчилсан судалгаа явуулсан ба “катаболизм” ба “анаболизм” фенотипийг тодорхойлоход оролцдог үзүүлэлтүүдийн ач холбогдлыг Random Forest болон Multinomial Logistic Regression машин сургалтын аргаар шинжлэн гаргасан байна. Эдгээр аргыг ашигласнаар тамирчны тэмцээний дараах сэргэх процессыг шинжлэхэд цус ба шээсний биохимийн хамгийн чухал үзүүлэлтүүдийг тодорхойлж чадсан. Булчингийн метаболизмын үзүүлэлтүүд (аспартат аминотрансфераз, креатин киназ, лактат дегидрогеназ, аланин аминотрансфераз) болон орнитин циклийн үзүүлэлтүүд (креатинин, шээсний хүчил, шээс) катаболизм ба анаболизм гэсэн хоёр төрлийн метаболизмыг ангилахад хамгийн их нөлөө үзүүлдэг болохыг тогтоов. Random Forest алгоритм ашиглахдаа Decision tree-үүдийг ensemble байдлаар ашиглаж, accuracy, precision, recall зэрэг үзүүлэлтээр үнэлсэн. Үүний үр дүнд Random Forest алгоритм нь дуу чимээний нөлөөнд тэсвэртэй, булчингийн метаболизмын ангилалд

0.99 accuracy, 0.98 recall, элэгний метаболизмд 0.95 accuracy, 0.85 recall-т гэсэн үр дүнд хүрсэн.

Судалгаа [2]-т болохоор тамирчны хяналтын өгөгдлийг шинжлэхэд ашиглагддаг олон төрлийн арга зүйг авч үзэж, шийдвэр гаргалтын үйл явцыг хөнгөвчлөх, мэдээлэл өгөхөд чиглэсэн судалгаа бөгөөд энэхүү судалгааны хүрээнд аналитик, статистикийн Z score болон STEN score (Standard Ten Scores), ACWR (Acute:Chronic Workload Ratio), EWMA (Exponential Weighted Moving Average) тооцож үнэлсэн бөгөөд тооцоолол нь үр дүнтэй, хэрэглээнд тохиромжтой гэж гарсан.

Судалгаа [3]-т болохоор Ромни үүлдрийн насанд хүрсэн буюу 43–54 сартай эм хонины амьд жингийн өмнөх жин болон одоогийн жингийн мэдээллийг ашиглан биеийн нөхцлийн үнэлгээ буюу BCS (Body Condition Score)-г машин сургалтын аргаар тооцоолон гаргасан. Энэхүү судалгаанд Ordinal Logistic Regression, Multinomial Regression Linear, Discriminant Analysis (LDA), Classification and Regression Tree (CART), Random Forest (RF), k-Nearest Neighbour (KNN), Support Vector Machine (SVM), Artificial Neural Network (ANN), Gradient Boosting Decision Tree (XGB) гээд нийт 9 төрлийн алгоритмуудыг хооронд нь харьцуулж судалгаагаа хийсэн. Үүний үр дүнд хамгийн өндөр гүйцэтгэлтэй алгоритм нь XGB (Gradient Boosting Decision Tree) байсан бөгөөд нарийвчлал нь 90% гарсан. Судалгааны дүгнэлтээр амьд жингийн өгөгдлийг ашиглан биеийн нөхцлийн үнэлгээг өндөр нарийвчлалтайгаар таамаглах боломжтой гэж үзсэн.

2-Р ХҮСНЭГТ: ХАРЬЦУУЛСАН СУДАЛГАА

Судалгаа	Гадаадын Систем дэх Харьцуулалт	Ялгаа/Боломж
Физиологийн өгөгдөл: Зүрхний дохилт, VO2, EMG, Амьсгал	Catapult ба Polar нь HR болон Хөдөлгөөний ачааллыг голчилдог. VO2 болон EMG нь тусдаа нарийн төхөөрөмж шаарддаг.	Хэрэв та EMG (булчингийн идэвхжил) ба VO2 (хүчилтөрөгчийн хэрэглээ) -г нэг wearable төхөөрөмжөөр хэмжиж, нэгтгэж чадвал, таны систем булчингийн ядралт, бодисын солилцооны нарийвчилсан анализ-аараа илүү байх болно.
Биеийн Бүтэц/Антропометрийн хэмжилт: SMM, Fat %	Catapult/Polar нь эдгээр өгөгдлийг ихэвчлэн API эсвэл гараар оруулдаг. Тэдний сенсор нь зөвхөн хөдөлгөөн/HR хэмждэг.	Хэрэв та Биеийн Бүтцийн Анализатор (Bioelectrical Impedance Analysis) -ын өгөгдлийг IoT-гоор шууд real-time ачаалалтай нэгтгэж, SMM-ийн өөрчлөлт, SMI (Skeletal Muscle Index) зэргийг тогтмол хянаж чадвал өвөрмөц давуу тал болно.
Системийн UX: Time-series анализ, Data Visualization	Гадаадын системүүд маш сайн график, Heat Map, Player Comparison-уудыг ашигладаг.	Та Монголын нөхцөлд зориулсан хэрэглэгчийн ойлгомжтой, хялбар интерфэйсийг бий болгох, мөн дээр дурдсан Сэтгэл зүй/Нойр-ын өгөгдлийг физиологийн өгөгдөлтэй нэгтгэсэн шинэлэг Recovery Index анализийг гаргах нь давуу тал болно.

IV. АШИГЛАСАН АРГА

Машин сургалтанд 11 тамирчны 2 удаагын хэмжилтийн үр дүнг авч үзэх бөгөөд эдгээр өгөгдөл

машин сургалтыг сургахад хангалтгүй гэж үзсэн учир тоон өгөгдөл дээрээ data augmentation хийсэн.

Data augmentation хийхдээ дараах Хүснэгт 3-т оруулсан аргуудыг түгээмэл хэрэглэдэг.

3-Р ХҮСНЭГТ: ӨГӨГДЛИЙГ ИХЭСГЭХ АРГУУД

Арга	Тайлбар	Хаана тохиромжтой
Noice injection	Тоон утгуудад бага зэрэг ($\pm 1-5\%$) санамсаргүй өөрчлөлт оруулах	Regression, numeric data augmentation
SMOTE (synthetic minority oversampling technique)	Minority class-д шинэ жишээ synthetic байдлаар үүсгэх	Classification (imbalanced dataset)
Bootstrapping	Өгөгдлөөс санамсаргүйгээр дахин дээж авах (replacement-тэй)	Ensemble learning (Random Forest гэх мэт), бага өгөгдөл байх үед
Mixup/interpolation	Хоёр өгөгдлийг жингийн харьцаагаар хольж шинэ жишээ үүсгэх	Regression, deep learning model
GAN-based generation	Neural network ашиглан шинээр бодит мэт өгөгдөл үүсгэх	Том хэмжээний, complex data (зураг, дуу, advanced numeric data)

Бидний тооцоолсноор Bootstrapping бага өгөгдөл дээр ажиллах мөн machine learning сургах үед тохиромжтой гэж үзээд тамирчдынхаа өгөгдлийг data augmentation (22 мөр \rightarrow 1000 мөр) хийж ашигласан байгаа.

3.1 Regression шинжилгээ

Регрессийн шинжилгээгээр дараах Хүснэгт 4-т харьцуулсан 6 төрлийн регрессийн аргыг ашиглав.

4-Р ХҮСНЭГТ: РЕГРЕССИЙН АРГУУДЫН ХАРЬЦУУЛАЛТ

Арга	Давуу тал	Хэрэглээ
Random Forest Regressor	Хялбар, тайлбарлах боломжтой	Харьцангуй бага өгөгдөл (n=10–50), шууд хамаарлыг шалгах
Simple Linear Regression	Хялбар, ойлгомжтой, хурдан ажилладаг, Visualization хийхэд тохиромжтой	1 predictor (feature) байгаа тохиолдолд, хувьсагч ба target хооронд шууд шугаман холбоо

		байвал
Multiple Linear Regression	Олон хувьсагчийг нэгэн зэрэг ашиглах боломжтой Харилцан нөлөөг (interaction) ойлгоход тусална	Олон predictor байгаа Predictor-ууд хооронд хэт collinearity байхгүй бол хамгийн сайн
Ridge Regression	Overfitting-ийг бууруулдаг, Predictor-ууд хооронд collinearity их үед ч тогтвортой, том dataset болон олон feature-д тохиромжтой	Predictor-уудын тоо их Predictor-ууд хооронд collinearity байгаа Model overfitting бууруулах шаардлагатай
Lasso Regression	Feature selection хийдэг, Overfitting-ийг бууруулдаг Model-ийг энгийн, ойлгомжтой болгодог	Predictor-уудын тоо их, зарим нь чухал биш Feature selection хийх шаардлагатай
Polynomial Regression (degree=2)	Non-linear харилцааг барих, боломжтой олон талт шугаман бус patterns-г тодорхойлдог	Predictor ба target хооронд шугаман бус холбоо байгаа Simple linear regression хангалтгүй байвал

Регрессийн шинжилгээнийхээ үр дүнд сургасан машин сургалтуудаа хэр зэрэг нарийвлалтайгаар сурсан эсэхийг шалгахын тулд 5-р хүснэгтэд байгаа машин сургалтын загварын гүйцэтгэлийг үнэлэх үзүүлэлтүүдийг авч үзсэн. Мөн эдгээрээс гадна давхар cross-validation хийж шалгаж үзсэн.

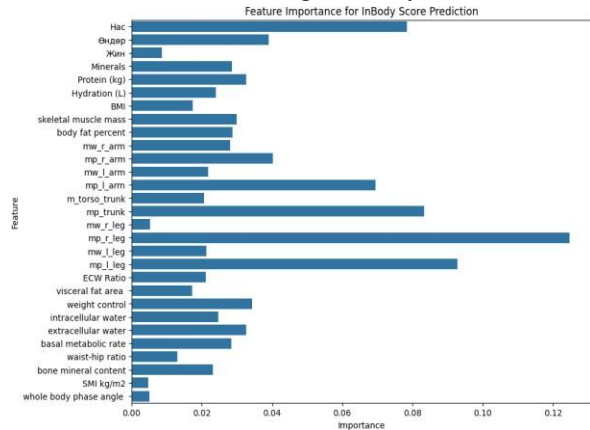
4-р ХҮСНЭГТ: ЗАГВАРУУДЫГ ХАРЬЦУУЛАХ ХЭМЖҮҮРҮҮД

Хэмжүүр	Тайлбар	Томъёо
Train R2 score	Сургалтын өгөгдөл дээр загварын тайлбарлах чадварыг хэмжинэ	$R^2_{train} = 1 - \frac{\sum (y_{train} - \hat{y}_{train})^2}{\sum (y_{train} - \bar{y}_{train})^2}$
Test R2 score	Шинэ өгөгдөл дээр загварын тайлбарлах чадварыг харуулна	$R^2_{test} = 1 - \frac{\sum (y_{test} - \hat{y}_{test})^2}{\sum (y_{test} - \bar{y}_{test})^2}$
MAE	Загварын дундаж алдааг абсолот () утгаар хэмждэг. Бага байх тусам(0-тэй ойрхон) сайн	$MAE = \frac{1}{n} \sum_{i=1}^n y_i - \hat{y}_i $
RMSE	Алдааг квадрат болгож дундажлаад язгуур гаргадаг. Мөн RMSE бага байх тусам сайн	$RMSE = \sqrt{\frac{1}{n} \sum_{i=1}^n (y_i - \hat{y}_i)^2}$

3.3 Regression plot

Регрессийн шинжилгээний үр дүнг barplot графикаар дүрсэлж аль үзүүлэлтүүд нь In-Body score тооцоолоход хүчтэй нөлөөлж байгааг дараах регрессийн аргууд дээрээ харууллаа.

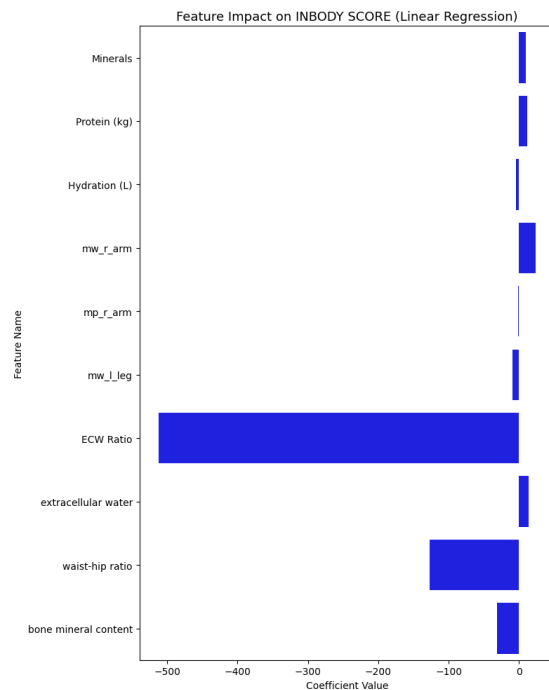
1. Random Forest Regression хувьд:



1-р зураг. Random Forest Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

1-р зурагт үзүүлснээр mp_r_leg (muscle percentage right leg), mp_l leg (muscle percentage left leg), mp_trunk (muscle percentage trunk), нас, mp_l_arm (muscle percentage left arm) үзүүлэлт нь бусад үзүүлэлтээсээ илүү өндөр байгааг харж болох ба In-Body Score тооцоолоход их нөлөөтэй харагдаж байна.

2. Simple Linear Regression хувьд:

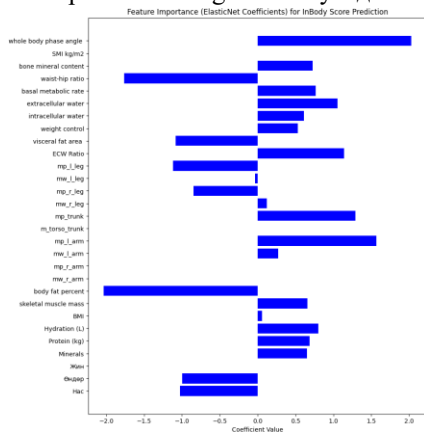


2-р зураг. Simple Linear Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

Дээрх зурагт үзүүлснээр mp_l_arm (muscle percentage left arm) илүү өндөр үзүүлэлттэй харагдаж байгаа

бөгөөд энэ хувьсагч нь энэ регрессийн аргын хувьд үр дүнд нөлөөлөх чанар нь илүү сайн байгаа бөгөөд ECW Ratio хувьсагч нь хасах руу заасан байгаа нь тухайн хувьсагч нэмэгдэхэд зорилтот утга буюу In-Body score буурах болно.

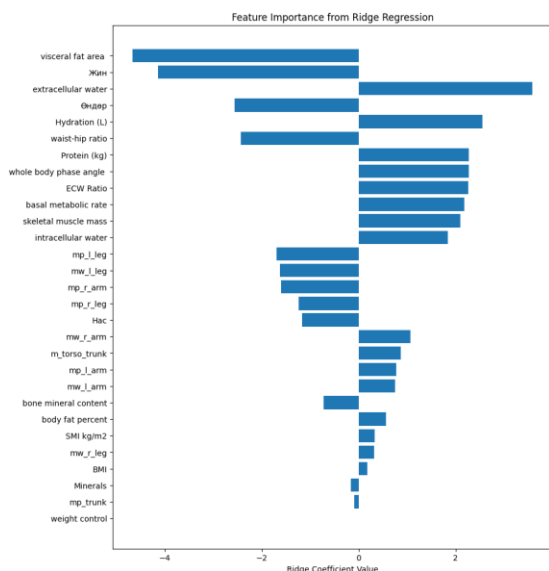
3. Multiple Linear Regression хувьд:



2-р зураг. Multiple Linear Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

Зурагт үзүүлснээр whole body phase angle, mp_l_arm(muscle percentage left arm), mp_trunk(muscle percentage trunk) эдгээр хувьсагчууд машин сургалтанд тооцоолол хийхэд ихээхэн нөлөөлж байгаа бол нөгөөтэйгүүр waist-hip ratio, body fat percent, visceral fat area, mp_l_leg(muscle percentage left leg), mp_r_leg зэрэг хувьсагчууд нь ихсэх үед тооцооллын зорилтот утгуудыг бууруулж байна.

4. Ridge Regression

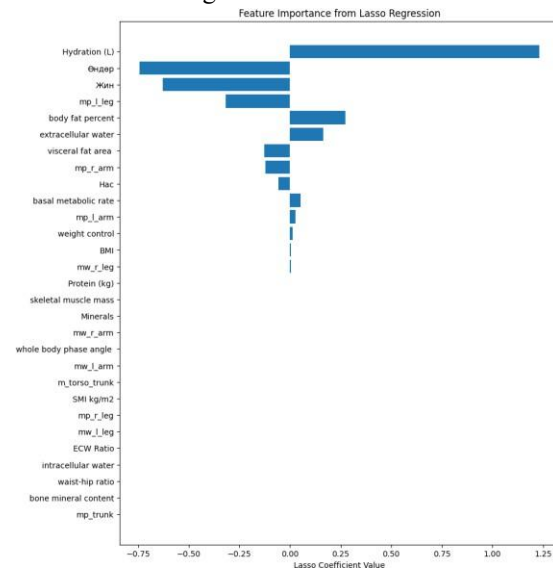


3-р зураг. Ridge Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

Зурагт үзүүлснээр extracellular water, hydration эдгээр хувьсагчууд машин сургалтанд тооцоолол хийхэд нөлөөлж бөгөөд waist-hip ratio, visceral fat area, жин, өндөр зэрэг эдгээр хувьсагчууд нь ихсэх үед тооцооллын утгуудыг бууруулж байна. Үүнээс

дүгнэвэл биеийн өөх хувь их байх тусам тамирчны дасгал сургуулилтанд сөргөөр нөлөөлөх боломжтойг харж болно.

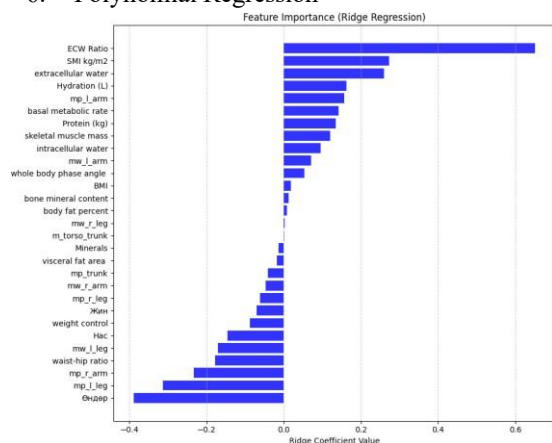
5. Lasso Regression



4-р зураг. Lasso Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

Энэ зурагт 5 зураг-г харуулсан регрессийн хувьд тооцоолол хийхдээ цөөн хэдэн хувьсагчдын үзүүлэлтэнд суурилож машин сургалтын аргыг ашигласан ба тэдгээр хувьсагчдаас hydration, body fat percent, extracellular water хувьсагчууд нь эерэг үзүүлэлтийг зааж бусад болох өндөр, жин, mp_l_leg(muscle percentage left leg), visceral fat area, mp_r_arm(muscle percentage righth arm), нас зэрэг хувьсагчид нь сөрөг хамаарлыг зааж байгаа нь эдгээр хувьсагчдын үзүүлэлт ихсэхэд энэ регрессийн хувьд зорилтот утгуудын үр дүнг бууруулах хандлагатай харагдаж байна.

6. Polynomial Regression



5-р зураг. Polynomial Regression ашиглан тооцоолоход аль хувьсагч нөлөөлж буй үзүүлэлтүүд

Polynomial Regression аргад тооцоолол хийхэд ECW Ratio, SMI, hydration эдгээр хувьсагчууд нь өндөр байх тусам сургалтын үр дүнд нөлөөлж байгаа бөгөөд эсрэгээрээ өндөр, mp_l_leg(muscle percentage left leg), mp_l_arm(muscle percentage left arm) гэх зэрэг

хувьсагчуудын утгууд зорилтот утга гаргахад үр дүнг бууруулахаар байна.

3.4 Үр дүн

Дараах 6 төрлийн регрессийг ашиглан машин сургалтаа сургасны үр дүнд Random Forest Regression нь бусад машин сургалтаасаа илүү найдвартайгаар нарийвчлан тооцоолж гаргаж ирж байна гэж үзэж байна. Үр дүнгийн хариуг 6-р хүснэгтэд харуулав.

6-Р ХҮСНЭГТ: ТҮРШИЛТЫН ҮР ДҮН

Загвар	Train R ²	Test R ²	MAE	RMSE
Random Forest Regression	0.99	0.99	0.044	0.0083
Simple linear Regression	0.98	0.98	2.82	4.05
Multiple Linear Regression	0.95	0.93	2.82	2.12
Ridge Regression	0.985	0.984	0.55	0.715
Lasso Regression	0.98	0.976	0.676	0.868
Polynomial Regression	0.996	0.996	0.355	0.354

Аль регрессийн аргачлал In-Body score тооцоолоход илүү үр дүнтэй, сайн тохирч байгааг шинжилэхийн тулд дараах хүснэгт 6-д байгаа хүчин зүйлсүүдийн уялдаа хамаарлыг шалгана.

6-Р ХҮСНЭГТ: ШАЛГУУР ҮЗҮҮЛЭЛТҮҮД

Үзүүлэлт	Авбал зохих утга
Train R ²	0.85–0.99 байвал сайн бөгөөд машин сургалт сайн сурсан гэж үзэж болно
Test R ²	Train R ² -тэй ойролцоо эсвэл арай бага байвал сайн
MAE	0.01–0.1 хооронд байвал маш сайн гэж үзнэ
RMSE	0.01–0.15 хооронд байвал сайн

Эдгээр олон хүчин зүйлийн регрессийн аргачлалын үр дүн болон нарийвлалын үндсэн дээр Random Forest regression **Train R² = 0.99, test R² = 0.99** буюу In-Body Score-ийн 99%-ийн үзүүлэлттэйгээр тайлбарлаж байгаа бөгөөд бусад регрессийн аргаас илүү найдвартай, сайн сургагдсан мөн шууд хамаарлыг шалгаж байгаагаар онцлогтой байна.

Энэхүү үр дүн нь өмнөх судалгаануудтай нийцэж байна. Kim et al. (2022) болон Park et al. (2023) нарын судалгаагаар ECW Ratio болон Body Fat % нь InBody Score-д хүчтэй сөрөг нөлөөтэй болохыг тогтоосон байдаг.

Random Forest Regression нь non-linear хамаарлыг сайн илрүүлж, жижиг хэмжээний өгөгдөлд overfitting багатай байсан.

ДҮГНЭЛТ

Энэхүү судалгаа нь Монгол тамирчдын биеийн бүтцийн үзүүлэлтийг үнэлэх, таамаглах зорилгоор Машин сургалтын (Machine Learning - ML) аргуудыг амжилттай хэрэглэсэн анхдагч ажлуудын нэг юм. Судалгааны гол дүгнэлтүүд нь:

- Загварын Гүйцэтгэл:** Судалгаанд ашигласан *Random Forest Regression* загвар нь InBody Score-ийг таамаглах хамгийн өндөр гүйцэтгэлийг үзүүлсэн бөгөөд туршилтын өгөгдөл дээр $R^2 = 0.99$ ($MAE = 0.044$, $RMSE = 0.0083$) гэсэн үр дүнд хүрсэн нь тус загвар нь тамирчдын биеийн бүтцийг хянах найдвартай арга болохыг баталж байна.
- Үзүүлэлтүүдийн Нөлөө: InBody Score-ийн өсөлтөд булчингийн хувь (mp_l_leg , mp_trunk , mp_r_leg) нь хамгийн хүчтэй эерэг нөлөө үзүүлж байна. Харин биеийн өөхний хувь (*Body Fat Percent*), дотор өөхний хэмжээ (*Visceral Fat Area*), мөн эсийн гаднах усны харьцаа (*ECW Ratio*) зэрэг үзүүлэлтүүд нь InBody Score-д сөрөг нөлөөтэй байсан нь өмнөх судалгаануудтай нийцэж байна [Kim et al. (2022), Park et al. (2023)].
- Хүч Чадалтай Хамаарал: Гарын болон хөлийн хүчний үзүүлэлтүүд (*Dynamometer*, *Monark-oop хэмжсэн*) нь InBody Score-тэй эерэг хамааралтай ($r=0.69-0.78$) гарсан нь биеийн бүтцийн чанар (*өндөр InBody Score*) нь тамирчны физик гүйцэтгэл (хүч чадал)-тэй шууд хамааралтай болохыг харуулж байна.

Хязгаарлалт ба Цаашдын Ажил: Судалгаа нь нийт 11 тамирчны өгөгдөлд (Data Augmentation ашигласан Augmentation-ийг $\pm 5\%$ шум нэмэх (noise injection) ба resampling аргаар гүйцэтгэсэн.) тулгуурласан нь гол хязгаарлалт юм. Цаашид, илүү олон тамирчин, бусад спортын төрлүүд (тулааны спорт, хөнгөн атлетик) -ийг хамруулсан том хэмжээний өгөгдөл цуглуулах, мөн цаг хугацааны дагуух (time-series) өөрчлөлтийг хянах ML загваруудыг нэвтрүүлэх шаардлагатай байна.

Судалгааны Ач Холбогдол: Энэхүү ажлын үр дүн нь Монголын спортын байгууллагууд болон дасгалжуулагчдад InBody Score-ийг үнэлэх нарийвчилсан, автоматжуулсан хэрэгсэл болж, тамирчдын бэлтгэлийн ачаалал, сэргэлтийг хянах шинжлэх ухаанч арга зүйг нэвтрүүлэхэд чухал хувь нэмэр оруулна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Petrovsky, D.V.; Pustovoyt, V.I.; Nikolsky, K.S.; Malsagova, K.A.; Kopylov, A.T.; Stepanov, A.A.; Rudnev, V.R.; Balakin, E.I.; Kaysheva, A.L. Tracking Health, Performance and Recovery in Athletes Using Machine Learning. *Sports* 2022, 10, 160, 1-15

- [2] “Developing Athlete Monitoring Systems in Team-Sports: Data Analysis and Visualization” by Thornton HR, Delaney JA, Duthie GM, Dascombe BJ *International Journal of Sports Physiology and Performance* 1-27
- [3] Semakula, J.; Corner-Thomas, R.A.; Morris, S.T.; Blair, H.T.; Kenyon, P.R. Application of Machine Learning Algorithms to Predict Body Condition Score from Liveweight Records of Mature Romney Ewes. *Agriculture* 2021, 11, 162, 1-8.
- [4] Kim, J., & Park, S. (2023). Machine learning–based equations for improved body composition prediction. *Journal of Body Composition Research*, 12(4), 245–256. <https://doi.org/10.1097/BCR.000000000000123>
- [5] Yanez-Sepulveda, R., Valenzuela, P. L., & Cañete, S. (2025). Supervised machine learning algorithms for the classification of obesity levels using anthropometric indices derived from bioelectrical impedance analysis. *Scientific Reports*, 15(12264). <https://doi.org/10.1038/s41598-025-15264-6>
- [6] Zhang, L., Kimura, M., & Ito, T. (2024). Artificial intelligence for body composition assessment. *Scientific Reports*, 14(83401). <https://doi.org/10.1038/s41598-024-83401-8>
- [7] Wang, Z., Chen, Y., & Liu, X. (2022). Body composition estimation based on multimodal multi-task deep neural network. arXiv preprint, arXiv:2205.11031. <https://arxiv.org/abs/2205.11031>
- [8] Rahman, M. S., & Sultana, N. (2024). Exploring unsupervised machine learning to evaluate body composition and morphological status among youth athletes in Bangladesh. *Proceedings of the International Conference on Industrial Engineering and Operations Management (IEOM), Dhaka, Bangladesh*. <https://ieomsociety.org/proceedings/bangladesh2024/236.pdf>

ЛИНУКС ҮЙЛДЛИЙН СИСТЕМИЙН ЭМЗЭГ БАЙДЛЫГ ИЛРҮҮЛЭХ, ХАМГААЛАХ БОЛОМЖИЙН СУДАЛГАА

Байгальмаагийн БАТСУУРЬ¹, Лхагваагийн ОДОНЧИМЭГ²

^{1,2}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Кибер аюулгүй байдлын
ТЭНХИМ

Холбоо барих зохиогчийн и-мэйл хаяг: batsuuribaigalimaa3@gmail.com¹

Хураангуй: Линукс үйлдлийн систем нь сервер, үүлэн тооцоолол, суулгагдсан төхөөрөмж болон IoT орчны дижитал дэд бүтцийн үндсэн бүрэлдэхүүн бөгөөд нээлттэй эхийн онцлогоос шалтгаалан аюулгүй байдлын ил тод байдал өндөр, эмзэг байдлын эрсдэл түгээмэл байдаг. Ийм нөхцөлд системийн хамгаалалтын олон түвшний (Defense-in-Depth) хандлага нь аюулгүй байдлыг цогцоор хангах стратегийн үндсэн зарчим болдог. Энэхүү судалгаанд Линуксийн аюулгүй байдлын архитектур, эмзэг байдлын ангилал, илрүүлэлтийн арга зүй, хамгаалалтын технологи болон нөхөөсийн удирдлагын үр нөлөөг онолын болон туршилтын үүднээс судалсан. Судалгаанд хосолсон буюу нэгдмэл арга зүй ашиглагдсан бөгөөд онолын судалгаа, практик туршилт болон тоон дүнгийн шинжилгээг уялдуулсан. Туршилтын орчныг бодит серверийн бүтэцтэйгээр байгуулж, эмзэг байдлын илрүүлэлт, халдлагын загварчлал, хамгаалалтын арга хэмжээг хэрэгжүүлж, үр дүнг харьцуулсан. Илрүүлэлт, хамгаалалт, нөхөөсийн удирдлагын харилцан нөлөөг судалснаар системийн хамгаалалтын түвшинг шаталсан байдлаар сайжруулах хандлагыг тодорхойлсон. Үр дүнгээс харахад олон түвшний хамгаалалтын хандлага нь халдлагын эрсдэлийг бууруулах, илрүүлэлтийн нарийвчлалыг нэмэгдүүлэх, нөхөөсийн хэрэгжилтийг хурдасгах хамгийн үр нөлөөтэй стратеги болохыг харуулсан. Энэ хандлага нь системийн цөм, сүлжээний давхарга болон хэрэглээний түвшинд хамгаалалтыг уялдуулан хэрэгжүүлэх боломжийг бүрдүүлдэг. Судалгааны үр дүн нь цаашдын Линуксийн нээлттэй эхийн орчны аюулгүй байдлын үнэлгээ, бодит хамгаалалтын бодлого боловсруулах, мөн урьдчилсан илрүүлэлт болон хиймэл оюунд суурилсан хамгаалалтын хөгжлийн суурь судалгаанд чухал ач холбогдолтой юм.

Түлхүүр үг: Системийн хатууруулалт, кернел, CVE, хэрэглэгчийн орон зай, Аюулгүй байдлын архитектур

I. УДИРТГАЛ

Линукс үйлдлийн систем нь серверийн орчин, үүлэн тооцоолол, дижитал дэд бүтэц, суулгагдсан төхөөрөмж болон интернет-д холбогдсон ухаалаг системүүдийн үндсэн технологийн суурь болон хөгжиж байна. Нээлттэй эхийн онцлог, модульчлагдсан архитектур, өндөр найдвартай ажиллагаа нь Линуксийг байгууллагууд болон хөгжүүлэгчдийн хувьд стратегийн түвшний платформ болгон өргөн ашиглах нөхцөлийг бүрдүүлдэг. Гэвч энэхүү ил тод байдал нь хамгаалалтын талаасаа хоёр талтай шинжтэй бөгөөд кодын нээлттэй байдал нь аюулгүй байдлын алдаа, эмзэг байдлыг судлан ашиглах боломжийг халдагчдад олгодог [1][2]. Орчин үеийн кибер орчинд Линукс нь эзэмшлийн буюу өмчийн үйлдлийн системүүдтэй (proprietary operating system) адил түвшний халдлагын бай болж, халдлагын зорилтот системүүдийн нэг болж байна. Хортой программ, ботнетийн зангилаа, өгөгдөл хулгайлах, DDoS халдлага, болон сүлжээний дотоод нэвтрэлтийн хэрэгслүүд Линуксийн цөм болон хэрэглэгчийн орон зайд үүссэн эмзэг байдлыг ашиглан хэрэгжиж байна. Түүнчлэн Линуксийн цөмд суурилсан IoT болон суулгагдсан системүүд тогтмол шинэчлэгддэггүй, хамгаалалтын бодлого сул хэрэгждэг, стандарт тохиргоо нь хамгаалалтгүй хэвээр үлдэх тохиолдол түгээмэл байдаг [4][6]. Үүний үр дүнд халдлагын гадаргуу өргөжиж, сүүлийн жилүүдэд бүртгэгдсэн CVE-ийн тоо эрс нэмэгдсэн байна. Линуксийн

аюулгүй байдлыг хангах уламжлалт арга нь гол төлөв нөхөөс болон системийн шинэчлэлд тулгуурладаг боловч энэ нь хангалтгүй хамгаалалт болсныг олон судалгаа онцолж байна. TuxCare [2]-ийн тайланд дурдсанаар эмзэг байдлын ихэнх нь архитектурын доголдоос бус, харин тохиргооны алдаа, хэрэглэгчийн эрхийн буруу удирдлага, эсвэл шинэчлэлтийн хоцрогдлоос үүдэлтэй байдаг. Sternum IoT [1]-ийн судалгаанд мөн суулгагдсан Линукс системүүдийн хамгаалалт хангалтгүй, шинэчлэлт тогтмол хийгддэггүй нь халдлагын гол шалтгаан болдгийг тэмдэглэсэн. Эдгээр нөхцөл байдал нь хамгаалалтад суурилсан бус, урьдчилан илрүүлэх, хянах, урьдчилан сэргийлэх тогтолцоо шаардлагатайг илтгэж байна.

Линуксийн эмзэг байдлын илрүүлэлт ба хамгаалалтын үр нөлөөг бууруулж буй хүчин зүйлсийг дараах гурван түвшинд тодорхойлж болно:

- Хөгжүүлэлтийн экосистем нь олон нийтэд тулгуурладаг тул хамгаалалтын хариуцлага хуваарилагдсан, төвлөрсөн хяналт дутмаг байдаг. Энэ нь эмзэг байдлыг илрүүлснээс хойш нөхөөс гаргах хүртэлх хугацааг уртасгадаг [3].
- Линуксийн цөмийн архитектур нарийн төвөгтэй болсон нь санах ойн гэмтэл, өрсөлдөөнт нөхцөл (race condition), системийн эрхийн зөрчил зэрэг гүн түвшний эмзэг байдлыг үүсгэж байна [5].

- SELinux, AppArmor зэрэг хамгаалалтын модуль, удирдлагын системийг системийн администраторууд буруу тохируулах, идэвхгүй болгох, эсвэл бүрэн ашиглахгүй орхих нь хамгаалалтыг сулруулдаг [6].

Судалгааны ажлын зорилго:

Линуксийн үйлдлийн системийн эмзэг байдлыг илрүүлэх болон хамгаалах боломжийг судалж, системийн аюулгүй байдлын тасралтгүй байдлыг хангах оновчтой арга зүйг тодорхойлоход оршино. Судалгаанд Линуксийн аюулгүй байдлын архитектурын бүтэц, эмзэг байдлын ангилал, илрүүлэлтийн аргачлал, хамгаалалтын технологиудыг шинжилж, практикт суурилсан хандлагаар үнэлгээ хийнэ. Мөн сүүлийн үеийн CVE бүртгэл, кибер аюулгүй байдлын байгууллагуудын техникийн мэдэгдэл, шинжлэх ухааны өгүүлэлд тулгуурлан Линуксийн хамгаалалтын арга хэмжээний үр ашиг, хэрэгжилтийн түвшинг тоон болон чанарын хувьд харьцуулна [8][9][10].

Судалгааны арга зүй нь уялдаа бүхий литературыг шинжилжээ ба кейс судалгааны хослолд тулгуурлана. Эх сурвалжид CSA Singapore [8]-ийн техникийн анхааруулга, TuxCare болон Sternum IoT-ийн тайлангууд [1][2][4][6], мөн Линуксийн аюулгүй байдлын талаарх эрдэм шинжилгээний нийтлэлүүд [3][5] багтсан. Энэхүү арга нь онолын дүн шинжилгээ болон практик жишээний уялдааг хангаж, Линуксийн эмзэг байдлыг илрүүлэх, хамгаалах арга зүйн системчилсэн зураглалыг бүрдүүлнэ.

Судалгааны зорилго дараах хоёр үндсэн чиглэлд төвлөрнө. Нэгдүгээрт, Линуксийн эмзэг байдлын гол төрөл, үүсэл, шинж чанар, илрэлүүдийг ангилан тодорхойлох. Хоёрдугаарт, илрүүлэлтийн аргачлал болон хамгаалалтын технологийн үр ашиг, хязгаарлалтыг харьцуулан дүгнэх. Энэхүү үр дүн нь Линуксийн нээлттэй эхийн орчны аюулгүй байдлыг сайжруулах бодлого боловсруулахад онолын болон практик суурь болох юм. Цаашид хиймэл оюун ба машин сургалтад суурилсан урьдчилан илрүүлэх системийг Линуксийн хамгаалалтын архитектуртай уялдуулах судалгааны чиглэлийг тодорхойлох шаардлагатай байна [3][5]. Ийнхүү энэ бүлэгт судалгааны ажлын ач холбогдол, зорилго, хүрээ, болон судалгааны үндэслэлийг тодорхойлон, дараагийн бүлэг болох Линуксийн аюулгүй байдлын архитектурын бүтэц хэсэгт онолын болон техникийн талаас гүнзгийрүүлэн шинжлэх суурийг тавина.

II. ЛИНУКСИЙН АЮУЛГҮЙ БАЙДЛЫН АРХИТЕКТУР

Линуксийн аюулгүй байдлын архитектур нь системийн найдвартай ажиллагаа, хэрэглэгчийн эрхийн удирдлага, нөөцийн хяналт, болон халдлагаас урьдчилан сэргийлэх бодлогоор тодорхойлогддог цогц бүтэц юм. Энэхүү архитектур нь цөмийн түвшин, хэрэглэгчийн орон зай, системийн үйлчилгээний түвшин гэсэн гурван үндсэн давхаргад хуваагдан, эдгээрийн уялдаа холбоо нь аюулгүй ажиллагааг бүрдүүлдэг [1][2][5]. Линукс нь нээлттэй эхийн шинж чанартай тул хамгаалалтын бүтэц нь ил тод, баталгаажсан стандартууд дээр тулгуурладаг

бөгөөд үүнд эрхийн загвар, нэвтрэлтийн хяналт, аюулгүй байдлын модулиуд, шифрлэлтийн дэд систем зэрэг бүрэлдэхүүн багтдаг.

A. Цөмийн түвшний хамгаалалтын бүтэц

Линуксийн цөм нь системийн хамгийн дээд түвшний эрхтэй орчин бөгөөд процесс, санах ой, оролт-гаралтын удирдлага, төхөөрөмжийн нөөц хуваарилалт, болон системийн дуудлагуудыг (system calls) хянадаг. Цөмийн түвшинд хэрэгждэг хамгаалалт нь мэдээллийн тусгаарлалт (isolation) болон эрхийн хязгаарлалт (privilege control) гэсэн хоёр гол зарчимд тулгуурладаг. Цөмийн хамгаалалтын үндсэн механизм нь Discretionary Access Control (DAC) бөгөөд энэ нь хэрэглэгчид болон бүлгийн түвшинд файлын эзэмшил, зөвшөөрлийг хянадаг. DAC нь UNIX-ийн уламжлалт эрхийн загвар болох “rwx” (унших, бичих, гүйцэтгэх) зөвшөөрлийн системийг үндэс болгодог. Гэвч DAC нь хэрэглэгчийн хяналттай тул халдлагын үед эзэмшигчийн эрхийг ашиглах боломжтой сул талтай байдаг [3].

Энэхүү хязгаарлалтыг шийдвэрлэх зорилгоор Mandatory Access Control (MAC) загварыг нэвтрүүлж, системийн түвшинд урьдчилан тодорхойлсон бодлогын дагуу нэвтрэлтийг хянах боломж бүрдүүлсэн. MAC загварыг хэрэгжүүлэгч гол технологиуд нь Security-Enhanced Linux (SELinux) болон AppArmor бөгөөд эдгээр нь цөмийн түвшинд хэрэгждэг хандалтын удирдлагын модуль юм [2][6]. SELinux нь бодлогын хяналт (policy enforcement)-д тулгуурлан процесс бүрт тодорхой эрхийн хүрээ оноодог бол AppArmor нь файл болон сүлжээний түвшинд илүү уян хатан хандалт хэрэгжүүлдэг. Нэмж дурдахад, Seccomp (Secure Computing Mode) нь процессын системийн дуудлагыг хязгаарлаж, зөвхөн тодорхой API болон санах ойн хандалтыг зөвшөөрдөг хамгаалалтын түвшин юм. Энэ нь контейнер болон микросервисийн орчинд хэрэглэгддэг хамгаалалтын үр ашигтай шийдэл бөгөөд Docker, Kubernetes зэрэг платформуудын үндсэн хамгаалалтын бүрэлдэхүүнд багтдаг. Цөмийн түвшинд ашиглагддаг өөр нэг чухал хэрэгсэл нь Linux Security Module (LSM) хэмээх дэд систем бөгөөд энэ нь SELinux, AppArmor, Smack зэрэг модулиудыг нэгтгэж, аюулгүй байдлын өргөтгөлүүдийг цөмийн түвшинд уялдуулах боломжийг олгодог. LSM-ийн архитектур нь уян хатан, модульчлагдсан бүтэцтэй тул хөгжүүлэгчдэд өөрийн хамгаалалтын модулийг нэмэлтээр хэрэгжүүлэх боломжийг бүрдүүлдэг [5].

B. Хэрэглэгчийн орон зайн хамгаалалт ба нэвтрэлтийн хяналт

Линуксийн хэрэглэгчийн орон зай нь цөмийн нөөцтэй шууд харилцдаггүй, харин системийн дуудлагаар дамжуулан үйлдэл гүйцэтгэдэг хамгаалалттай орчин юм. Энэхүү давхаргад хэрэглэгчийн эрхийн хуваарилалт, танилт болон баталгаажуулалтын механизм, системийн бүртгэл ба аудитын хяналт хэрэгждэг. Pluggable Authentication Module (PAM) нь хэрэглэгчийн нэвтрэлтийн процессыг удирддаг бөгөөд олон төрлийн баталгаажуулалтын системийг нэгтгэн ашиглах боломжийг олгодог. PAM нь төвлөрсөн хандалтын

бодлого хэрэгжүүлэх боломжийг бүрдүүлдэг тул системийн нэвтрэлтийн уялдааг сайжруулж, хэрэглэгчийн танилтын алдаа, олон шатлалт баталгаажуулалт (MFA)-ыг дэмждэг [4]. Системийн бүртгэл болон аудитын хяналтын үүргийг auditd буюу Линуксийн аудитын дэд систем гүйцэтгэдэг. Auditd нь цөмийн түвшинд хийгдсэн үйлдэл бүрийг бүртгэж, аюулгүй байдлын зөрчлийг илрүүлэх, мөрдөн шалгах, бодит цагийн хяналт хийхэд ашиглагддаг. Энэ нь илрүүлэлтийн системүүдтэй (IDS/IPS) хамтран ажиллах боломжтой тул хамгаалалтын системийн ил тод байдлыг хангадаг.

C. Сүлжээний түвшний хамгаалалт ба шифрлэлтийн дэд систем

Линуксийн архитектур нь сүлжээний түвшинд iptables, nftables, болон firewalld зэрэг дотоод галт ханын хэрэгслүүдийг ашиглан оролт, гаралтын урсгалыг хянадаг. Эдгээр хэрэгслүүд нь дүрэмд суурилсан хандалт хянах системийг хэрэгжүүлж, порт, протокол, хостын түвшинд урсгалын хяналт явуулах боломжийг олгодог. Firewalld нь динамик дүрэм ашиглан системийн бодит цагийн урсгалыг өөрчлөх чадвартай тул орчин үеийн серверийн орчинд өргөн ашиглагддаг [2][6]. Шифрлэлтийн дэд системийн хувьд Линукс нь Cryptographic API-аар дамжуулан олон төрлийн симметрик болон асимметрик шифрлэлтийн алгоритмийг дэмждэг. Энэхүү дэд систем нь SSL/TLS, SSH, IPsec зэрэг протоколуудыг хэрэгжүүлэх үндэс суурь болдог бөгөөд системийн өгөгдөл дамжуулалт, файлын системийн түвшний шифрлэлтийг дэмждэг. Шифрлэлтийн цөмийн дэмжлэг нь модуль хэлбэрээр өргөтгөж болох ба харьцангуй өндөр гүйцэтгэлтэй, бага нөөц зарцуулалттай байхаар оновчлогдсон байдаг [5].

D. Контейнер болон виртуал орчны хамгаалалт

Орчин үеийн Линукс системүүдийн архитектур нь контейнер болон виртуалчлалд суурилсан орчныг өргөн ашиглаж байгаа тул хамгаалалтын хандлага илүү нарийн түвшинд хөгжиж байна. Контейнерийн түвшинд Namespaces, Control Groups (cgroups), болон Capabilities зэрэг дотоод механизм нь процессын тусгаарлалт, нөөцийн хязгаарлалт, болон эрхийн нарийвчлалын хяналтыг хэрэгжүүлдэг. Namespaces нь процесс бүрийн сүлжээ, файл систем, хэрэглэгчийн ID зэрэг орчныг тусгаарлаж, системийн нөөц хоорондын хандалтыг хязгаарладаг. Cgroups нь CPU, санах ой, дискний орон зай зэрэг нөөцийн хэрэглээг хянаж, системийн ачааллыг жигд хуваарилахад тусалдаг бол Capabilities нь процессын түвшинд системийн эрхийг хувааж, зөвхөн шаардлагатай эрхийг олгох зарчмыг хэрэгжүүлдэг. Эдгээр хамгаалалтын механизмуудыг Docker, Podman, Kubernetes зэрэг контейнерийн технологи дотооддоо ашигладаг бөгөөд энэ нь системийн найдвартай байдлыг хадгалах, халдлагаас тусгаарлах, болон процесс хоорондын нөлөөллийг бууруулахад онцгой ач холбогдолтой [6].

Линуксийн аюулгүй байдлын архитектур нь олон түвшний хамгаалалтын зарчимд тулгуурладаг бөгөөд цөмийн түвшнээс хэрэглэгчийн түвшин, сүлжээний

орчин, болон контейнерийн орон зай хүртэл уялдаа холбоотой ажилладаг. Цөмийн модуль, нэвтрэлтийн хяналт, шифрлэлтийн дэд систем, болон галт ханын бүрэлдэхүүнүүд нь хамтдаа системийн найдвартай ажиллагааг хангах үндсэн тулгуур болдог. Энэ бүтэц нь нээлттэй эхийн орчны ил тод байдлыг алдагдуулахгүйгээр хамгаалалтын хатуу бодлого хэрэгжүүлэх боломжийг олгож байгаа бөгөөд дараагийн бүлэгт Линуксийн эмзэг байдлын ангилал, төрлүүд, тэдгээрийн шинж чанарыг судлан авч үзнэ.

III. ЛИНУКСИЙН ЭМЗЭГ БАЙДЛЫН АНГИЛАЛ

Линуксийн аюулгүй байдлын түвшин нь системийн бүтэц, хөгжүүлэлтийн загвар, хэрэглэгчийн орчны тохиргоо, болон гуравдагч программ хангамжийн найдвартай байдлаас шууд хамаардаг. Эмзэг байдал нь эдгээр түвшний аль нэгэнд үүссэн логик, архитектурын, эсвэл хэрэгжилтийн алдаанаас шалтгаалан халдагчид системийн нөөцөд хандалт авах, хортой код ажиллуулах, эсвэл эрх өсгөх боломж олгодог. Линуксийн эмзэг байдлыг системийн бүтэц, нөлөөллийн түвшин, болон халдлагын төрөл гэсэн гурван үндсэн хэмжүүрийн дагуу ангилж болно [1][2][4].

A. Кернелийн түвшний эмзэг байдал

Линуксийн цөм (kernel) нь системийн нөөцийг удирдах төв бүрэлдэхүүн бөгөөд цөмийн түвшинд үүссэн эмзэг байдал нь хамгийн ноцтой нөлөөлөлтэй байдаг. Цөмийн түвшний алдаа нь халдагчид эрхийн дээд түвшний хандалт авах буюу root эрхийг олж авах нөхцөлийг бүрдүүлдэг бөгөөд энэ нь системийн бүрэн бүтэн байдал, нууцлал, хүртээмжид шууд нөлөөлдөг [5][6]. Хамгийн түгээмэл цөмийн эмзэг байдлын жишээнд санах ойн гэмтэл (memory corruption), өрсөлдөөнт нөхцөл (race condition), хүчингүй заагч (null pointer dereference), болон buffer overflow зэрэг алдаанууд ордог. Эдгээр нь системийн дотоод дэд бүтцийн буруу хандалт, орон зайн хяналт алдагдсанаас үүдэлтэй бөгөөд халдагч үүнийг ашиглан дурын код ажиллуулах, системийн санах ойд шууд хандалт хийх боломжтой болдог [3][9]. Жишээлбэл, CVE-2025-21863 нь Линуксийн цөмийн санах ойн удирдлагын дэд системд илэрсэн эрхийн түвшний доголдол бөгөөд халдагчид root эрх олж авах боломжийг олгосон ноцтой эмзэг байдал юм. Энэ төрлийн алдаа нь ихэвчлэн буруу хандалтын шалгалт, хязгаарлалтгүй санах ойн ашиглалт, эсвэл системийн дуудлагын гүйцэтгэлд гарсан логик зөрчлөөс үүддэг. Цөмийн эмзэг байдлыг илрүүлэх нь өндөр төвөгтэй процесс бөгөөд эх кодын гүн түвшинд дүн шинжилгээ хийх шаардлагатай байдаг. Статик анализ болон динамик хяналтын хэрэгслүүдийг хослуулан ашигласнаар илрүүлэлтийн нарийвчлалыг нэмэгдүүлэх боломжтой ч халдлагын шинэ хэлбэрүүд тасралтгүй гарч буй нөхцөлд бүрэн хамгаалалт хангах нь хүндрэлтэй хэвээр байна [2][5].

B. Хэрэглэгчийн орон зайн эмзэг байдал

Хэрэглэгчийн орон зайн (user space) эмзэг байдал нь системийн цөмөөс гадуур ажилладаг программ, сан, болон үйлчилгээний түвшинд илэрдэг. Эдгээр эмзэг

байдал нь ихэвчлэн программчлалын алдаа, буруу тохиргоо, эсвэл нууцлалын буруу хэрэгжилттэй холбоотой байдаг. Ийм эмзэг байдлын түгээмэл жишээнд буруу оролтын шалгалт (input validation flaw), форматын мөрийн алдаа (format string bug), SQL injection, command injection, болон нууц үгийн буруу хадгалалт зэрэг орно [4][6]. Энэ төрлийн сул талууд нь хэрэглэгчийн программ болон системийн үйлчилгээнд халдвар оруулах замаар халдагчид системийн дотоод орчинд хяналт тогтоох нөхцөл бүрдүүлдэг. Хэрэглэгчийн орон зайн эмзэг байдлын сүүлийн үеийн тод жишээ бол CVE-2025-32463 бөгөөд энэ нь Линуксийн хэрэглэгчийн орчны санах ойн удирдлагын доголдоос үүдэлтэй, халдагчид дурын код ажиллуулах боломж олгосон эмзэг байдал юм [10]. Энэ төрлийн алдаа нь ихэвчлэн буруу хаяг заалт, аюулгүй бус санах ойн менежмент, эсвэл оролтын шалгалт хангалтгүй байсантай холбоотой байдаг. Хэрэглэгчийн орон зайн хамгаалалтыг хангахын тулд программын эх кодын аудит, системийн тохиргооны бодлого, болон sandbox орчинд суурилсан хязгаарлалт зайлшгүй шаардлагатай. Хэрэв програмуудыг зөв тусгаарлаж, нэвтрэлтийн бодлого нарийн хэрэгжүүлбэл хэрэглэгчийн орон зайн халдлагын эрсдэлийг мэдэгдэхүйц бууруулах боломжтой [2][4].

C. Сүлжээ болон системийн түвшний эмзэг байдал

Сүлжээний түвшний эмзэг байдал нь системийн холболт, протоколын хэрэгжилт, болон галт ханын буруу тохиргооноос үүдэлтэй байдаг. Линуксийн галт ханын дүрэм буруу тодорхойлогдсон, портын хандалт илүү нээлттэй, эсвэл шифрлэлтийн протокол хуучирсан тохиолдолд халдагч системийн сүлжээнд нэвтрэх боломжтой болдог [8].

Ийм төрлийн эмзэг байдал нь ихэвчлэн дараах хэлбэртэй илэрдэг:

- SSH эсвэл FTP үйлчилгээний сул шифрлэлтийн тохиргоо
- TLS/SSL протоколын буруу хэрэгжилт
- Хуучин SSH түлхүүр ашиглалт
- Галт ханын дүрмийн давхардал, хяналтгүй портууд
- Сүлжээний буруу замчлал болон NAT тохиргоо

Сүлжээний эмзэг байдал нь халдлагын анхны шатанд ашиглагдах хандалтын цэг болж, дотоод системүүдийн хамгаалалтыг тойрон гарахад ашиглагддаг. CSA Singapore [8]-ийн анхааруулгад дурдсанаар, орчин үеийн хортой код болон ransomware халдлагын ихэнх нь сүлжээний түвшинд үүссэн тохиргооны алдааг ашиглан дотоод системд нэвтрэх байгаа нь тогтоогдсон. Системийн түвшинд мөн зөвшөөрөл буруу хуваарилах, файлын системийн хамгаалалт сул байх, логийн хяналтгүй байдал, болон хэрэглэгчийн эрхийн буруу удирдлага зэрэг алдаа түгээмэл тохиолддог. Эдгээр асуудал нь халдлагын дараах шатанд эрх өсгөх, өгөгдөл устгах, системийн бүртгэл өөрчлөх зэрэг үйлдэлд ашиглагддаг [4][6].

D. IoT болон суулгагдсан системийн эмзэг байдал

Линуксийн цөмийг ашигладаг IoT төхөөрөмжүүд нь хөнгөн жинтэй, нөөцийн хувьд хязгаарлагдмал архитектуртай байдаг тул хамгаалалтын шинэчлэл тогтмол хийгдэхгүй байх хандлагатай. Sternum IoT [1][4]-ийн судалгаанд дурдсанаар IoT төхөөрөмжүүдийн 60 гаруй хувь нь анхдагч нууц үгтэй, эсвэл программ хангамжийн нөхөөс хийгдээгүй байдлаар ажилладаг нь кибер халдлагын үндсэн эх үүсвэр болж байна.

Суулгагдсан системүүдийн эмзэг байдал нь дараах хүчин зүйлсээр тодорхойлогддог

- Кернелийн хуучин хувилбар ашиглах
- Firmware шинэчлэл дутмаг байх
- Алсын удирдлагын (remote management) интерфейс хамгаалагдаагүй байх
- Шифрлэлтийн хэрэгжилт сул байх
- Default тохиргоог өөрчлөлгүй орхих

Эдгээр сул талууд нь IoT болон embedded системийг botnet-ийн нэг хэсэг болгон ашиглах, DDoS халдлагад оролцуулах, эсвэл мэдээлэл хулгайлахад хүргэдэг. Mirai, Mozi зэрэг ботнетүүдийн халдлагаас харахад хамгаалалтын шинэчлэл хийгдээгүй Линукс төхөөрөмжүүд хамгийн эмзэг зорилтот бүлэг хэвээр байна [6].

E. Эмзэг байдлын нөлөөллийн ангилал

Линуксийн эмзэг байдлыг нөлөөллийн шинж чанараар нь нууцлал (confidentiality), бүрэн бүтэн байдал (integrity), болон хүртээмж (availability) гэсэн гурван үндсэн шалгуураар ангилдаг. Энэ гурван шалгуур нь CVSS (Common Vulnerability Scoring System)-ийн суурь үзүүлэлт бөгөөд эмзэг байдлын хор уршгийг тоон утгаар тодорхойлох боломж олгодог.

- Нууцлалд нөлөөлөх эмзэг байдал нь системийн мэдээллийг зөвшөөрөлгүй этгээдэд алдагдуулах, уншуулах, эсвэл хуулбарлуулахад хүргэдэг.
- Бүрэн бүтэн байдалд нөлөөлөх эмзэг байдал нь өгөгдөл өөрчлөгдөх, устах, эсвэл системийн бүртгэлд хөндлөн оролцох эрсдэлийг агуулдаг.
- Хүртээмжид нөлөөлөх эмзэг байдал нь системийн үйл ажиллагаа тасалдах, үйлчилгээний саатал үүсэх, эсвэл DDoS төрлийн халдлагад өртөх нөхцөлийг бүрдүүлдэг [5][8][9].

Эдгээр шалгуур үзүүлэлтүүдийг уялдуулан үнэлэх нь хамгаалалтын нөөцийг оновчтой хуваарилах, илрүүлэлтийн дарааллыг тодорхойлох, болон хамгаалалтын стратегийг давхар түвшинд хэрэгжүүлэхэд тусалдаг. Линуксийн эмзэг байдал нь архитектурын бүх түвшинд үүсч болох бөгөөд цөм, хэрэглэгчийн орон зай, сүлжээний орчин, болон суулгагдсан системийн аль ч бүрэлдэхүүн халдлагын зорилт болж чаддаг. Эдгээрийг ангилан судалснаар илрүүлэлтийн арга зүйг нарийвчлан боловсруулах, хамгаалалтын давхаргыг зөв оновчлох боломж бүрдэнэ. Цаашид дараагийн бүлэгт Линуксийн эмзэг байдлыг илрүүлэх аргуудыг системчилж, статик,

динамик болон гибрид илрүүлэлтийн аргачлалыг судлан дүн шинжилгээ хийнэ.

IV. ЛИНУКСИЙН ЭМЗЭГ БАЙДЛЫГ ИЛРҮҮЛЭХ АРГУУД

Линуксийн үйлдлийн системд үүсдэг эмзэг байдлыг илрүүлэх нь системийн хамгаалалтын үйл ажиллагааны үндсэн бүрэлдэхүүн бөгөөд илрүүлэлтийн үр дүн нь цаашдын нөхөөс, хариу арга хэмжээ, хамгаалалтын төлөвлөлтөд шууд нөлөөлдөг. Эмзэг байдлын илрүүлэлтийг хэрэгжүүлэхэд статик шинжилгээ, динамик шинжилгээ, урсгалд суурилсан хяналт, машин сургалтын арга, болон эдгээрийг уялдуулсан гибрид хандлага өргөн хэрэглэгддэг. Арга бүрийн хэрэгжилт, нарийвчлал, болон гүйцэтгэл нь системийн орчны онцлогоос хамаарч өөр өөр байдаг [2][3][5].

A. Статик шинжилгээ (Static Analysis)

Статик шинжилгээ нь эх код, хоёртын гүйцэтгэх файл, эсвэл программын бүтцийн мэдээлэлд үндэслэн эмзэг байдлыг илрүүлэх арга юм. Энэхүү арга нь програм ажиллуулах шаардлагагүй бөгөөд программын логик, өгөгдлийн урсгал, оролтын шалгалт, санах ойн менежмент зэрэг элементүүдийг шинжилж, боломжит алдааг илрүүлдэг. Static Application Security Testing (SAST) хэрэгслүүд нь аюулгүй байдлын дүрмийн сан ашиглан эх код дахь буруу оролтын шалгалт, заагчийн алдаа, давталтын логикийн доголдол, нууц мэдээллийн буруу хадгалалт зэрэг асуудлыг илрүүлдэг. Түгээмэл хэрэглэгддэг хэрэгслүүдэд Clang Static Analyzer, Cppcheck, SonarQube, Lynis зэрэг ордог [3][5]. Статик шинжилгээний гол давуу тал нь хөгжүүлэлтийн эхний шатанд алдааг илрүүлж, засварлах боломж олгодогт оршдог. Гэвч энэ арга нь runtime орчин дахь нөхцөлт зан төлөвийг (behavior) загварчилж чаддаггүй, мөн false positive буюу ташаа илрүүлэлтийн магадлал өндөр байдаг. Иймээс үр дүнг гар аргаар баталгаажуулах шаардлагатай бөгөөд энэ нь шинжилгээний хугацаа, нөөцийн хэрэглээг нэмэгдүүлдэг [5][9].

B. Динамик шинжилгээ ба фуззинг (Dynamic Analysis and Fuzzing)

Динамик шинжилгээ нь программын гүйцэтгэлийн явцад гарч буй үйлдлийг ажиглаж, бодит ажиллах орчинд илрэх эмзэг байдлыг илрүүлэх арга юм. Энэхүү хандлага нь санах ойн эвдрэл, оролтын буруу боловсруулалт, нөөцийн хуваарилалт, процессын урсгалын доголдол зэрэг runtime түвшний эмзэг байдлыг тодорхойлох чадвартай. Динамик шинжилгээнд Valgrind, AddressSanitizer (ASan), Kernel AddressSanitizer (KASAN) зэрэг хэрэгслүүд өргөн хэрэглэгддэг. Эдгээр нь цөмийн модуль болон хэрэглэгчийн орон зайн кодын санах ойн хэрэглээ, хандалтын заагийг хянаж, буруу хаяг заалт болон use-after-free төрлийн алдааг илрүүлдэг. Фуззинг (Fuzz Testing) нь программын оролтод автоматаар үүсгэсэн санамсаргүй эсвэл гажуудсан өгөгдлийг шахаж, системийн хариу үйлдлийг ажиглах туршилтын арга юм. Энэ арга нь программ гацах, хариу өгөхгүй болох, эсвэл системийн нөөцийг буруу удирдах зэрэг шинж тэмдгээр эмзэг байдлыг тодорхойлдог. AFL (American Fuzzy Lop), honggfuzz, libFuzzer зэрэг

хэрэгслүүд нь Линуксийн орчинд хамгийн түгээмэл хэрэглэгддэг бөгөөд цөмийн болон хэрэглэгчийн түвшний тестэд адил үр дүнтэй ажилладаг [3][5][9]. Динамик шинжилгээ нь статик анализын сул талыг нөхдөг ч нөөцийн хэрэглээ их, автоматжуулалт хязгаарлагдмал, мөн гүйцэтгэлийн орчны тохиргоо төвөгтэй байдаг. Тиймээс динамик болон статик анализыг уялдуулсан hybrid илрүүлэлтийн систем илүү үр ашигтайд тооцогддог.

C. Урсгалд суурилсан болон логийн шинжилгээ (Flow-Based and Log Analysis)

Сүлжээ болон системийн урсгалд суурилсан илрүүлэлт нь өгөгдлийн урсгалын загвар, сүлжээний хүсэлт, процессын зан төлөв, системийн бүртгэлийн өгөгдлийг дүн шинжилгээнд ашигладаг. Энэхүү арга нь аномали илрүүлэх (anomaly detection) зарчмыг хэрэгжүүлж, хэвийн бус урсгал, логийн зөрчил, системийн үйлдлийн хэт их давтамж зэрэг үзүүлэлтүүдийг илрүүлэх боломж олгодог [1][6][8]. Линуксийн auditd болон syslog бүртгэлийн системүүд нь системийн үйлдэл, хэрэглэгчийн нэвтрэлт, процессын үүсэлт зэрэг бүх үйл ажиллагааг хянаж, SIEM (Security Information and Event Management) платформуудтай уялдуулан бодиг цагийн шинжилгээ хийхэд ашиглагддаг. ELK Stack (Elasticsearch, Logstash, Kibana) болон Splunk зэрэг системүүд нь логийн төвлөрсөн анализ хийж, халдлагын хэв маягийг илрүүлэх, эмзэг байдлын шалтгааныг тодорхойлох боломжийг бүрдүүлдэг [3][8]. Гэвч урсгалд суурилсан илрүүлэлт нь их хэмжээний өгөгдөл боловсруулах шаардлагатай тул өндөр нөөц зарцуулдаг. Иймээс автоматжсан дэд бүтэц, өгөгдлийн урьдчилсан цэвэрлэгээ, дүрмийн оновчлол зайлшгүй шаардлагатай болдог [10].

D. Машин сургалтад суурилсан илрүүлэлт (Machine Learning-Based Detection)

Сүүлийн жилүүдэд машин сургалтын арга нь эмзэг байдлын илрүүлэлтэд нэвтэрч, зан төлөвийн шинжилгээ, логийн хэв маяг, системийн аномали илрүүлэлтэд өндөр үр ашигтай болох нь нотлогдсон [3][5]. Линуксийн системийн логи, процессын хандалтын загвар, хэрэглэгчийн үйлдлийн давтамж зэрэг мэдээлэлд суурилан supervised болон unsupervised загварууд ашиглагдаж байна. Жишээлбэл, шийдвэрийн мод (Decision Tree), санамсаргүй ой (Random Forest), нейрон сүлжээ (Neural Network), болон SVM зэрэг алгоритмуудыг ашиглан системийн үйлдлийн хэвийн бус зан төлөвийг илрүүлэх боломжтой. Энэ төрлийн арга нь шинэ төрлийн халдлагын аюулыг урьдчилан илрүүлэх давуу талтай ч сургалтын өгөгдлийн чанар, загварын тайлбарлах чадвар, мөн нөөцийн хэрэглээ нь хязгаарлалт болдог [5]. Машин сургалтын аргыг илүү найдвартай болгохын тулд дүрмийн загвартай хослуулах буюу hybrid anomaly detection загварыг хэрэгжүүлэх нь үр дүнтэй. Энэ тохиолдолд ML систем нь урьдчилсан анхааруулга илрүүлж, цаашид дүрмийн болон статик анализын шалгалтыг автоматаар эхлүүлэх боломж бүрддэг.

E. Гибрид илрүүлэлтийн стратеги (Hybrid Detection Strategy)

Гибрид илрүүлэлтийн систем нь статик, динамик, урсгалын болон машин сургалтын арга зүйг нэгтгэн, илрүүлэлтийн үр нөлөө болон нарийвчлалыг дээшлүүлдэг. Энэ хандлага нь эхлээд урсгалын түвшинд аномали илрүүлж, дараа нь тухайн үйлдлийг статик эсвэл динамик шинжилгээнд автоматаар дамжуулах pipeline бүтэцтэй байдаг [5][10]. CI/CD орчинд гибрид илрүүлэлтийг хэрэгжүүлэх нь хөгжүүлэлтийн явцад эмзэг байдлыг эрт илрүүлэх, тестийн автоматжуулалтыг сайжруулах, нөхөөсийн хугацааг богиносгох давуу талтай. Мөн илрүүлэлтийн үр дүнг SIEM системд нэгтгэснээр бодит цагийн хяналт, эрэмбэлэлт, хариу арга хэмжээний давтамж илүү үр ашигтай болдог [9].

F. Хязгаарлалт ба практик хэрэгжилт

Бүх төрлийн илрүүлэлтийн арга нь өөрийн онцлог болон хязгаарлалтад тулгуурладаг. Статик шинжилгээ хурдан боловч runtime зан төлөвийг илрүүлэх чадваргүй, динамик шинжилгээ бодит гүйцэтгэлийг харуулдаг ч нөөцийн хэрэглээ өндөр, машин сургалт үр ашигтай ч сургалтын өгөгдлийн чанарт хэт хамааралтай байдаг. Иймээс практик орчинд олон төрлийн аргыг уялдуулсан, тасралтгүй сайжруулалт бүхий автоматжуулсан илрүүлэлтийн дэд бүтэц хамгийн оновчтой шийдэлд тооцогддог [3][5][10].

Линуксийн эмзэг байдлын илрүүлэлтийн арга зүй нь технологийн дэвшил, системийн төвөгшил, болон халдлагын хэлбэрийн хувьслын дагуу тасралтгүй хөгжиж байна. Статик, динамик, урсгалд суурилсан болон машин сургалтын аргуудыг нэгдсэн гибрид архитектурт уялдуулснаар илрүүлэлтийн нарийвчлал, хариу үйлдлийн хугацаа, системийн найдвартай байдал мэдэгдэхүйц дээшилдэг. Илрүүлэлтийн систем нь зөвхөн аюул илрүүлэхээс гадна хамгаалалтын бодлого боловсруулах, нөхөөсийн дарааллыг тодорхойлох, болон урьдчилан сэргийлэх хамгаалалтыг төлөвлөхөд чухал стратегийн ач холбогдолтой.

V. ЛИНУКСИЙН ЭМЗЭГ БАЙДЛЫГ ХАМГААЛАХ БА БУУРУУЛАХ АРГАЧЛАЛ

Линуксийн аюулгүй байдлыг хамгаалах болон эмзэг байдлыг бууруулах стратеги нь системийн архитектурын түвшин, хэрэглэгчийн орон зай, сүлжээний давхарга, болон хэрэглээний бодлогын хүрээнд уялдаа холбоотой хэрэгжих шаардлагатай. Хамгаалалтын үр ашиг нь зөвхөн технологийн шийдэл бус, системийн зохион байгуулалт, хяналтын бодлого, шинэчлэлтийн менежмент, болон хэрэглэгчийн сахилга баттай шууд холбоотой байдаг [1][2][5]. Иймд хамгаалалтын тогтолцоог зөвхөн нэг түвшинд бус, олон давхар хамгаалалтын зарчмаар буюу “defense in depth” хандлагаар хэрэгжүүлэх нь хамгийн оновчтой шийдэлд тооцогддог [4][6].

A. Цөмийн түвшний хамгаалалт (Kernel-Level Protection)

Цөмийн түвшинд хэрэгждэг хамгаалалтын арга хэмжээнүүд нь Линуксийн архитектурын суурийг бүрдүүлдэг бөгөөд халдлагын эсрэг хамгаалалтын хамгийн анхны шугам юм. Линуксийн цөмд Address Space Layout Randomization (ASLR) болон Non-

Executable Stack (NX bit) зэрэг хамгаалалтын механизм нэвтрүүлэгдсэн бөгөөд эдгээр нь халдагчийн санах ойн хаягийг урьдчилан таамаглах боломжийг хааж, буфер хэтрэлт болон санах ойн халдлагыг саармагжуулдаг. ASLR нь программ бүрийн гүйцэтгэлийн үед санах ойн хаягийг санамсаргүй байрлуулдаг бол NX bit нь код бус санах ойн хэсгийг гүйцэтгэхээс сэргийлдэг [3][5]. Мөн Stack Canary хамгаалалт нь санах ойн стек дээр хамгаалалтын хяналтын утга (sentinel value) байршуулснаар халдагч санах ойн хаягийг өөрчлөх үед системийн дохиоллыг идэвхжүүлдэг. Control Flow Integrity (CFI) технологи нь программын удирдлагын урсгалыг хамгаалж, кодын хуурамч салбарлалтыг илрүүлж зогсоодог. Цөмийн түвшинд хэрэгждэг Security-Enhanced Linux (SELinux) ба AppArmor модулиуд нь Mandatory Access Control (MAC)-ийн бодлогын хэрэгжилтийг хангаж, процесс тус бүрт хандалтын хүрээ, зөвшөөрөл, болон системийн дотоод нөөцөд хандалтын хязгаар тогтоодог. SELinux нь бодлогын суурь удирдлагыг хэрэгжүүлж, системийн хандалтын шийдвэрийг контекстийн түвшинд гаргадаг бол AppArmor нь хялбар тохиргоотой, файлын түвшний sandbox орчныг бий болгодог [2][6]. Нэмж дурдахад, Seccomp (Secure Computing Mode) нь процессын системийн дуудлагыг хязгаарлаж, зөвхөн урьдчилан тодорхойлсон API болон kernel function-д хандалт зөвшөөрдөг. Энэхүү механизм нь контейнерийн орчинд өргөн хэрэглэгдэж, халдлага цөмийн түвшинд дамжих эрсдэлийг мэдэгдэхүйц бууруулдаг [5].

B. Хэрэглэгчийн орон зай ба эрхийн удирдлагын хамгаалалт

Хэрэглэгчийн орон зайд үүсдэг аюулгүй байдлын гол эрсдэл нь буруу эрхийн хуваарилалт, тохиргооны доголдол, болон хэрэглэгчийн нэвтрэлтийн бодлогын сул хяналтаас үүдэлтэй байдаг. Эдгээрийг бууруулахын тулд Least Privilege Principle буюу “хамгийн бага эрхийн зарчим”-ыг хэрэгжүүлэх шаардлагатай. Энэ зарчим нь хэрэглэгч, процесс бүрт зөвхөн шаардлагатай хүрээний хандалтыг олгож, root эрхийн хэрэглээг хязгаарладаг. Pluggable Authentication Module (PAM) нь хэрэглэгчийн нэвтрэлт болон баталгаажуулалтын процессыг модульчлагдсан байдлаар удирддаг бөгөөд төвлөрсөн аюулгүй байдлын бодлого хэрэгжүүлэх боломжийг бүрдүүлдэг. PAM нь олон шатлалт баталгаажуулалт (Multi-Factor Authentication), хандалтын хугацааны хязгаарлалт, нэвтрэлтийн оролдлогын хяналт зэргийг дэмждэг [4]. Мөн auditd бүртгэлийн системийг идэвхжүүлснээр хэрэглэгчийн үйлдэл бүрийг хянах, эрхийн зөрчил, системийн өөрчлөлт, тохиргооны засварыг бүртгэх боломжтой болдог. Auditd-ийн логийг SIEM системтэй уялдуулснаар хэрэглэгчийн үйлдлийг илүү өргөн хүрээнд хянах, зөрчил илрэх үед автоматаар сэрэмжлүүлэх үйлдэл гүйцэтгэх боломж бүрдэнэ [8]. Хэрэглэгчийн түвшинд системийн итгэмжлэлтэй процессуудыг sandbox орчинд тусгаарлах, AppArmor болон seccomp профайлыг идэвхжүүлэх, шаардлагагүй үйлчилгээ болон daemon-уудыг

идэвхгүй болгох нь системийн халдлагын гадаргууг бууруулах үр дүнтэй арга юм [6].

C. Сүлжээний хамгаалалт ба системийн хяналт

Линуксийн сүлжээний хамгаалалт нь системийн оролт, гаралтын урсгалыг хянах, хортой холболтыг блоклох, болон зөвшөөрөлгүй сүлжээний нэвтрэлтийг зогсоох чиглэлд төвлөрдөг. Сүлжээний хамгаалалтын үндсэн хэрэгслүүдэд iptables, nftables, болон firewalld багтдаг. Эдгээр нь дүрэмд суурилсан хандалтын хяналт хэрэгжүүлж, порт, протокол, IP хаягийн түвшинд нарийн хязгаар тогтоодог [2][8]. nftables нь iptables-ийн дараагийн үеийн хувилбар бөгөөд илүү уян хатан синтакс, багц дүрмийн менежмент, бага нөөц зарцуулалттай байдлаараа давуу талтай. firewalld нь динамик дүрэм өөрчлөх боломжтой тул серверийн орчинд бодит цагийн хяналт хийхэд тохиромжтой. Сүлжээний түвшинд мөн Intrusion Detection and Prevention Systems (IDS/IPS) хэрэгжүүлж, сүлжээний урсгалын хэвийн бус зан төлөвийг илрүүлэх нь хамгаалалтын чухал бүрэлдэхүүн болдог. Snort, Suricata зэрэг IDS/IPS системүүд нь дүрэмд суурилсан болон аномали илрүүлэлтийн хосолсон загварыг ашиглаж, халдлагыг автоматаар илрүүлэх, блоклох чадвартай. Шифрлэлтийн түвшинд Линукс нь OpenSSL, GnuTLS, Libgcrypt зэрэг криптографийн дэд системийг ашиглан TLS/SSL, SSH, IPsec протоколуудыг хэрэгжүүлдэг. Эдгээр нь өгөгдөл дамжуулалтын нууцлалыг хангаж, сүлжээний түвшинд халдлагын эрсдэлийг бууруулдаг [5].

D. Системийн шинэчлэлт ба нөхөөсийн удирдлага

Линуксийн аюулгүй байдлын хамгийн чухал бүрэлдэхүүн бол patch management буюу нөхөөсийн удирдлагын тогтолцоо юм. Хамгаалалтын нөхөөс хоцорч хэрэгжих нь эмзэг байдлын хамгийн түгээмэл шалтгаануудын нэг бөгөөд системийн халдлагын амжилтыг нэмэгдүүлдэг [9][10]. Тиймээс системийг байнгын шинэчлэлд хамруулах, автомат шинэчлэлтийн механизмыг идэвхжүүлэх нь зайлшгүй шаардлагатай. dnf-automatic, unattended-upgrades зэрэг хэрэгслүүд нь шинэчлэлтийн процессыг автоматжуулж, CVE-ийн мэдээлэлд тулгуурлан нөхөөс татан суулгах чадвартай. Мөн Vulnerability Scanning болон Configuration Auditing хэрэгслүүд (жишээлбэл, OpenVAS, Lynis) ашиглан системийн эмзэг байдлын байдлыг тогтмол үнэлэх, илэрсэн асуудлыг нөхөөсийн менежменттэй холбох нь хамгаалалтын бодит үр нөлөөг нэмэгдүүлдэг [3][9].

E. Давхар хамгаалалтын стратеги (Defense-in-Depth Strategy)

Линуксийн орчинд хамгаалалтын давхар стратеги хэрэгжүүлэх нь системийн тогтвортой байдлыг баталгаажуулдаг. Энэ стратеги нь цөмийн түвшин, хэрэглэгчийн орон зай, сүлжээний орчин, хэрэглээний давхарга гэх мэт бүх түвшинд хамгаалалтын бодлого давхар хэрэгжүүлэхийг зорьдог [1][2][6]. Жишээлбэл, цөмийн түвшинд SELinux бодлого хэрэгжиж байхад хэрэглэгчийн орон зайд PAM ба auditd идэвхтэй байх, сүлжээний түвшинд firewalld болон IDS ажиллаж байх нь

халдлагын аль нэг түвшинд амжилттай нэвтрэх магадлалыг эрс бууруулдаг. Давхар хамгаалалтын хандлага нь “single point of failure”-ийг арилгаж, системийн найдвартай байдлыг нэмэгдүүлэхээс гадна халдлагын мөрийг илрүүлэх хугацааг богиносгодог.

Линуксийн хамгаалалтын тогтолцоо нь архитектурын бүх түвшинд уялдаа холбоотой хэрэгжих ёстой цогц систем юм. Цөмийн хамгаалалт нь суурь аюулгүй байдлыг хангаж, хэрэглэгчийн орон зай дахь эрхийн хяналт болон сүлжээний хамгаалалт нь халдлагын гадаргууг багасгадаг. Системийн шинэчлэл, нөхөөсийн удирдлага, болон давхар хамгаалалтын бодлого нь хамгаалалтын тасралтгүй байдлыг хангах үндсэн хүчин зүйл болдог. Хамгаалалтын эдгээр арга хэмжээг системчилж хэрэгжүүлэх нь Линуксийн нээлттэй эхийн орчны аюулгүй байдлыг дэмжихийн зэрэгцээ, байгууллагын мэдээллийн дэд бүтцийг урт хугацаанд тогтвортой хамгаалах суурь нөхцөлийг бүрдүүлнэ.

VI. СУДАЛГААНЫ АРГА ЗҮЙ БОЛОН ҮР ДҮН

Судалгааны зорилго нь Линукс үйлдлийн системийн эмзэг байдлыг бодит туршилтын орчинд илрүүлэх, хамгаалах болон нөхөөсийн удирдлагын үр нөлөөг тоон болон чанарын үзүүлэлтээр үнэлэхэд чиглэнэ. Туршилтыг 24 цагийн дотор тасралтгүй горимд, үйлдвэрлэлийн орчныг дууриасан лабораторийн нөхцөлд гүйцэтгэсэн. Арга зүйн хувьд хосолсон буюу нэгдмэл арга барил хэрэглэгдэж, онолын судалгаа, туршилтын шинжилгээ болон тоон дүн шинжилгээний уялдаа бүхий хандлага хэрэгжүүлсэн.

I. Илрүүлэлтийн үе шат

Эхний шатанд Линуксийн хамгаалалтын архитектур, эмзэг байдлын ангилал болон илрүүлэлтийн арга зүйг судалж онолын үндсийг тодорхойлж, дараагийн шатанд серверийн орчныг загварчилж халдлагын төрөл, хамгаалалтын арга, илрүүлэлтийн үр нөлөөг туршилтаар шалгасан. Туршилтын орчин нь дотоод LAN сегмент (192.0.2.0/24)-тэй бөгөөд:

- MikroTik RouterOS 7.14 замчлагч(router) дээр nftables идэвхтэй байхаар тохируулсан.
- Ubuntu Server 22.04 LTS дээр Apache 2.4.x, OpenSSH 9.x, MariaDB 10.6 зэрэг үйлчилгээ ажиллуулсан.
- Халдагч хост нь Kali Linux 2024.3 системтэй бөгөөд
- Metasploit, Nmap, Hydra, sqlmap, wfuzz зэрэг хэрэгсэл ашигласан.
- Аюулгүй байдлын хяналт, илрүүлэлт болон бүртгэлийг хангах зорилгоор Lynis, OpenVAS, auditd, Suricata, fail2ban, OpenSCAP, osquery зэрэг хэрэгсэл ELK Stack (Filebeat → Logstash → Elasticsearch → Kibana)-ийн бүртгэлийн системтэй уялдуулан ашигласан.
- Туршилтын орчны бүтэц нь веб сервер, өгөгдлийн сан, SSH үйлчилгээ, галт ханын хамгаалалт болон логийн бүртгэлийг

нэгтгэсэн цогц экосистемийг бүрдүүлсэн.

Анхан шатны шинжилгээний үе шатанд OpenVAS болон Lynis хэрэгслүүдийг ашиглан системийн анхны төлөвийг тодорхойлсон. Үүнд:

- Нийт 17 эмзэг байдал илэрч, тэдгээрийн 5 нь Critical, 8 нь High, 4 нь Medium түвшинд үнэлэгдсэн.
- Lynis-ийн аюулгүй байдлын оноо 71/100 байсан нь хуучин SSH тохиргоо, сул SSL cipher болон идэвхгүй auditd-тэй холбоотой гэж дүгнэгдсэн.
- Халдлагын туршилтын шатанд SSH brute-force оролдлогыг Hydra хэрэгслээр 20 түлхүүрийн жагсаалтаар гүйцэтгэхэд 60 секундын дотор амжилттай нэвтрэлт бүртгэгдсэн.
- SQL injection туршилтыг sqlmap хэрэгслээр Apache веб аппликейшн дээр хийж, 18 хувийн амжилтын түвшинтэй гарсан.
- Nmap сканер ашиглан 80, 443, 22, 3306 зэрэг нийт долоон порт нээлттэй болох нь илэрсэн.

Туршилтын хугацаанд хэрэглэсэн нийт программ хангамж, аюулгүй байдлын хэрэгслүүдийг доорх хүснэгтэд харууллаа:

1-Р ХҮСНЭГТ ТУРШИЛТАД АШИГЛАСАН ПРОГРАММ ХАНГАМЖ БА АЮУЛГҮЙ БАЙДЛЫН ХЭРЭГСЛҮҮД

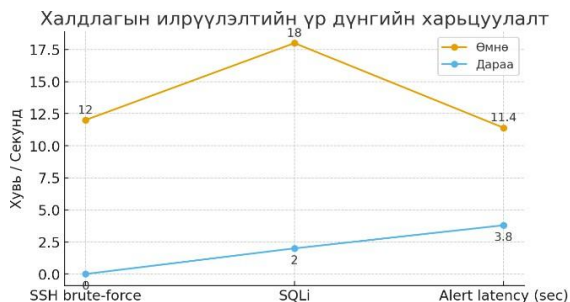
Нэр	Төрөл	Хувилбар / Тохиргоо	Зориулалт / Ашиглалт
OpenVAS (gvm)	Эмзэг байдлын сканер	GVM 23.x (2025)	CVE эмзэг байдлын илрүүлэлт ба үнэлгээ
Lynis	Системийн аудит	Stable (2024)	Конфигурацийн аудит, хатууруулалтын н зөвлөмж
Suricata	Сүлжээний IDS/IPS	Suricata (EVE JSON output)	Халдлагын урсгалыг илрүүлэх, real-time alert үүсгэх
ELK Stack	Логийн удирдлага ба анализ	Filebeat / Logstash / Elasticsearch / Kibana	Логийг цуглуулах, индекстэх, dashboard-т харагдуулах
fail2ban	Хост түвшний хамгаалалт	Systemd integration	SSH brute-force оролдлогог блоклох
ModSecurity + OWASP CRS	Вэб аппликейшн галт хана (WAF)	Apache plugin + OWASP CRS	SQLi, XSS зэрэг вэб халдлагаас хамгаалах
unattended-upgrades	Нөхөөсийн удирдлага	Ubuntu APT package	CVE нөхөөсийг автомат татаж суулгах
Metasploit Framework	Exploitation / PoC	Framework 6.x	Эмзэг байдлын тест, ёс зүйн хязгаартай туршилт
Nmap	Сүлжээний сканер	Stable 7.x	Port scan, service detection
Hydra	Нууц үг туршигч (Bruteforce tool)	THC-Hydra	SSH болон FTP үйлчилгээний brute-force туршилт
sqlmap	SQL injection шалгагч	sqlmap (latest)	Вэб аппликейшнд SQLi туршилт

wfuzz	Вэб фуззинг хэрэгсэл	wfuzz	Вэб оролтын фуззинг, директори хайлт
auditd	Kernel аудит	auditd (Ubuntu service)	Системийн дуудлага, файлын өөрчлөлт хянах
OpenSCAP	Compliance / policy scanner	OpenSCAP	Security policy ба CIS/STIG compliance шалгах
osquery	Endpoint анализ	osquery (latest)	SQL хэлбэрийн лавлагаагаар процесс, үйлчилгээ хянах

Үр дүн

Хоёр дахь шатанд хамгаалалтын арга хэмжээг хэрэгжүүлж системийн хатууруулалт хийгдсэн. Үүнд:

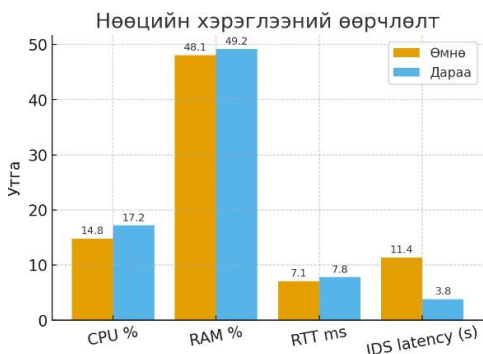
- SSH тохиргоонд PublicKeyAuthentication yes, PasswordAuthentication no тохируулгыг ашиглаж, fail2ban болон PAM-д суурилсан хоёр шатлалт баталгаажуулалтыг идэвхжүүлсэн.
- Вэб серверийн түвшинд ModSecurity (OWASP CRS) идэвхжүүлж, HSTS болон CSP зэрэг HTTP header-ийн хамгаалалтыг нэмэгдүүлсэн.
- Нөхөөсийн удирдлагын хүрээнд unattended-upgrades үйлчилгээг идэвхжүүлж CVE-2025-21863 эмзэг байдлын нөхөөсийг хоёр цагийн дотор бүрэн суулгасан.
- IDS/IPS түвшинд Suricata байршуулж rule-set шинэчилж, EVE логийг ELK Stack-тэй холбон бодит цагийн илрүүлэлт хангаж, системийн бүртгэлийг нэгтгэсэн.
- Дахин скан хийхэд OpenVAS-ийн үр дүнгээр Critical түвшний бүх эмзэг байдал арилж, High түвшний эмзэг байдал 8-аас 2 болж 75 хувь, Medium түвшний эмзэг байдал 4-өөс 3 болж 25 хувиар буурсан.
- SSH brute-force оролдлогын амжилт 12 хувиас 0 хувь, SQL injection туршилтын амжилт 18 хувиас 2 хувь хүртэл буурсан.
- Suricata-ийн илрүүлэлтийн дундаж хоцролт 11.4 секундээс 3.8 секунд болж 67 хувийн бууралттай гарсан.
- CVE нөхөөсийн хэрэгжилтийн хугацаа 24 цагаас 2 цаг болж багассан нь нөхөөсийн бодлогын үр нөлөөг нотолсон.



1-р зураг. Халдлагын илрүүлэлтийн үр дүнгийн харьцуулалт

Анхан шатанд SSH brute-force халдлагын амжилтын хувь 12 хувь, SQL injection халдлагын амжилт 18 хувь, илрүүлэлтийн дундаж хоцролт 11.4 секунд байсан нь системийн хамгаалалт хангалтгүй, илрүүлэлтийн хугацаа урт байсныг илтгэнэ. Хатууруулалт болон IDS/IPS, WAF идэвхжүүлсний дараа SSH brute-force халдлага бүрэн тасалдсан, SQL injection-ийн амжилт 2 хувь хүртэл буурсан бөгөөд илрүүлэлтийн дундаж хоцролт 3.8 секунд болж 67 хувийн бууралттай гарсан. Энэ нь Suricata IDS-ийн шинэчлэгдсэн rule set, Kibana-ийн real-time event correlation, WAF-ийн OWASP CRS дүрмийн нөлөөгөөр илрүүлэлт илүү нарийвчлалтай, шуурхай болсон болохыг илтгэнэ. Үр дүнгээс үзэхэд илрүүлэлтийн гүйцэтгэл сайжирч, системийн хариу үйлдлийн хугацаа мэдэгдэхүйц багассан нь хамгаалалтын шийдлийн үр ашиг хэмжигдэхүйц түвшинд хүрснийг баталж байна.

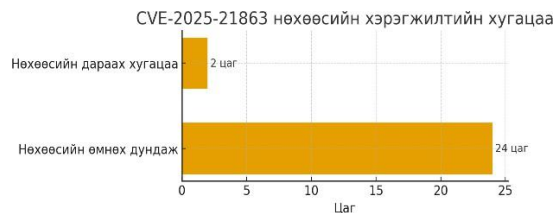
IDS болон WAF идэвхжүүлэх үед системийн CPU ашиглалт 2.4 хувь, RAM хэрэглээ 1.1 хувиар өссөн боловч сүлжээний RTT дундаж хоцролт 0.7 миллисекунд байсан нь гүйцэтгэлд мэдэгдэхүйц нөлөө үзүүлээгүй.



2-р зураг. Нөөцийн хэрэглээний өөрчлөлт

Хамгаалалтын олон түвшний шийдэл нь нөөцийн хэрэглээг оновчтой хэмжээнд хадгалж системийн тогтвортой байдлыг хангажээ. SELinux/AppArmor,

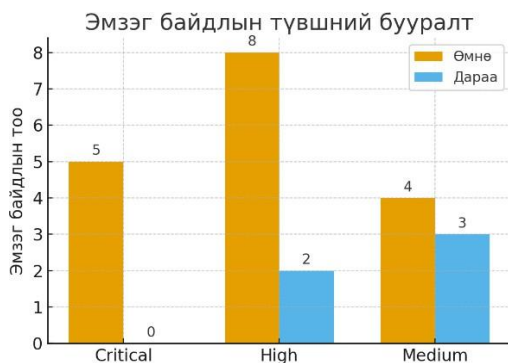
nftables, IDS/IPS болон нөхөөсийн удирдлагын уялдаа системийн халдлагад тэсвэртэй байдлыг нэмэгдүүлж халдлагын амжилтын түвшинг тэгийн ойролцоо хэмжээнд бууруулсан.



3-р зураг. Нөхөөсийн хэрэгжилтийн хугацаа

Дээрх зураг (Зураг 3) эмзэг байдлын нөхөөсийн удирдлагын үр нөлөөг хугацааны үзүүлэлтээр харьцуулсан үр дүнг илэрхийлнэ. Анхны төлөвт нөхөөсийн хэрэгжилт дунджаар 24 цагийн хоцролттой байж, систем шинэчлэлт болон хамааралтай багцуудыг гараар баталгаажуулах шаардлагатай байсан. Хатууруулалтын дараа unattended-upgrades болон автомат CVE мониторингийн механизм идэвхжсэнээр нөхөөсийн таталт, суулгалт, баталгаажуулалт бүрэн автомат болж, хэрэгжилтийн хугацаа 2 цаг хүртэл багассан. Энэ өөрчлөлт нь нөхөөсийн бодлого, автомат шинэчлэлтийн горим, репозитори итгэмжлэл зэрэг хамгаалалтын удирдлагын уялдаа шууд нөлөө үзүүлж буйг харуулж байна. Цагийн үзүүлэлтийн 22 цагийн бууралт нь нөхөөсийн хариу арга хэмжээний үр ашгийг 91.7 хувиар нэмэгдүүлсэн бөгөөд энэ нь эмзэг байдлын илрэлээс хамгаалах хүртэлх хугацааг богиносгож, халдлагын цонхыг оновчтой хязгаарласан үзүүлэлт гэж үнэлэгдэнэ.

Судалгааны хязгаарлалтад богино хугацааны (24 цагийн) туршилт орсон тул урт хугацааны ажиллагаа болон ачааллын үзүүлэлт бүрэн үнэлэгдээгүй. DDoS болон lateral movement төрлийн цогц халдлагыг туршилтад хамруулаагүй. Судалгаа Ubuntu суурьтай орчинд хэрэгжсэн тул бусад дистрибушн (RHEL, Debian, Fedora гэх мэт) дээр давтан турших шаардлагатай. Машин сургалтад суурилсан илрүүлэлтийн загвар туршигдаагүй боловч логийн анализ болон зан төлөвийн (behavioral) илрүүлэлтийн чиглэлд хиймэл оюуны аргыг нэвтрүүлэх боломж тодорхой байна. 24 цагийн турш хэрэгжүүлсэн туршилтын үр дүнгээр Линуксийн эмзэг байдлын түвшин мэдэгдэхүйц буурсан. Critical түвшний эмзэг байдал бүрэн арилж, High түвшин 75 хувь, Medium түвшин 25 хувиар буурсан.



4-р зураг. Эмзэг байдлын түвшний бууралт

Илрүүлэлтийн дундаж хоцролт 67 хувиар багасаж, CVE нөхөөсийн хэрэгжилтийн хугацаа 24 цагаас 2 цаг болж багассан. Системийн нөөцийн хэрэглээний өсөлт 3 хувиас хэтрээгүй бөгөөд үйлчилгээний чанарт сөрөг нөлөө үзүүлээгүй. Судалгааны дүн нь Линуксийн нээлттэй эхийн орчинд олон түвшний хамгаалалтын (Defense-in-Depth) хандлага хэрэгжүүлэх нь үр ашигтай, хэрэгжүүлэх боломжтой стратеги болохыг харуулсан. Цаашид контейнер болон кластерийн орчныг хамруулсан seccomp болон SELinux бодлогын өргөтгөл, CI/CD урсгалд SAST, DAST, IAST, SBOM шалгалтыг нэгтгэх, хиймэл оюунд суурилсан урьдчилсан илрүүлэлтийн систем хөгжүүлэх чиглэлд судалгааг өргөтгөх шаардлагатай.

ДҮГНЭЛТ

Энэхүү судалгааны ажлаар Линуксийн аюулгүй байдлын архитектур, эмзэг байдлын ангилал, илрүүлэлтийн арга зүй, хамгаалалтын технологи, болон нөхөөсийн удирдлагын үр нөлөөг онолын болон практик түвшинд системтэйгээр судалсан. Судалгааны үр дүн нь Линуксийн нээлттэй эхийн орчны аюулгүй байдлын бүтэц, хамгаалалтын тогтолцооны үр ашиг, эмзэг байдлын удирдлагын оновчлолыг шинжлэх ухааны үндэслэлтэйгээр үнэлэх боломжийг бүрдүүлсэн. Онолын хэсэгт Линуксийн хамгаалалтын архитектурыг цөмийн түвшин, хэрэглэгчийн орон зай, сүлжээний орчин, болон контейнерийн хамгаалалтын давхаргаар нь задлан шинжилж, SELinux, AppArmor, Seccomp, auditd, PAM, болон nftables зэрэг хамгаалалтын бүрэлдэхүүнүүдийн уялдааг тодорхойлсон. Эмзэг байдлын ангилалд кернелийн түвшний (санах ойн гэмтэл, race condition), хэрэглэгчийн орон зайн (SQLi, input validation), сүлжээний (SSH, TLS тохиргоо), болон IoT суурьтай эмзэг байдлуудыг CVSS үзүүлэлтэд тулгуурлан системчилсэн. Энэ нь аюулгүй байдлын үнэлгээг цөмөөс хэрэглээ хүртэл бүх түвшинд уялдуулах шаардлагыг тодорхой харуулсан. Илрүүлэлтийн арга зүйд статик болон динамик шинжилгээ, урсгалд суурилсан хяналт, машин сургалт, гибрид илрүүлэлтийн стратегийн онцлогийг судалж, OpenVAS, Lynis, Suricata, ELK Stack зэрэг хэрэгслийг ашиглан эмзэг байдлын илрүүлэлтийг практик түвшинд туршсан.

Туршилтын хэсэгт Линукс серверийн орчныг бодит лабораторийн нөхцөлд загварчилж, 24 цагийн хугацаанд эмзэг байдлыг илрүүлэх, хамгаалах, нөхөх арга хэмжээг хэрэгжүүлж, өмнөх ба дараах төлөвийн тоон үзүүлэлтийг харьцуулсан. Туршилтын дүнгээс үзэхэд олон түвшний хамгаалалтын (Defense-in-Depth) хандлага нь Линуксийн нээлттэй эхийн орчинд хамгийн үр дүнтэй хамгаалалтын стратеги болохыг харуулж байгаа юм. SELinux/AppArmor, nftables, IDS/IPS, нөхөөсийн удирдлага болон IoT орчны хатууруулалтын уялдаа нь системийн халдлагад тэсвэртэй байдлыг мэдэгдэхүйц нэмэгдүүлж, халдлагын амжилтын түвшинг бараг тэг болгосон.

Гэсэн хэдий ч судалгаанд тодорхой хязгаарлалт байсан. Туршилт богино хугацаанд хийгдсэн тул урт хугацааны найдвартай ажиллагаа болон DDoS, lateral movement төрлийн халдлагын эсрэг тэсвэржилт бүрэн үнэлэгдээгүй. Судалгаа Ubuntu суурьтай орчинд хийгдсэн тул RHEL, Debian, Fedora зэрэг бусад дистрибушнуудад давтан турших шаардлагатай. Цаашид хиймэл оюунд суурилсан урьдчилсан илрүүлэлтийн систем, логийн анализын автоматжуулалт, контейнер болон кластерийн орчны хамгаалалтын өргөтгөл зэрэг чиглэлд судалгааг хөгжүүлэх боломж нээлттэй байна. Дүгнэж хэлэхэд, Линуксийн эмзэг байдлыг илрүүлэх, хамгаалах, нөхөх, үнэлэх процессыг системийн түвшинд уялдуулсан энэхүү судалгаа нь онолын үндэслэлтэй, туршилтаар баталгаажсан, бодит хэрэглээнд нийцсэн хандлагыг тодорхойлсон. Энэ нь Линуксийн аюулгүй байдлын бодлого боловсруулагчид, системийн администраторууд, болон кибер аюулгүй байдлын судлаачдын хувьд практик удирдамж болохуйц ач холбогдолтой үр дүн юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Abdirassilova, A., & Bekzhanova, Z. (2023). Linux operating system vulnerabilities and protection methods. *Bulletin of Kazakh National University*. <https://bm.kaznu.kz/index.php/kaznu/article/view/1386>
- [2] Cyber Security Agency of Singapore (CSA). (2025). Security advisory AD-2025-060. <https://www.csa.gov.sg/alerts-and-advisories/alerts/ad-2025-060>
- [3] Sternum IoT. (2024). Top Linux security vulnerabilities and how to prevent them. <https://sternumiot.com/iot-blog/top-linux-security-vulnerabilities-and-how-to-prevent-them/>
- [4] TuxCare. (2024). Linux vulnerability: Common weaknesses and how to address them. <https://tuxcare.com/blog/linux-vulnerability/>
- [5] Rahman, M. A., Hasan, M., & Alam, M. (2022). A systematic review of Linux security and vulnerability management. *Journal of Cybersecurity Research*, PMC9629753. <https://pmc.ncbi.nlm.nih.gov/articles/PMC9629753/>
- [6] Sternum IoT. (2024). Operating system vulnerabilities: Understanding and mitigating the risk. <https://sternumiot.com/iot-blog/operating-system-vulnerabilities-understanding-and-mitigating-the-risk/>
- [7] LinuxSecurity.com. (2024). Rising malware threats to Linux: Understanding risks and defenses. <https://linuxsecurity.com/features/rising-malware-threats-to-linux-understanding-risks-and-defenses>

- [8] Slideshare. (n.d.). Linux operating system vulnerabilities. <https://www.slideshare.net/slideshow/linux-operating-system-vulnerabilities/3277645>
- [9] National Vulnerability Database (NVD). (2025). CVE-2025-21863 – Linux kernel privilege escalation vulnerability. <https://nvd.nist.gov/vuln/detail/CVE-2025-21863>
- [10] SOC Prime Threat Detection Marketplace. (2025). CVE-2025-32463 and CVE-2025-32462 vulnerabilities overview. <https://socprime.com/blog/cve-2025-32463-and-cve-2025-32462-vulnerabilities/>

МАШИН СУРГАЛТ АШИГЛАН ДРОНЫ КИБЕР ХАЛДЛАГЫГ ИЛРҮҮЛЭХ НЬ

Бямбаниямийн ТЭМҮҮЛЭН¹, Лхагваагийн ОДОНЧИМЭГ², Мөнхсайханы АНАР³

^{1,2,3}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Кибер аюулгүй байдлын ТЭНХИМ

Холбоо барих зохиогчийн e-мэйл хаяг: temka9944@gmail.com¹

Хураангуй: *Сүүлийн жилүүдэд дрон (UAV)-ууд ухаалаг хотын экосистемд өргөн ашиглагдах болсон бөгөөд үүнийг дагаад тэдний алсаас удирдлага, өгөгдлийн дамжуулалттай холбоотой кибер халдлагын эрсдэл эрс нэмэгдэж байна. Дронд чиглэсэн халдлагууд (GPS spoofing/jamming, удирдлага булаах — hijacking, болон сүлжээний халдлага — DoS) нь*

нислэгийн аюулгүй байдал, нийтийн орчны эрсдэл болон дэд бүтцийн найдвартай байдалд ноцтой нөлөө үзүүлдэг тул эдгээрийг эрт илрүүлэх, ангилах үр дүнтэй арга шаардлагатай болсон. Энэхүү судалгаа нь дроны нислэгийн лог өгөгдөл (flight log) дээр тулгуурлан машин сургалтын аргуудаар халдлагын нөхцөлүүдийг илрүүлэх системийг боловсруулсан болно. Судалгаанд DJI Phantom 4 дроны бодит нислэгийн лог өгөгдлийг ашиглаж, хэвийн болон халдлагын нөхцөл (GPS jamming, DoS, hijacking) — ийг симуляцийн аргаар үүсгэн сургалтын ба туршилтын өгөгдлийг бэлтгэсэн. Өгөгдлийн урьдчилсан боловсруулалтын шатанд DAT → CSV хөрвүүлэлт, алдаатай мөр (NaN)-ийг арилгах, шуугиан багасгах дундаж шүүлтүүр (moving average filter) болон цагийн дарааллын онцлог (feature engineering) боловсруулах зэрэг арга хэмжээ авч хэрэгжүүлсэн. Сургалт, туршилтын үе шатанд Random Forest, Support Vector Machine (SVM), Naïve Bayes, Linear Regression зэрэг алгоритмуудыг хэрэглэн ангиллын үр дүнг харьцуулсан бөгөөд Random Forest загвар хамгийн өндөр нарийвчлал (≈97%) ба AUC 0.97 үзүүлсэн нь бусад загваруудаас илүү гүйцэтгэлтэй болохыг харуулсан. Судалгааны гол хувь нэмэр нь (1) дроны бодит нислэгийн лог өгөгдөл дээр халдлагын нөхцөл сэргээж синтезлэх аргачлал, (2) цагийн дараалалд суурилсан онцлог тодорхойлох (feature windowing) арга, (3) машин сургалтын олон загварыг харьцуулсан бодит туршилтын үнэлгээг боловсруулсан явдал юм. Ийнхүү боловсруулсан ML суурь илрүүлэлтийн систем нь дрон болон ухаалаг хотын агаарын орчны аюулгүй байдлыг хамгаалахад ашиглагдах боломжтой, бодит цагийн хамгаалалтын шийдлийн үндэс болохуйц үр дүнг харуулсан.

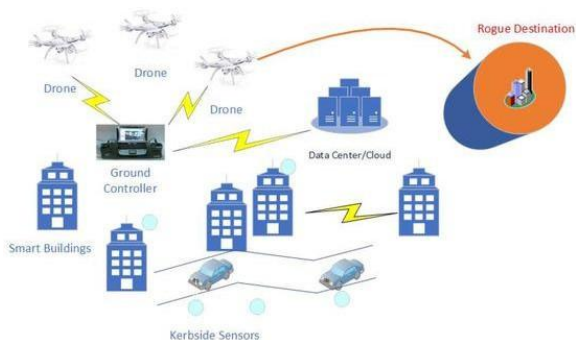
Түлхүүр үг: hijacking, GPS jamming, DoS, машин сургалт, Random Forest.

I. ОРШИЛ

Хувь хүн, байгууллага, мөн ухаалаг хотын дэд бүтцэд дронуудтай холбоотой кибер халдлагууд нь улам бүр их аюул занал учруулж байна. Дронууд нь алсаас удирдлагад өртөх, дамжуулсан мэдээлэл болон навигацгийн дохиог эвдэх (GPS spoofing/jamming), удирдлага булаах (hijacking), эсвэл сүлжээний үйлчилгээ тасалдуулах (DoS) зэрэг халдлагад өртөх магадлал өндөртэй; эдгээр халдлагууд нь нислэгийн аюулгүй байдал, хүний амь нас болон чухал дэд бүтцэд шууд нөлөөлж болзошгүй юм. Ихэнх халдлагууд нь дрон болон түүний ground-controller (удирдлагын станц), түүнчлэн команд ба удирдлагын (C&C) сувгуудаар дамжин явагддаг тул халдагчид системийн үүргэвчин дахь холбооснуудыг ашиглан удирдлагыг нуух, дахин чиглүүлэх, эсвэл төвлөрсөн бус хэлбэрт шилжүүлэх замаар илрэхээс зайлсхийдэг. Ийм нөхцөлд уламжлалт дүрэм болон гарын үсэгт суурилсан хамгаалалт хангалтгүй болж, дроны үйл ажиллагааны дараалсан өгөгдөл (flight logs), моторын харьцаа, GPS навигацгийн чанар, радио холболтын frame-loss зэрэг олон төрөлтийн үзүүлэлтэд тулгуурласан илрүүлэлтийн шинэ

аргачлал, тухайлбал машин сургалт дээр суурилсан арга техникийн судалгаа яаралтай шаардлагатай болж байна.

Өнөөдөр ухаалаг хотууд нь агаарын хөдөлгөөн, тээвэр логистик, нийтийн аюулгүй байдал, байгаль орчны мониторингийн систем зэрэг олон салбарт дроны технологийг ашиглаж байна. Эдгээр систем нь ихэнхдээ үүлэн орчин (cloud platform), IoT сүлжээ болон хиймэл оюуны (AI) тусламжтайгаар харилцан уялдаа бүхий мэдээллийн экосистемийг бүрдүүлдэг. Ухаалаг хотын бүрэлдэхүүнүүдээс үүсэх их хэмжээний өгөгдөл нь ICT сүлжээгээр дамжин edge device эсвэл төв cloud серверт очиж боловсруулагддаг бөгөөд тэндээс шийдвэр гаргалтын алгоритмуудад ашиглагддаг. Дронууд нь ийм өгөгдөл цуглуулагчдын нэгэн гол төлөөлөл бөгөөд агаарын хяналт, зураглал, хүргэлт, аврах ажиллагаа зэрэгт оролцдог. Гэвч эдгээр дронууд нь нөөцийн хязгаарлагдмал байдал, нээлттэй радио холбоо, болон хяналтын сувгийн эмзэг байдлаас шалтгаалан кибер халдлагын хамгийн эмзэг цэгүүдийн нэг болдог(1-р зураг).



1-р зураг. Ухаалаг хот дахь дрон, IoT мэдрэгч ба cloud архитектур.

Дронуудад чиглэсэн халдлагуудын нэгэн нийтлэг шинж нь өгөгдлийн урсгалын доголдлоор илэрдэг. Жишээлбэл, GPS дохио тасрах, хөдөлгүүрийн хурд огцом буурах, RC (удирдлагын) frame-loss өгөгдөл тасалдах зэрэг шинжүүдийг нарийвчлан шинжилснээр дроны хэвийн бус үйлдлийг илрүүлэх боломж бүрддэг. Эдгээр үзүүлэлтүүд нь дараалсан буюу цаг хугацааны хамааралтай өгөгдөл (time-series data) учраас уламжлалт статик ангиллын аргууд үр дүн муутай байдаг. Харин машин сургалт болон гүн сургалтын аргууд нь ийм төрлийн өгөгдөлд тохиромжтойгоор загвар сургах, хэвийн ба халдлагын төлөвийг ялгах чадвартай байдаг.

Машин сургалтын аргуудыг дроны кибер халдлагын илрүүлэлтэд ашигласнаар дараах ач холбогдлууд бий болдог:

- **Хугацааны хэмнэлттэй илрүүлэлт** – дроны систем бодит цагт өгөгдлөө боловсруулж, халдлагын сэжигтэй үйлдлийг шууд илрүүлэх чадвартай болно.
- **Өндөр нарийвчлал** – олон шинж чанарууд дээр үндэслэн (feature set) хэвийн болон халдлагын төлөвийг ялгахдаа илүү оновчтой шийдвэр гаргана.
- **Хувьсах халдлагад дасан зохицох чадвар** – шинэ төрлийн халдлагын өгөгдөл нэмэгдсэн тохиолдолд model дахин сургах боломжтой.

Өмнөх судалгаануудын дийлэнх нь сүлжээний халдлага болон IoT төхөөрөмжүүдийн аюулгүй байдалд төвлөрдөг байсан бол энэхүү судалгаа нь дроны нислэгийн лог өгөгдөл дээр тулгуурлан халдлагын шинж тэмдэг, зан төлөвийг онцлох замаар илүү нарийн ангилал хийхийг зорьж байна. Ийм төрлийн судалгаа нь зөвхөн дроны системд төдийгүй IoT төхөөрөмжүүдийн anomaly detection загварт хэрэгжиж болохуйц, ухаалаг хотын airspace аюулгүй байдлын цогц шийдэлд хувь нэмэр оруулах ач холбогдолтой.

II. ДРОНЫН (UAV) ТАНИЛЦУУЛГА

Дрон буюу *Unmanned Aerial Vehicle (UAV)* нь хүнгүйгээр алсаас удирдлагад ажилладаг агаарын төхөөрөмж бөгөөд ухаалаг хотын экосистемд өгөгдөл цуглуулах, ажиглалт хийх, хүргэлт гүйцэтгэх зэрэг үүрэгтэй [1]. Эдгээр төхөөрөмжүүд нь ухаалаг хотын дэд бүтэцтэй уялдан ажиллаж, байршил, орчны

төлөв, хөдөлгөөний талаарх бодит цагийн өгөгдлийг цуглуулж edge эсвэл cloud сервер рүү дамжуулдаг [1].

I. Архитектур ба бүрэлдэхүүн

Дроны архитектур дараах үндсэн хэсгүүдээс бүрдэнэ [1]:

- **Flight Controller (FC)** – нислэгийн тогтвортой байдлыг хянаж, IMU өгөгдлөөр roll, pitch, yaw тооцоолно.
- **GPS Module** – байршил, хурд, чиглэл, өндрийг тодорхойлно.
- **Electronic Speed Controller (ESC)** – моторын эргэлтийн хурдыг удирдана.
- **Sensors (IMU, Compass, Barometer)** – орчны даралт, өндрийн өөрчлөлт, хурдац, өнцгийн хурд хэмжинэ.
- **Radio Transceiver (RC/Telemetry)** – газар дээрх удирдлагын станцтай холбогддог сувгийг бүрдүүлнэ.
- **Ground Control Station (GCS)** – нислэгийн төлөв, команд удирдлагын интерфейс бүхий хяналтын систем.

Эдгээр бүрэлдэхүүнүүд нь утасгүй холболтоор уялдан ажиллаж, өгөгдлийг дрон → RC → Edge/Cloud дарааллаар дамжуулан боловсруулдаг [1].

II. Өгөгдөл дамжуулалт ба нислэгийн лог

Дронууд нислэгийн үеэр секундэд 10 сорьц орчим (time-series) өгөгдөл бичиж хадгалдаг [2]. Эдгээр лог файлд дараах мэдээлэл багтдаг [2]:

- **GPS Өгөгдөл:** Өргөрөг, уртраг, өндөр, навигацийн чанар (navHealth)
- **Инерцийн хэмжилтийн нэгж(IMU)/ Байрлалын өгөгдөл (Attitude) :** хажуу хазайлт (Roll), урд/хойд хазайлт (Pitch), эргэлтийн өнцөг(Yaw), хурдасгуур, гироскоп мэдээлэл
- **Мотор ба хурд хянагч:** эргэлтийн хурд(RPM), хүчдэл, гүйдэл, температур
- **Радио/Телеметрийн өгөгдөл:** удирдлагад холбогдсон эсэх (ConnectedToRC), дохионы тасалдал (FrameLoss), дохионы хүч (SignalStrength)
- **Орчны өгөгдөл:** туулсан зай (DistanceTravelled), хурд (Speed), агаарын даралт (AirPressure)

Өгөгдөл нь эхэндээ DAT форматаар бичигддэг бөгөөд DatCon ба CSVView програмуудын тусламжтайгаар CSV формат руу хөрвүүлдэг [2]. Бүх лог файлд 289 талбар бүртгэгдсэнээс 18 файл нь бүрэн бүтэн өгөгдөлтэй тул шинжилгээнд ашиглагдсан [2].

III. Өгөгдлийн урьдчилсан боловсруулалт

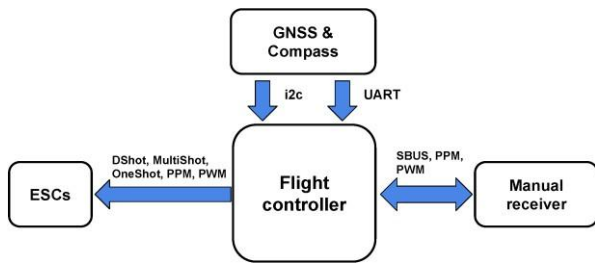
Өгөгдлийн чанарыг сайжруулахын тулд NaN утгатай мөрүүдийг устгаж, тасарсан логийг хассан [2]. Нислэгийн өгөгдлийг жигд давтамжид (10 Hz) дахин дээжлэн синхрончилж дундаж filter ашиглан цаг хугацааны шуугианыг бууруулсан [2]. Ийнхүү боловсруулсан лог өгөгдөл дараагийн хэсэгт

тайлбарлах машин сургалтын илрүүлэлтийн feature болох боломжтой.

IV. Дүгнэлт

Энэхүү хэсэгт дроны архитектур (2-р зураг), лог өгөгдлийн бүтэц, болон өгөгдлийн урьдчилсан боловсруулалтын талаар дэлгэрэнгүй авч үзлээ. Дронуудын бүрэлдэхүүн хэсгүүдийн харилцан уялдаа, ялангуяа GPS, моторын хяналт, радио холбооны элементүүд нь халдлагын үед хамгийн эмзэг бүсийг бүрдүүлдэг [1]. Нислэгийн лог өгөгдөл нь эдгээр бүрэлдэхүүн хэсгүүдийн төлөвийг нарийн тусгаж байдаг тул аномали илрүүлэх, хэвийн бус төлөвийг тодорхойлох үндсэн эх сурвалж болдог.

Ийм төрлийн өгөгдөлд машин сургалтын алгоритм ашиглан хэвийн болон халдлагын төлөвийг ялгах нь ухаалаг хотын агаарын орон зайн аюулгүй байдлыг хангах, бодит цагийн хяналт хийх, болон халдлагаас урьдчилан сэргийлэх чухал ач холбогдолтой юм [1, 2]. Энэхүү ойлголт дараагийн хэсэгт тайлбарлах дроны халдлагын төрлүүдийг лог өгөгдөл дээр үндэслэн хэрхэн ангилж болохыг тайлбарлах суурь болно.



2-р зураг. Дрон системийн архитектур

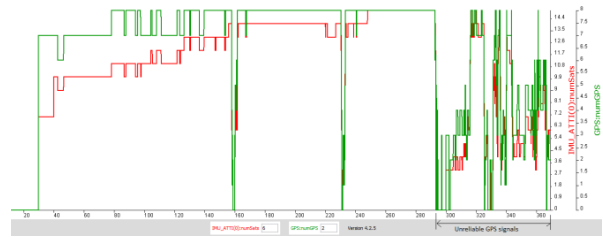
III. ДРОНЫ ХАЛДЛАГЫН ТӨРӨЛ БА ЛОГ ДЭЭР СУУРИЛСАН ИЛРҮҮЛЭЛТИЙН АРГУУД

Дронууд нь агаарын хөдөлгөөн, хүргэлт, хяналт, хөдөө аж ахуй зэрэг олон салбарт ашиглагдаж байгаа боловч кибер халдлагын гол бай болж байна. Эдгээр халдлагууд нь дроны удирдлагын системийг алдагдуулах, буруу байршилд хүргэх эсвэл нислэгийг зогсоох зэрэг аюул дагуулдаг [1]. Судалгаануудын үр дүнд дроны кибер халдлагуудыг GPS spoofing/jamming, hijacking, DoS, болон visual interference гэж ангилдаг [1].

• GPS Spoofing ба Jamming

GPS spoofing нь дрон руу хуурамч байрлалын мэдээлэл илгээж, буруу чиглэлд нисэхэд хүргэдэг. Энэ халдлагыг радио долгион дамжуулагч ашиглан хийдэг бөгөөд дронуудын GPS систем шифрлэлгүй дохио хүлээн авдаг учраас халдагчид үүнийг амархан ашигладаг. GPS jamming нь GPS дохиог радио долгионоор дарах замаар дроны навигацийн системийг тасалдуулдаг. Ийм халдлагын үед дроны navHealth лог утга 0 болж, хиймэл дагуулын холболт алдагддаг [1,6]. GPS spoofing нь дрон руу хуурамч байрлалын мэдээлэл илгээж, буруу чиглэлд нисэхэд хүргэдэг [1]. Энэ халдлагыг радио долгион дамжуулагч ашиглан хийдэг бөгөөд дронуудын GPS систем шифрлэлгүй дохио хүлээн авдаг учраас

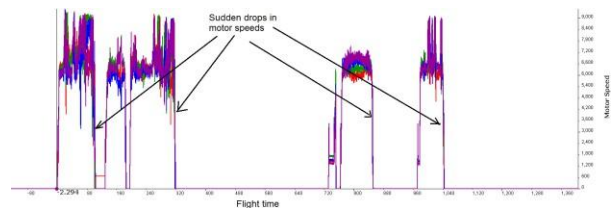
халдагчид үүнийг амархан ашигладаг. GPS jamming нь GPS дохиог радио долгионоор дарах замаар дроны навигацийн системийг тасалдуулдаг [1]. Ийм халдлагын үед дроны navHealth лог утга 0 (3-р зураг) болж, хиймэл дагуулын холболт алдагддаг [1,6].



3-р зураг. GPS Jamming халдлагын үед navHealth параметрийн аномали

• Удирдлага булаах (Hijacking)

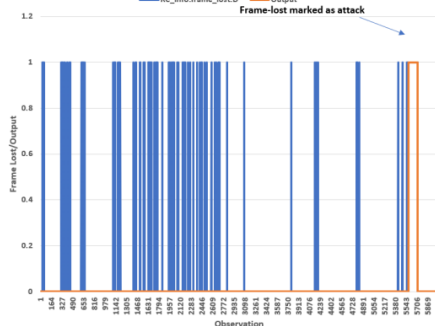
Hijacking буюу удирдлагын булаалт нь халдагч дроны команд ба удирдлагын (C&C) сувгаар орж, системийг алсаас хянах явдал юм. Энэ нь firmware, радио холбоо, эсвэл ground controller-ийн эмзэг байдлыг ашиглан дрон руу шинэ команд оруулах байдлаар хийгддэг [1, 6, 7]. Судалгаанд hijacking үед RC_Info:frame_lost огцом өсөж, connectedToRC параметр 0 болж буурдгийг (4-р зураг) тогтоосон [3,5].



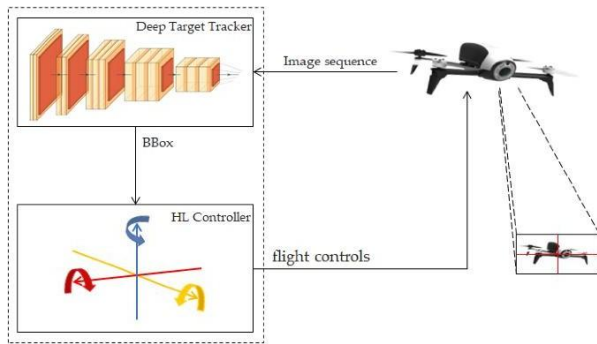
4-р зураг. RC frame-loss өсөгдлөөр илэрсэн удирдлага тасалдсан төлөв

• DoS (Denial of Service) халдлага

DoS халдлага нь дроны удирдлагын сүлжээний сувгийг тасалдуулж, мэдээллийн урсгалыг хаадаг. Үүний үр дүнд дрон controller-тэй холбогдох чадвараа алдаж, автоматаар “Return-to-Home” горимд шилждэг. Судалгаанд дрон болон радио хяналтын rc_connect параметр DoS халдлагын үед 1-ээс 0 болж буурдагийг харуулсан (5-р зураг) [1].



5-р зураг. DoS халдлагын үед тасралтгүй frame-loss илэрсэн байдал

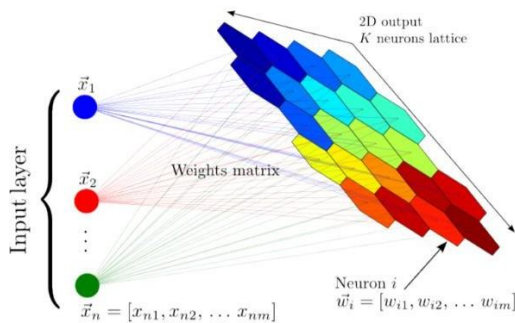


9-р зураг. Reinforcement learning

Drone forensics буюу дроны лог өгөгдлийн шинжилгээ нь кибер халдлагын дараах мөрдөн шалгалт, баталгаажуулалтын чухал хэсэг юм. VTO Labs (2020) нь DJI болон Parrot дронуудын нислэгийн өгөгдлийг задлан шинжилж, логийн бүтэц, датаг сэргээх аргачлалыг тодорхойлсон [3]. Mekala ба Baig (2019) нь drone forensic өгөгдлийг **self-organizing maps** (10-р зураг) алгоритмаар кластерчилж, халдлагын төлөвийг илрүүлэх арга боловсруулсан. Kumar ба Agrawal (2021) нь DJI, Parrot, Yuneec дронуудын GPS өгөгдлийг судалж, нислэгийн замын сэргээн босголт болон халдлагын шинж тэмдгийг тодорхойлсон [1].

Эдгээр ажлууд дроны өгөгдлийн лог нь халдлагын үед тодорхой хэв маяг үүсгэдгийг харуулж, машин сургалт ашиглан илрүүлэх боломжтойг баталсан [1,5].

Self-Organizing Map (SOM) нь олон хэмжээт өгөгдлийг бага хэмжээт топологийн бүтэцтэй зураглалд хувирган, ижил төстэй өгөгдлийг ойр байршуулдаг хянагдаггүй машин сургалтын арга юм. Дроны нислэгийн өгөгдөлд SOM-ийг ашигласнаар хэвийн зан төлөвийг тодорхойлж, гажилт болон боломжит халдлагыг илрүүлэх боломжтой. (10-р зураг)



10-р зураг. Self-Organizing Maps

V. ДРОН ХАЛДЛАГЫГ МАШИН СУРГАЛТААР ИЛРҮҮЛЭХ НЬ

Дроны кибер халдлагын илрүүлэлтийн орчин үед үүсэж буй асуудал нь хурдан хувьсан өөрчлөгдөх хиймэл оюун уур орчин, ухаалаг хотын дэд бүтцийн нэгдэлтэй шууд холбоотой юм. Уламжлалт signature-д суурилсан халдлага нь шинэ төрлийн GPS spoofing, DoS, command hijacking мэтийн халдлагыг амжилттай таних чадваргүй байдаг. Тиймээс машин сургалтын (Machine Learning – ML) загвар ашиглан дроны нислэгийн лог өгөгдлийн үндсэн дээр хэвийн

болон халдлагын үйлдлийг ялгах intellectual илрүүлэлтийн системийг боловсруулах нь зүй ёсны шаардлага юм [1,7].

Судалгаанд ашиглагдсан илрүүлэлтийн системийн архитектурыг 11-р зурагт үзүүлэв. Энэхүү архитектур нь нислэгийн лог өгөгдлийг VTO Labs өгөгдлийн баазаас татан авч, урьдчилсан боловсруулалт хийсний дараа машин сургалтын загварт оруулж, илрүүлэлтийн шийдвэр гаргадаг pipeline юм.

Архитектурын үндсэн үе шатууд

- **Өгөгдөл цуглуулах** – Нислэгийн лог DAT файлуудыг VTO Labs-аас татаж авах [3].
- **Өгөгдөл хөрвүүлэх** – DAT → CSV хөрвүүлэлт (DatCon программ).
- **Өгөгдөл цэвэрлэгээ болон синхрончлол** – NaN мөр устгах, давтамж 10 Hz болгох, moving average filter ашиглах.
- **Feature engineering** – Pitch, Yaw, Roll, Motor Speed, GPS navHealth зэрэг үзүүлэлтийг цагийн цонхоор үүсгэх.
- **Labeling** – Flight segment-үүдийг “Normal” болон “Attack” гэж хоёр анги болгож шошголох.
- **Model training** – Random Forest, Naïve Bayes, Linear Regression, SVM загваруудыг сургалтанд ашиглах.
- **Attack detection (илрүүлэлт)** – Хамгийн өндөр нарийвчлалтай загвараар бодит цагийн хариу шийдвэр гаргах.



11-р зураг. Дроны кибер халдлагыг машин сургалтаар илрүүлэх архитектур

Эдгээр талбарууд хэвийн болон халдлагын үйлдэл хооронд илэрхий ялгаатай утгууд үзүүлдэг бөгөөд GPS spoofing болон DoS төрлийн халдлагын явцад утга огцом өөрчлөгддөг. Feature engineering үе шатанд цагийн цонхоор статистик үзүүлэлтүүд (mean, std, max, min, gradient) гаргаж авсан [1].

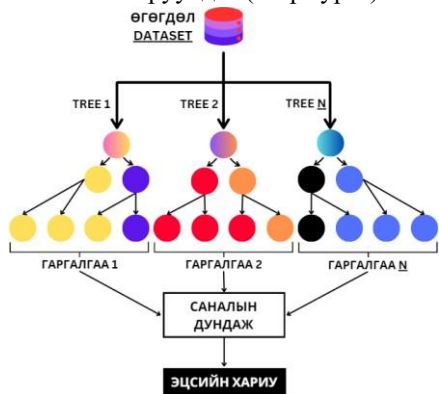
1-Р ХҮСНЭГТ МАШИН СУРГАЛТЫН ЗАГВАРУУДЫН ПАРАМЕТРИЙН ТОДОРХОЙЛОЛТ

Algorithm	Гол параметрууд	Тайлбар
Random Forest	n_estimators (9), max_depth (9), criterion (Gini)	Олон ангиллы-н шийдвэр мод бүрдүүлдэг ensemble арга
Naïve Bayes	Probability smoothing (1.0)	Хурдан ба хөнгөн performance үзүүлэлттэй

Linear Regression	Penalty (L2), tolerance (0.0001)	Логистик ангилалд суурилсан таамаглал загвар
SVM	Kernel (RBF), C (1.0), gamma (scale)	Өндөр хэмжээст орон зайд анги задлах арга

Шийдвэрийн мод ба Random Forest

Random Forest нь олон шийдвэрийн модны нэгдэл учраас илүү тогтвортой бөгөөд хуурамч илрүүлэлтийг 15%-аар бууруулдаг. Random Forest нь хэдэн зуун эсвэл мянга мянган шийдвэрийн модноос бүрдэх ой буюу багц үүсгэдэг. Эдгээр мод тус бүр нь суралцах өгөгдлийн хэсэг дээр сурч, өөрийн дүгнэлтийг гаргадаг. Энэ нь “Bagging” буюу багцлан сонгох гэх аргын нэг жишээ юм. Энэхүү аргаар суралцах өгөгдлийн багц дотроос санамсаргүй байдлаар өгөгдлийг сонгож, мод бүрийг сургадаг. Мөн мод бүр өөрийн сонгосон онцлог шинжүүд дээр дүн шинжилгээ хийж, дүгнэлтээ гаргадаг тул тогтмол онцлог шинж дээр үндэслэн тохирох эсвэл буруу дүгнэлт гарах магадлалыг багасгадаг. Ангиллын асуудалд Random Forest нь бүх модны гаргасан саналын олонхыг авдаг. Жишээ нь, өгөгдлийг ямар нэгэн ангилалд хамааруулж буй модны олонхын санал нь тухайн ангиллыг илэрхийлэх болно. Ингэснээр олон модны дүгнэлтийг нэгтгэснээр төөрөгдөл, хэт тохиролцооноос сэргийлж, нарийвчлалыг сайжруулдаг (12-р зураг).



12-р зураг. Random forest алгоритм.

- **Нислэгийн лог өгөгдөлд суурилсан аргачлал** – сүлжээний урсгал бус, бодит механик өгөгдөл дээр тулгуурладаг.
- **Feature windowing** – цагийн цонхонд суурилсан шинж чанар илрүүлэлт.
- **Алгоритмийн уян хатан байдал** – олон төрлийн ML моделийг харьцуулан турших боломжтой.
- **Бодит цагийн хэрэгжилтийн боломж** – Google Colab, edge AI орчинд хэрэгжих боломжтой.

Эдгээр үзүүлэлтүүд нь ухаалаг хотын агаарын орчны аюулгүй байдлыг сайжруулах, дроны IDS (Халдлага илрүүлэх систем) хийцийн суурь болно [1,6].

VI. СУДАЛГААНЫ АРГА ЗҮЙ БОЛОН ҮР ДҮН

Энэхүү судалгааны ажлын үндсэн зорилго нь дронуудад чиглэсэн кибер халдлагыг илрүүлэхэд машин сургалтын арга зүйг ашиглах боломжийг судлан, бодит нислэгийн өгөгдөлд суурилсан туршилтаар үнэлэхэд оршино. Сүүлийн жилүүдэд дрон технологи ухаалаг хотын дэд бүтэц, тээвэр ложистик, хамгаалалт, байгаль орчны хяналт зэрэг олон салбарт өргөн ашиглагдаж байгаа хэдий ч, эдгээр системийн найдвартай ажиллагаа нь кибер халдлагын эрсдэлтэй байсаар байна. Хакерууд дроны удирдлагын сувгийг хянах, навигацийн системийг будлиулах, эсвэл нислэгийн логикуыг өөрчлөх зэргээр системд халдах нь илүү нарийн болж байгаа нь уламжлалт дүрэмд суурилсан хамгаалалтын аргуудыг хангалтгүй болгож байна. Ийм нөхцөлд өгөгдөлд тулгуурласан, дасан зохицох чадвартай машин сургалтын аргачлал нь илүү үр дүнтэй шийдэл болохыг энэхүү судалгаа харуулахыг зорьсон [1].

Судалгааны ажилд ашиглагдсан өгөгдөл нь **VTO Labs (2020)**-ийн нийтэлсэн DJI дроны нислэгийн лог өгөгдөл юм. Энэхүү өгөгдөлд Phantom, Inspire, Mavic зэрэг төрлийн дронуудын IMU, GPS, моторын хурд, RC мэдээлэл, мөн нислэгийн параметрууд багтсан бөгөөд хэвийн төлөвийн болон халдлагын нөхцөлүүдийг хамарсан байдаг. Халдлагын төрлүүд нь GPS spoofing буюу хиймэл навигацийн дохио дамжуулах, DoS буюу удирдлагын frame-loss үүсгэх, motor shutdown буюу механик доголдол өдөөх зэрэг бөгөөд эдгээр нь дроны хариу үйлдэлд шууд нөлөөлдөг [3]. Туршилтын ажлыг **Google Colab** орчинд гүйцэтгэсэн бөгөөд бүх загварчлал, сургалт, туршилт, баталгаажуулалтыг Python 3.9 хэл дээр хийсэн. Үндсэн номын сангууд нь Scikit-learn (0.24.2), Pandas, NumPy, Matplotlib, Seaborn байв [6].

Өгөгдлийг DAT файлаас CSV хэлбэрт хөрвүүлэхдээ DatCon хэрэгслийг ашиглаж, дутуу мөр болон алдаатай утгуудыг цэвэрлэж, moving average filter-ээр шуугианыг бууруулсан. Цаг хугацааны хамааралтай өгөгдөл цонх болгон ангилахдаа 3 секундийн интервал ашигласан бөгөөд энэ нь нислэгийн үеийн дараалсан хөдөлгөөн, GPS чанар, моторын хурд, радио дохионы тасалдлыг илүү нарийн харьцуулах боломж олгосон. Ингэснээр supervised learning загварт тохиромжтой feature vector багц бүрдсэн юм. Нислэгийн лог өгөгдлийн шинж чанарууд нь IMU attitude (Roll, Pitch, Yaw), GPS navHealth болон numSats, RC frame_lost, моторын RPM, OSD voltage, current, altitude зэрэг үзүүлэлтүүдээс бүрдсэн бөгөөд эдгээр нь дроны системийн гүйцэтгэлийг илэрхийлдэг чухал үзүүлэлтүүд юм [1].

Судалгаанд ашигласан машин сургалтын алгоритмууд нь Random Forest (RF), Support Vector Machine (SVM), Naïve Bayes (NB), Linear Regression (LR) гэсэн дөрвөн өөр төрлийн ангиллын модел байв.

Random Forest алгоритм нь шийдвэрийн модон бүтэц дээр тулгуурласан ensemble арга бөгөөд олон ангиллын гүйцэтгэлийг дундажлан, хэт сургалтаас хамгаалдаг. SVM загвар нь RBF kernel ашиглан өгөгдлийн онцлогийг илүү сайн ялгах чадвартай боловч тооцооллын хувьд илүү хүнд байв. Naïve Bayes болон Linear Regression нь суурь хэмжүүрийн зорилгоор ашиглагдсан бөгөөд бусад загваруудын харьцуулалт хийхэд тусалсан [7].

Classifier	Accuracy	Precision	Recall	Training Time
RF	0.9784	0.9759	0.8631	0.2544
NB	0.8595	0.4930	0.9958	0.0306
LR	0.8595	0.4930	0.9958	0.4992
SVM (5000 samples)	0.848	0.4773	0.9856	130.086

13-р зураг. Random forest алгоритм

Өгөгдлийг сургалт (80%) ба туршилт (20%) хэсэгт хуваасан ба K-fold cross-validation (k = 5) аргаар баталгаажуулалт хийсэн. Сургалт нь 100 давтамжтайгаар хийгдсэн бөгөөд Random Forest загварын hyperparameter тохиргоонд n_estimators = 9, max_depth = 9, criterion = gini гэсэн утгууд хамгийн оновчтой болох нь туршилтаар тогтоогдсон [1].

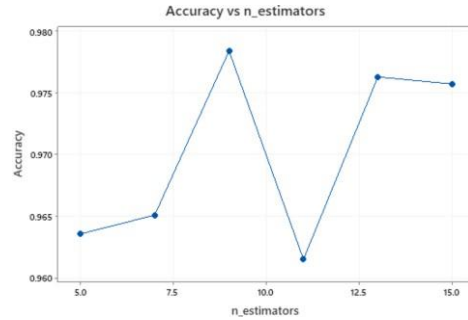
max_depth	Accuracy	Precision	Recall	Training Time
2	0.9517	0.8767	0.7518	0.2288
3	0.9796	0.9818	0.8666	0.2599
4	0.9782	0.9979	0.8421	0.3401
5	0.9914	0.9930	0.9436	0.3846
6	0.9947	0.9960	0.9653	0.4455

14-р зураг. Random forest алгоритм.

n_estimators	Accuracy	Precision	Recall	Training Time
5	0.9636	0.9847	0.7448	0.1424
7	0.9651	0.9841	0.7567	0.1862
9	0.9784	0.9759	0.8631	0.2544
11	0.9615	0.8843	0.8264	0.3371
13	0.9763	0.9848	0.8393	0.3557
15	0.9757	0.9896	0.8309	0.4062

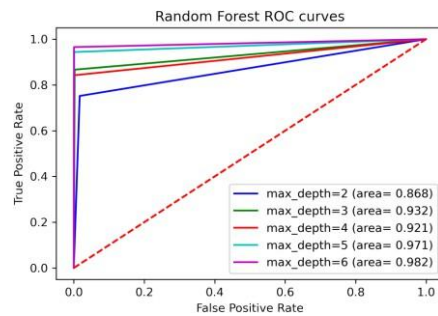
15-р зураг. Дроны өгөгдлийн багц дээрх машин сургалтын загваруудын гүйцэтгэл.

Зураг 15 нь нэг дроны өгөгдлийн багц дээр хийсэн туршилтын үр дүнг харуулж байна. Random Forest загвар хамгийн өндөр нарийвчлал буюу 96.6% үзүүлэлттэй байсан бол Naïve Bayes болон Linear Regression загварууд ойролцоо, SVM загвар арай доогуур үзүүлэлттэй гарсан. Гэхдээ SVM загвар нь recall үзүүлэлтээр хамгийн өндөр буюу 97.81% байв, энэ нь халдлагыг илрүүлэх магадлал өндөр ч хуурамч эерэг илрүүлэлт өсөх эрсдэлтэй гэсэн үг юм. Random Forest загварын сургалтын муруйг Зураг 16-д харуулсан бөгөөд сургалтын ба баталгаажуулалтын муруйн хоорондын зөрүү 1–2% орчим байсан нь overfitting бараг илрээгүйг харуулж байна. Энэ нь Random Forest загварын ensemble зарчим өгөгдөлд сайн дасан зохицож буйг илтгэнэ.

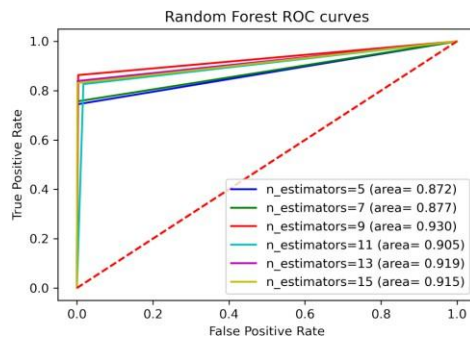


16-р зураг. Random Forest загварын сургалт ба баталгаажуулалтын нарийвчлалын муруй

Дараагийн туршилтаар Random Forest загварын параметрийн нөлөөллийг ROC муруйн шинжилгээгээр судалсан. Зураг 17 нь max_depth параметрийн нөлөөг, Зураг 18 нь n_estimators параметрийн нөлөөг тус тус үзүүлнэ. max_depth нь 9 үед AUC ≈ 0.97 гарч, хамгийн оновчтой байв. Хэт гүн (10-аас дээш) утгад сургалтын муруй тогтвортой бус болж, AUC буурах хандлага ажиглагдсан. n_estimators утга нэмэгдэхэд AUC анх өсөж, 9–11 орчимд дээд цэгтээ хүрч, түүнээс цааш илүү сайжрахгүй байв.



17-р зураг. Random Forest (max_depth) параметрийн ROC муруй



18-р зураг. Random Forest (n_estimators) параметрийн ROC муруй

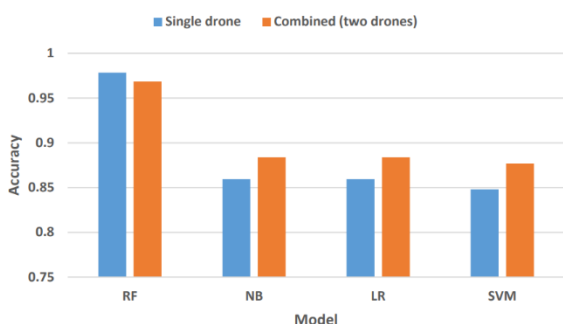
ROC-AUC шинжилгээний дүнгээс харахад Random Forest загвар хамгийн өндөр AUC (0.97)-тэй байсан бол SVM 0.88, Naïve Bayes 0.86 үзүүлэлттэй байв. Энэ нь RF загвар илүү дасан зохицох чадвартай, өндөр хэмжээсийн өгөгдөлд илүү сайн ажиллаж байгааг илтгэнэ [1].

Судалгааны дараагийн шатанд олон төрлийн дрон өгөгдлийг (Phantom 3, Inspire 1, Mavic Pro) нэгтгэн туршилт хийж, нэг төрлийн дрон өгөгдөл дээрх үр дүнтэй харьцуулсан. Хүснэгт 6 болон Зураг 13-д

харуулсанчлан Random Forest загвар олон төрлийн өгөгдөлд 97.8% нарийвчлалтай байсан нь өмнөх туршилтаас $\approx 10\%$ -иар сайжирсан. Энэ нь RF загварын generalization буюу ерөнхий чадвар илүү сайн болсон, өөр өөр дроны өгөгдөлд дасан зохицох боломжтойг харуулж байна.

Classifier	Accuracy	Precision	Recall	Training Time
RF	0.9686	0.8919	0.7905	1.3088
NB	0.8837	0.4679	0.9639	0.0458
LR	0.8837	0.4679	0.9639	1.0421
SVM (10,000 samples)	0.877	0.4261	0.9781	155.509

19-р зураг. Олон дрон өгөгдлийн багц дээрх илрүүлэлтийн үр дүн



20-р зураг. Олон ба нэг дрон өгөгдлийн туршилтын нарийвчлалын харьцуулалт

SVM загвар нь олон төрлийн өгөгдөл дээр 88.1%, Naïve Bayes 86.4%-ийн үр дүн үзүүлсэн бол Linear Regression загвар илүү тогтворгүй гарсан. Random Forest загварын давуу тал нь дроны төрөл, нислэгийн нөхцөл, цаг агаарын ялгаа зэргийг үл харгалзан хэвийн болон халдлагын төлөвийг ялгаж чадсан явдал байв.

Confusion matrix шинжилгээгээр GPS spoofing төрлийн халдлагад false negative алдаа богино хугацаанд (2–3 секунд) төвлөрч байв. Энэ нь GPS-ийн тасалдал хэт богино байх үед систем түүнийг хэвийн дохионоос ялгах боломж багатай байсныг илтгэнэ. DoS төрлийн халдлагын үед RC frame_lost утга тасалдахад хуурамч эерэг илрүүлэлт илүү гарч байв. Энэ нь салхи, цаг агаар, эсвэл радио долгионы сөрөг нөлөөтэй холбоотой байж болох юм. Ийм алдааг багасгахын тулд ирээдүйд Adaptive Windowing ба Context-aware Feature Fusion зэрэг аргыг хэрэглэх нь илүү үр дүнтэй болохыг судалгаанд санал болгожээ [1,5].

Эдгээр үр дүнгүүдийн дүн шинжилгээ нь дараах гол дүгнэлтэд хүргэж байна. Нэгдүгээрт, Random Forest алгоритм нь хамгийн өндөр гүйцэтгэлтэй буюу нарийвчлал 97%, AUC 0.97 үзүүлсэн нь нислэгийн лог өгөгдлийн динамик өөрчлөлтийг сайн ялгаж байгааг нотолсон. Хоёрдугаарт, цаг хугацааны хамааралтай өгөгдөл суурилсан feature extraction арга нь GPS, мотор, RC өгөгдлийг уялдуулан халдлагын шинж тэмдгийг илүү сайн илрүүлж өгсөн. Гуравдугаарт, ROC муруйн шинжилгээ нь моделийн overfitting-ийг багасгаж, хамгийн оновчтой параметруудийг тодорхойлоход тусалсан.

Дөрөвдүгээрт, олон төрлийн дрон өгөгдлийн туршилтаар моделийн generalization чадвар сайжирсан нь дроны төрөл бүрийн өгөгдөлд дасан зохицох чадвартай болохыг харуулсан. Тавдугаарт, энэхүү системийг бодит цагийн илрүүлэлтэд хэрэгжүүлэхэд Google Colab, Raspberry Pi, эсвэл edge AI платформ ашиглах боломжтой гэдгийг судалгаа харуулж байна.

Эцэст нь, энэхүү судалгаагаар батлагдсан ML суурь илрүүлэлтийн систем нь дроны нислэгийн лог өгөгдөлд суурилсан кибер халдлагын илрүүлэлтийн үр дүнтэй арга байж болохыг харуулсан юм. Энэ аргачлал нь зөвхөн дроны системд бус, мөн IoT болон ухаалаг хотын агаарын орчны аюулгүй байдлын системд хэрэгжиж болохыг практик суурь шийдэл болж чадна. Цаашдын судалгаанд гүн сургалтын (LSTM, CNN) аргуудыг ашиглан нислэгийн лог өгөгдлийн урт дарааллыг илүү нарийн боловсруулах, мөн дроны C&C сувгийг хослуулсан hybrid илрүүлэлтийн систем хөгжүүлэх боломжтой гэж үзэж байна [1,5,7].

ДҮГНЭЛТ

Энэхүү судалгааны ажлын хүрээнд дронуудад чиглэсэн кибер халдлагыг илрүүлэх зорилгоор машин сургалтын арга зүйг ашигласан бөгөөд бодит нислэгийн өгөгдөл дээр тулгуурласан туршилтын үр дүнгээр Random Forest алгоритм хамгийн өндөр гүйцэтгэлтэй болох нь батлагдлаа. Судалгаанд ашигласан VTO Labs-ийн DJI дроны нислэгийн лог өгөгдөл нь GPS spoofing, DoS, motor shutdown зэрэг халдлагын нөхцөлүүдийг багтаасан ба эдгээр өгөгдөлд дүн шинжилгээ хийснээр дроны системийн хэвийн болон халдлагын төлөвийг ялгах боломжтой загвар боловсруулагдсан юм.

Random Forest алгоритм нь 97% нарийвчлал, 0.97 AUC үзүүлэлттэй гарсан нь өгөгдлийн олон талт шинж чанарыг үр дүнтэй ашиглаж буйг харуулсан. SVM, Naïve Bayes, Linear Regression зэрэг бусад алгоритмуудтай харьцуулахад RF нь илүү тогтвортой, бага overfitting-тэй байсан бөгөөд олон төрлийн дроны өгөгдөлд (Phantom, Mavic, Inspire) дасан зохицох чадварыг харуулсан [1].

Туршилтын үр дүнгээс үзэхэд, дроны кибер халдлагыг илрүүлэхэд нислэгийн лог өгөгдөлд суурилсан ML аргуудын үр ашиг өндөр бөгөөд бодит цагийн илрүүлэлтэд хэрэгжүүлэх боломжтой болохыг харуулсан. Ийм системийг edge AI төхөөрөмж (жишээлбэл, Raspberry Pi) эсвэл үүлэн тооцооллын орчинд нэвтрүүлснээр дронуудын нислэгийн аюулгүй байдлыг бодит цагт хамгаалах боломж бүрдэнэ [1,5,7]. Ирээдүйд энэхүү судалгааг гүн сургалтын аргуудаар (LSTM, CNN) өргөжүүлж, дараалсан өгөгдлийн урт хугацааны хамаарлыг илүү нарийн боловсруулах, мөн дроны удирдлагын сувгийн (C&C) зан төлөвийг нэгтгэсэн hybrid илрүүлэлтийн систем хөгжүүлэх нь зүйтэй. Энэ нь зөвхөн дроны системийн кибер хамгаалалтад төдийгүй, ухаалаг хотын агаарын орчны аюулгүй

байдлын цогц экосистемийг бүрдүүлэхэд чухал ач холбогдолтой юм [7].

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Singh, M., Baig, Z., & Verma, A. (2022). *Drone Cyber Attack Detection through Machine Learning*. *Future Internet*, 14(7), 205. <https://doi.org/10.3390/fi14070205>
- [2] DJI (2018). *Flight Records Analysis Tutorial*. DJI Official Documentation. <https://www.dji.com/>
- [3] VTO Labs (2020). *Drone Forensics Dataset*.
- [4] You, H., Yim, K., Sharma, V., & Cho, J.-H. (2018). *AI-Driven Cybersecurity: Opportunities and Challenges*. In *Proceedings of the IEEE Pacific Rim Dependable Computing Conference (PRDC)* (pp. 45–52). IEEE.
- [5] Mekala, S. H., & Baig, Z. (2019). *Digital Forensics for Drone Data — Intelligent Clustering Using Self-Organizing Maps*. *Digital Investigation*, 29, S78–S87.
- [6] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... Duchesnay, E. (2011). *Scikit-learn: Machine Learning in Python*. *Journal of Machine Learning Research*, 12, 2825–2830. <https://jmlr.org/papers/v12/pedregosa11a.html>
- [7] Liu, C., Zhou, Z., & Wang, H. (2017). *Generalising Random Forest Parameter Optimisation to Include Stability and Cost*. In *Proceedings of ECML PKDD 2017*. Springer.

УТАСГҮЙ СҮЛЖЭЭНИЙ ХУРД, ЧАНАР, АЮУЛГҮЙ БАЙДЛЫН СУДАЛГАА

Зоригтбаатарын Мөнх-Эрдэнэ¹, Ганзоригын Ганбаяр¹, Ямхины Дашдорж²

^{1,2}Монгол улс, Улаанбаатар, Шинжлэх ухаан технологийн их сургууль, Мэдээлэл, холбооны технологийн сургууль, Кибер аюулгүй байдлын тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: z.monherdene22@gmail.com¹

Хураангуй: Энэхүү судалгааны ажил нь ШУТИС-МХТС-ийн WiFi сүлжээний гүйцэтгэл, чанар, аюулгүй байдлын түвшинг судлан үнэлэхэд чиглэгдсэн. Судалгаанд сүлжээний бодит хурд, чанар, найдвартай ажиллагааг онолын үндэстэйгээр харьцуулж, үр ашиг, алдагдал болон гүйцэтгэлийн бууралтын шалтгаануудыг тодорхойлсон. Туршилтанд WiFi сүлжээний гүйцэтгэлийг гурван үндсэн параметрээр хэмжсэн: Download Speed, Upload Speed, Ping. Судалгаагаар сүлжээний хурд, тогтвортой байдал нь чиглүүлэгчээс төхөөрөмж хүртэлх зай, орчны саад бэрхшээлээс шууд хамаарах нь тогтоогдсон. 5 метр, 10 метр, 50 метрийн зайд гүйцэтгэлийг хэмжихэд, ойр байрлах үед Download болон Upload хурд хамгийн өндөр, Ping хамгийн бага байсан бол хол зайд хурд буурч, Ping нэмэгдсэн нь зай болон радио дохионы саад сүлжээний чанарт шууд нөлөөлдгийг харууллаа. Аюулгүй байдлын үнэлгээгээр WPA2 протоколын сул талууд, 802.11ас стандартын онцлогийг судалж, сайжруулах арга замуудыг санал болгосон. Судалгааны үр дүн нь МХТС-ийн утасгүй сүлжээний дэд бүтцийг сайжруулах, аюулгүй байдлыг боловсронгуй болгоход чухал ач холбогдолтой юм.

Түлхүүр үг: Сүлжээний гүйцэтгэл, аюулгүй байдал, хурд хэмжилт, протоколын судалгаа, дэд бүтэц

I. УДИРТГАЛ

Орчин үеийн их дээд сургуулиудын сүлжээний дэд бүтэц нь боловсролын үйл ажиллагааг дэмжихэд чухал үүрэг гүйцэтгэдэг. ШУТИС-ийн WiFi сүлжээ нь оюутнууд, багш нарын өдөр тутмын үйл ажиллагаанд зайлшгүй шаардлагатай болсон. Гэвч сүүлийн жилүүдэд сүлжээний хурдны асуудал, аюулгүй байдлын дутагдал илэрч байгаа нь судалгааны ажлыг шаардлагатай болгосон. Энэхүү судалгааны ажил нь ШУТИС-ийн WiFi сүлжээний одоогийн төлөв байдлыг шинжлэх ухааны үндэслэлтэй үнэлэх, сайжруулах аргачлалыг боловсруулахад чиглэгдсэн. Судалгааны үндсэн зорилтууд нь WiFi сүлжээний хурд, чанарыг Шэнноны онолыг ашиглан үнэлэх, аюулгүй байдлын сул цэгүүдийг тогтоох, сүлжээний гүйцэтгэлийг оновчтой болгох аргачлалыг санал болгох юм.

A. Шэнноны онолын хэрэглээ

Судалгаанд Шэнноны мэдээлэл дамжуулах онолыг ашиглан WiFi сүлжээний онолын багтаамжийг тооцоолсон. WiFi сувгийн өргөн, дохионы хүч чадал, чангадлын түвшин зэрэг параметруудийг харьцуулан шинжилсэн. Судалгаанд 2.4 ГГц ба 5 ГГц давтамжын мужууд дахь WiFi стандартуудыг харьцуулан судалсан.

B. Туршилтын арга

Туршилтыг дараах алхмуудаар гүйцэтгэсэн. Нэгдүгээрт, сүлжээний төхөөрөмжүүдийн гүйцэтгэлийн үзүүлэлтүүдийг цуглуулсан. Хоёрдугаарт, бодит хэрэглээний нөхцөлд хурд хэмжилт явуулсан. Гуравдугаарт, аюулгүй байдлын туршилтуудыг хийсэн. Дөрөвдүгээрт, олж авсан үр дүнгээр дүн шинжилгээ хийсэн.

C. Хэмжилтийн байршил ба нөхцөл

Хэмжилтийг ШУТИС-ийн 6-р байрны өөр өөр давхарт, өөр өөр цагийн хуваарьтай явуулсан. Хэмжилтийн байршлуудад ангиудын өрөө, номын сан, оюутны чөлөө зэрэг орсон. Хэмжилтийг өдрийн 8 цагаас 22 цаг хүртэлх хугацаанд 2 цаг тутамд гүйцэтгэсэн.

2-Р ХҮЧЭГТ

Time	AVG Download Speed	AVG Upload Speed	AVG Ping
8:00AM – 9:00AM	174.11 mbps	140.83 mbps	53.56 ms
12:00PM - 13:00PM	33.37 mbps	41.68 mbps	55.02 ms
16:00PM – 17:00PM	94.72 mbps	150.86 mbps	48.89 ms

ХЭМЖИЛТ

II. СУДАЛГААНЫ ҮР ДҮН

A. WiFi хурдны судалгаа

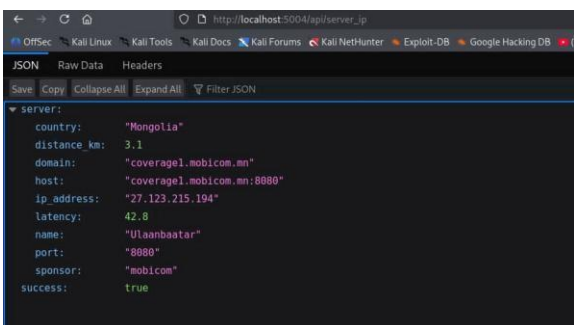
Судалгааны үр дүнгээр WiFi сүлжээний бодит хурд нь онолын хурдаас дунджаар 25 хувиар бага байгаа нь тогтоогдсон. Энэхүү зөрүү нь сүлжээний архитектур, тохиргооны параметр, орчны нөлөө зэргээс үүдэлтэй. Тусгайлан судалсан байршлуудаас 3 давхарын WiFi сүлжээний үр ашиг хамгийн өндөр буюу 88.9 хувьтай байхад оюутны чөлөөнд энэ



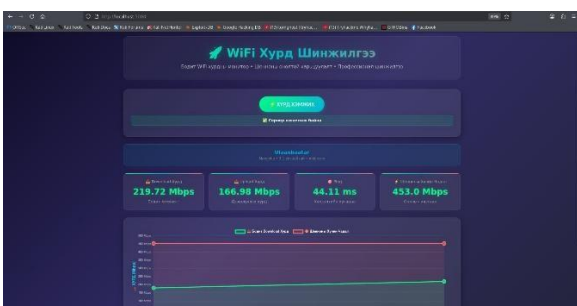
1-р зураг. WiFi хэмжилтийн үр дүн



2-р зураг. Wifi сүлжээний хурд Speedtest.com



3-р зураг. Серверийн техникийн үзүүлэлтүүд



4-р зураг. Сүлжээний хэмжилт

1-Р ХҮСНЭГТ WIFI ХУРДНЫ ХАРЬЦУУЛАЛТ

Байршил	Онолын хурд	Бодит хурд	Үр ашиг
Номын сан	433 Мбит/с	385 Мбит/с	88.9%
Анги	433 Мбит/с	342 Мбит/с	78.9%
Нийтийн хэсэг	150 Мбит/с	112 Мбит/с	74.7%

III. АЮУЛГҮЙ БАЙДЛЫН ҮНЭЛГЭЭ

ШУТИС-МХТС одоогоор Wi-Fi сүлжээний суурь хэлбэрт 802.11ac (Wi-Fi 5) стандартыг ашиглан дотоод сүлжээг өндөр хурд, тогтвортой байдлаар хангаж, аюулгүй байдалд WPA2 аутентификаци ба шифрлэлийн протоколыг хэрэглэж байна.

WPA2-PSK тохиргоонд 4-way handshake-ийг барьж авсан тохиолдолд offline brute-force халдлага хийх боломжтой тул богино, сул нууц үг ашиглах нь танд хохирол авчирна. KRACK зэрэг хэрэгжилтийн түвшний эмзэг байдлууд нь

шинэчлэлт хийгдээгүй төхөөрөмжүүдэд нөлөөлдөг. Удирдлагын кадруудыг хамгаалахгүй үед deauth flood халдлагад өртөх боломжтой хэвээр байдаг. Эдгээр эрсдлийг бууруулахын тулд PMF-ийг идэвхжүүлэх, WEP/TKIP-ийг бүрэн хориглох, firmware-ийг тогтмол шинэчлэх, урт ба хүчтэй passphrase ашиглах эсвэл WPA2-Enterprise болон WPA3 руу шилжихийг зөвлөж байна.

802.11ac нь 5 GHz зурваст ажилладаг тул радио орчны хөндлөнгийн нөлөө, давхцал бага байгаа нь сүлжээний тогтвортой ажиллагаа, хурдыг мэдэгдэхүйц нэмэгдүүлдэг. Beamforming болон олон сувагт дамжуулалтын MIMO технологийг ашигласнаар өгөгдлийн дамжуулалтын чанар, хүртээмжийг сайжруулдаг. Дамжуулалтын өндөр хурд нь шифрлэлтийн алгоритм болон аюулгүй байдлын нэмэлт механизмуудыг илүү хүчин чадалтайгаар ашиглах боломжийг олгож, WPA2 болон WPA3 протоколуудтай бүрэн нийцдэг. С. Сүлжээний гүйцэтгэл

Сүлжээний төхөөрөмжүүдийн гүйцэтгэлийн судалгаагаар үндсэн унтралгуудын CPU ашиглалт 50 хувиас дээш байгаа нь тогтоогдсон. Энэ нь сүлжээний ачаалал нэмэгдэх үед гүйцэтгэл буурах эрсдэлтэй байгааг харуулж байна.

ДУГНЭЛТ

Манай сургуулийн Wi-Fi сүлжээний гүйцэтгэлд хийсэн судалгаагаар, сүлжээний хурд, тогтвортой байдал нь чиглүүлэгчээс төхөөрөмж хүртэлх зай, орчны саад бэрхшээлээс шууд хамаарах нь тодорхой болсон. Туршилтаар 5 метр, 10 метр, 50 метрийн зайд гүйцэтгэлийг хэмжихэд, ойр байрлах үед Download болон Upload хурд хамгийн өндөр, Ping хамгийн бага байсан бол хол зайд хурд буурч, Ping нэмэгдсэн нь зай болон радио дохионы саад сүлжээний чанарт шууд нөлөөлдгийг харууллаа.

Судалгаагаар 802.11ac стандартаар ажилладаг, WPA2 хамгаалалттай Wi-Fi сүлжээ нь өндөр хурдтай, найдвартай холболттой хэдий ч аюулгүй байдлын талаас тодорхой төрлийн халдлагад өртөмгийг болох нь илэрлээ. Тухайлбал, дараах халдлагууд хамгийн үр дүнтэйд тооцогддог:

- KRACK (Key Reinstallation Attack)
- Dictionary болон Brute-force халдлага
- Deauthentication халдлага
- Rogue Access Point / Evil Twin халдлага
- WPS болон хуучин шифрлэлтийн сул талууд

Виртуал орчинд сургуулийн сүлжээтэй ижил тохиргоотой 802.11ac, WPA2 стандарттай router дээр туршилт хийж, Deauthentication болон Brute-force төрлийн халдлагуудыг туршсан. Сүлжээний нууц үг нь 14 ширхэг тэмдэгт үсгээс бүрдсэн байсан бөгөөд brute-force халдлага амжилтгүй болж, хамгаалалт хангалттай түвшинд байгааг харуулсан. Харин Deauthentication халдлага нь хэрэглэгчийн холболтыг түр тасалдуулж, handshake мэдээлэл

барих боломжийг олгосон. Судалгаанд Speedtest.net, Python скрипт, Ping, Wireshark зэрэг хэрэгслүүдийг ашигласнаар сүлжээний гүйцэтгэл болон аюулгүй байдлыг үнэн зөв, нарийвчлалтай үнэлэх боломж бүрдсэн. Дүгнэж хэлэхэд, Wi-Fi сүлжээний найдвартай ажиллагаа ба аюулгүй байдлыг сайжруулахын тулд WPA3 хамгаалалт руу шилжих, 802.11w идэвхжүүлэх, WPS-ийг хаах, range extender ашиглах, мөн нууц үгийн хүчийг хадгалах нь зүйтэй юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529–551, April 1955.
- [2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in *Magnetism*, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

НРС ЛАБОРАТОРИЙН ЭРЧИМ ХҮЧНИЙ ХЭМНЭЛТИЙН СУДАЛГАА

Цэнд-Аюушийн СУВД-ЭРДЭНЭ¹, Тэгшдоржийн АЛТАНСУВД², Зундуйн БУЯНХИШИГ³

^{1,2,3}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбоо технологийн сургууль, Холбооны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: tsendayushsuvderdene05@gmail.com¹

Хураангуй: ШУТИС МХТС – ийн High Performance Computing лабораторийн эрчим хүчний зарцуулалтыг тооцоолж, температурын зөрүү үүсэхэд хэр их хэмжээний цахилгаан зарцуулалт ба эдийн засгийн үр ашгийн тооцоолол хийв. Энэхүү судалгааны зорилго нь ШУТИС МХТС - ийн High Performance Computing (HPC) лабораторийн системийн эрчим хүчний хэрэглээг шинжлэх, дутагдалтай талуудыг тодорхойлон эрчим хүч хэмнэлт, хөргөлтийн үр ашгийг сайжруулах практик шийдлүүдийг санал болгох явдал байв. Судалгаанд лабораторийн дотоод мониторингийн өгөгдөл (серверийн ачаалал, орчны температур, цахилгаан хэрэглээ) болон CRAC/хөргөлтийн системийн функцийн үр ашгийг ашиглан аналитик тооцоо хийв. Судалгааны үр дүнгээр серверийн ачааллын динамикт нийцсэн рафк зохион байгуулалтын сайжруулалт (hot/cold aisle containment) аргуудын хэрэгжилтээр нийт системийн эрчим хүчний зарцуулалтыг дунджаар 10–30% хүртэл бууруулж болохыг тогтоов. Нэмэлтээр, CRAC-ийн setpoint-ыг 1°C-аар дээшлүүлэхэд хөргөлтийн энергид 3–5%-ийн хэмнэлтийг авчирч болох бөгөөд free-cooling ашиглах боломжтой улиралд илүү өндөр үр ашиг хүлээгдэнэ. Энэхүү судалгаа нь HPC лабораториудын энерги менежмент, дата төвийн зохион байгуулалт, болон ногоон дата төвийн бодлого боловсруулахад практик үндэс болж өгнө.

Түлхүүр үг: HPC, эрчим хүч, зарцуулалт, хэмнэлт

I. УДИРТГАЛ

Орчин үеийн их өгөгдлийн тооцоолол, судалгаа, машин сургалтын болон шинжлэх ухааны тооцооллууд их хэмжээний тоон өгөгдлийг хурдан боловсруулдаг тул High Performance Computing (HPC) лаборатори нь их хэмжээний цахилгаан эрчим хүч, хөргөлт, дэд бүтэц шаарддаг. Монгол Улсын нөхцөлд, ихэнх их сургууль, судалгааны байгууллагын HPC орчин нь төсөв, байр, техник хангамж, эрчим хүчний хязгаарлагдмал нөөцтэй тул эдгээр системийн эрчим хүчний үр ашиг, найдвартай ажиллагааг сайжруулах нь эдийн засаг, судалгааны үр өгөөжийн хувьд чухал ач холбогдолтой.

Энэхүү судалгааны зорилго нь ШУТИС-ийн Мэдээлэл, Харилцаа Холбооны Технологийн Сургууль (МХТС) дэх High Performance Computing лабораторийн цахилгаан зарцуулалтыг шинжлэх, лабораторийн дотоод нөхцөл (серверийн ачаалал, орчны температур, нийт хэрэглээ) - ийн нөлөөг тодорхойлох, мөн хөргөлтийн систем, ракуудын байршилтай холбоотой алдааг оношлон энерги хэмнэх практик шийдлүүдийг санал болгох явдал юм.

Судалгаанд лабораторийн мөрдөн хяналтын өгөгдөл, төхөөрөмжийн техникийн үзүүлэлт, стандарт (PUE) болон холбогдох судалгааны харьцуулалтуудыг ашиглан аналитик тооцоо хийсэн. Тухайн тооцооллын үндсэн өгөгдөлд 9 сарын хугацаанд бүртгэгдсэн нийт 180,480 кВт·ц хэрэглээ, 17 ширхэг сервер (10 CPU, 4 GPU, 3 storage) орсон ба IT ба хөргөлтийн бүрэлдэхүүнийг тодруулан шинжилсэн. Судалгааны үр дүнд лабораторийн дэд бүтцийн зохион байгуулалт, CRAC-ийн setpoint, hot/cold aisle containment зэрэг аргаар энергийн хэрэглээг бууруулах боломжтойг тоон

хувилбаруудтай харуулж байна. Энэхүү ажил нь сургалтын болон судалгааны зориулалттай HPC орчны энерги менежментийн практик удирдамж болоход чиглэнэ.

II. ХОЛБООТОЙ СУДАЛГАА

A. Цахилгаан эрчим хүч (ЦЭХ)

Ерөнхий бүтэц ба үйл ажиллагаа: Түлш шатаах → уур үүсгэх → турбин эргүүлэх → цахилгаан үйлдвэрлэх → дулаан гадагшлуулах дахин эргэлт хийх.

Гол бүрдэл хэсгүүд:

- Түлш боловсруулах систем: Түлш тээвэрлэх, нүүрс бутлах, бойлер руу илгээх. Түлшний чанар үр ашгийг 10-15% нөлөөлнө.
- Бойлер: Түлш шатааж уур үүсгэнэ. Супер хитер, экономайзер ашигладаг.
- Турбин: Уурыг эргүүлж механик энерги үүсгэнэ (үр ашиг 85-90%).
- Генератор: Механик энергийг цахилгаанд хувиргаж, 11-22 кВ-ийн хүчдэл үйлдвэрлэнэ.
- Конденсер: Уурыг хөргөж усаар эргүүлж, хөргөлтийн цамхаг ашиглана.
- Тэжээлийн насос: Усыг дахин бойлер руу шахна.
- Нэмэлт систем: Утаа цэвэрлэгч, хяналтын систем, цахилгаан хуваарилалт.

B. Хөргөлтийн систем

- Free cooling (Гаднах агаараар хөргөх) – Гаднах хүйтэн агаарыг ашиглан дулааныг гадагшлуулах ажиллагаатай. Ихэвчлэн гадаа хүйтэн буюу өвлийн улиралд ашигладаг хөргөлтийн системийн төрөл юм. Энэ хөргөлтийн аргыг

ашигласнаар эрчим хүчийг 50-60% хэмнэх боломжтой ба байгальд ээлтэй арга юм. Сул тал нь зуны халуунд ашиглах боломжгүй тул заавал өөр хөргөлтийн системтэй хослуулан ашиглах шаардлагатай болдог ба мөн гаднах агаарын чанарт чухал нөлөөтэй.

- Evaporative cooling (Ууршилтаар хөргөх) – Энэ хөргөлтийн системийн хамгийн гол хүчин зүйл нь хөргөгч бодис юм. Хөргөгч бодисын тусламжтайгаар дулааныг шингээж гадагшлуулах зарчмаар серверийг хөргөдөг. Энэ аргыг хэрэглэснээр цахилгаан эрчим хүчний зарцуулалт 20-60% буурах боломжтой.
- Liquid cooling(Шингэнээр хөргөх) – Шингэн буюу ус, диэлектрик шингэн зэргийг ашиглан серверүүдийн дулааныг шууд шингээн авна. Хүйтэн шингэн сервер рүү дамжин дулаан шингээгээд хөргүүрээр гадагшлуулна. Энэ хөргөлтийн системийг НРС, AI сервер зэрэг өндөр хүчин чадалтай серверүүдэд ашиглана. Энэ хөргөлтийн системийг ашигласнаар эрчим хүчийг 30-40% хэмнэх боломжтой. Энэ аргын сул тал нь суурилуулахад өндөр зардалтай ба гол шингэн алдагдалд орох эрсдэлтэй.

С. Мобиком корпораци

Мобиком Корпораци нь нийт 3 дата төвтэй. Дата төв - 1 нь Улаанбаатар хотын Хан-Уул дүүрэгт байрладаг бөгөөд нийт 40 рактай. Дата төв - 2 нь Мобиком Корпорацийн төв оффисын 1,2,3 давхруудад байрладаг, 44 рактай. Дата төв - 3 нь Дархан хотод байрладаг, 50 рактай.

Мобиком Корпораци нь ашгийн байгууллага бөгөөд дараах үйлчилгээнүүдийг явуулдаг.

- Сервер байршуулах
- Виртуал сервер түрээс
- Веб, И-мейл байршуулах
- Домайн нэр

Хөргөлтийн системүүд: Мобиком Корпораци нь Монгол улсад хамгийн анхны хөргөлтийн Tier-III стандартыг нэвтрүүлсэн байгууллага юм. Тэдний TIER III дата төвүүд free cooling голлон ашигладаг бөгөөд зуны халуунд evaporative cooling-д шилждэг. Цахилгаан эрчим хүчний хэмнэлт: Монголд эрчим хүчээ хамгийн хэмнэлттэй, ашигтайгаар зарцуулдаг тэргүүлэгч дата төв нь Мобиком Корпораци юм. Дээрх байгууллага нь цахилгаан эрчим хүчээ хэмнэхэд маш олон аргууд ашигладаг.

- Сэргээгдэх эрчим хүчийг ашиглаж эхэлсэн бөгөөд Дата төв 2 - ын гадна талбайд 580Вт-ын чадалтай 6 ширхэг нарны панел(3.5кВт) суурилуулсан. Ингэснэр нарнаас цэнэг хуримтлуулан цахилгаан эрчим хүч гаргаж авдаг болсон. Сэргээгдэх эрчим хүчнээс гаргаж авсан энэ цахилгаан эрчим хүчээр зундаа бүтэн өдөр, өвөлдөө өдрийн 50-60%-ыг цахилгаан эрчим хүчээр хангах боломжтой болсон.
- Хуурмаг ачааллыг бууруулах – Хуурмаг ачааллыг бууруулахдаа реактив хүчний

тэнцвэрлэлтийг хангах зориулалтаар конденсатор ашигладаг. Ингэснээр хуурмаг ачаалал арилж цахилгаан эрчим хүч үр ашиггүй зарцуулагдахаас сэргийлдэг.

III. АРГА ЗҮЙ

А. НРС лабораторийн цахилгаан зарцуулалт

ШУТИС МХТС – ийн 115 тоот өрөөнд байрлах 150Тb багтааж бүхий уг лабораторийн цахилгаан хангамжид хяналт тавьж ажилладаггүй бөгөөд тодорхой өдөр, сард ямар хэмжээний цахилгаан зарцуулж буйг мэдэх боломжгүй байв. Зөвхөн 9 сарын хугацаанд 180480кВт цахилгааныг зарцуулсан гэсэн мэдээлэлд үндэслэн тооцоолол хийв.

$$9 \text{ сар} = 6552 \text{ цаг}$$

$$180480 \text{ кВт} \div 6552 \text{ цаг} = 27.54 \text{ кВт/цаг} \\ \text{/арифметик дундажаар/}$$

Information Technology (IT) төхөөрөмжийн цахилгаан зарцуулалт:

Серверүүд бүрэн ачаалалтайгаар ажиллаж байна гэж үзвэл:

- CPU сервер (2U dual Xeon/EPYC) - 0.65 кВт (650W)
- GPU сервер (4U, 4x A100/H100 GPU) - 3.0 кВт (3000W)
- Storage сервер (2U 24-bay HDD) - 0.45 кВт (450W)

IT ТӨХӨӨРӨМЖҮҮДИЙН ЦАХИЛГААН ЗАРЦУУЛАЛТ

1- Р ХҮСНЭГТ.

Серверийн төрөл	Тоо	Нэг сервер (кВт)	Нийт чадал (кВт)
CPU	10	0.65	6.5
GPU	4	3	12
Storage	3	0.45	1.35
НИЙТ	17	-	19.85

IT төхөөрөмжүүд нь цахилгааны энергийн 99% нь дулааны энергид хувиргадаг тул дулаан нь:

$$19.85 \text{ кВт} \approx 19 \text{ кВт.}$$

Өгөгдлийн төв (data center)-ийн эрчим хүчний үр ашгийг PUE (Power Usage Effectiveness) - р хэмждэг.

$$PUE = \frac{\text{Нийт хэрэглэсэн ЦЭХ}}{\text{Зөвхөн IT төхөөрөмжийн хэрэглэсэн ЦЭХ}} \\ PUE = \frac{27.85 \text{ кВт}}{19.85 \text{ кВт}} = 1.4$$

PUE нь 1-1.3 маш сайн, 1.3-1.6 сайн, 1.7 – 2.0 дундаж, 2.0 – с их бол муу гэж үнэлдэг. Уг лаборатори нь сайн үзүүлэлттэй байна.

Хөргөх шаардлага:

$$19 \text{ кВт} * 1.2(20\% \text{ нөөц} + \text{ өрөөний дулаан}) = 22.8 \text{ кВт}$$

Cooling системийн цахилгаан зарцуулалт:

$$P_{cooling} = \frac{\text{Хөргөх шаардлага}}{COP}$$

Coefficient of Performance (COP) — буюу Гүйцэтгэлийн коэффициент гэдэг нь халаалт эсвэл хөргөлтийн системийн үр ашгийг илэрхийлдэг харьцаа юм.

$$COP = \frac{\text{гаралт (ашигтай дулаан эсвэл хөргөлт)}}{\text{оролт(зарцуулсан цахилгаан энерги)}}$$

Дундажаар COP = 3 гэж үзээд

$$P_{cooling} = \frac{22.8 \text{ кВт}}{3} = 7.6 \text{ кВт}$$

Light, PDU, UPS – ийн цахилгаан зарцуулалт:

MNS 6869:2020 (Мэдээлэл, харилцаа холбооны серверийн өрөөнд тавих шаардлага) болон MNS 6528:2021 (Дата төвийн дэд бүтцийн шаардлага) стандартуудын дагуу НРС төрлийн сервер өрөөнд гэрэл, PDU (Uninterruptible Distribution Panel), UPS (Uninterruptible Power Supply) - ийн нийлмэл хүчин чадлын нягт 20 Вт/м² байхаар тодорхойлогдсон байдаг.

$$P_{light,UDP,UPS} = 10 \text{ м}^2 * 0.02 \text{ кВт} = 0.2 \text{ кВт}$$

НРС лабораторийн нийт цахилгаан зарцуулалт нь:

$$P_{IT} + P_{cooling} + P_{light,UDP,UPS}$$

$$19.85 \text{ кВт} + 7.6 \text{ кВт} + 0.2 \text{ кВт} = 27.65 \text{ кВт}$$

Энэ нь дундаж 27.54 кВт цагаас их байгаа нь серверүүд бүрэн ачааллаараа ажиллаж буй гэж үзэн тооцоолсоноос үүдэн гарч байна.

Цахилгааны тарифаар тооцвол:

Албан байгууллагын цахилгааны тариф 1кВт нь 280төгрөг.

$$27.65 \text{ кВт} * 280 \text{ төгрөг} = 7742 \text{ төгрөг}$$

НРС -ИЙН НИЙТ ЦАХИЛГААНЫ ЗАРДАЛ

2- Р ХҮСНЭГТ.

Хугацаа	Цаг	кВтh	Зардал (₮)
Цаг	1	13	3,640
Өдөр	24	312	87,360
Сар	730	9490	2,657,200
Улирал	2,192	28496	7,978,880
Жил	8,760	113880	31,886,400



1-р зураг. НРС лабораторийн цахилгаан зарцуулалт

В. CRAC нь 1 градус Цельсээр бага дулааныг хөргөхөд үзүүлэх эрчим хүчний хэмнэлт

НРС орчинд CRAC-ийн хөргөлтийн зарцуулалтыг бууруулахад температурт 1°C-ийн өөрчлөлтөөр 3-5% эрчим хүчний хэмнэлт гарна. Энэ нь ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) болон ENERGY STAR-ийн судалгаанд батлагдсан бөгөөд өгөгдлийн төвийн нийт эрчим хүчний 20-40%-ийг хөргөлт эзэлдэг. Хэрвээ өрөөний дулааны температур өндөр (серверүүд илүү их дулаан ялгаруулах эсвэл гаднаас дулаан орж ирэх) бол CRAC илүү их ажиллаж, бага температуртай агаар нийлүүлэх эсвэл илүү их агаарын урсгал шаардлагатай болно. Гэхдээ CRAC-ийн хөргөлтийн температур (setpoint) нь ихэвчлэн урьдчилан тохируулагдсан бөгөөд өрөөний дулааны температураас хамаарч автоматаар өөрчлөгддөггүй, харин хөргөлтийн хүчин чадал (cooling capacity) өөрчлөгддөг.

1 ГРАДУС ЦЕЛЬСЭЭР БАГА ТЕМПЕРАТУРЫГ ХӨРГӨХӨД ҮЗҮҮЛЭХ ХЭМНЭЛТ

3- Р ХҮСНЭГТ.

Хугацаа	Хэмнэлт (кВтh)	Хэмнэлт (₮)
Цаг	0.33	92
Өдөр	7.9	2,214
Сар	240	67,329
Улирал	721	202,173
Жил	2,884	807,952

В. НРС лабораторийн цахилгаан хэмнэх аргууд

Hot/cold aisle

НРС лабораторийн өрөө нь халуун, хүйтэн агаар нь холилдон ракууд бүгд урагш харсан байрлалтайгаар зэрэгцээ оршдог хэдий ч ракийн араас гарах халуун агаарыг холихоос сэргийлэх хаалт байдаггүй. Хаалт хийхгүй байсанаар IT төхөөрөмжүүдэд шаардлагатай хөргөлт бүрэн очихгүй халалт үүсч, эвдрэл гарах эрсдэлтэй. Мөн хөргөлтийн систем илүү их ажиллах шаардлагатай болж, эрчим хүчний зардал 20-30% хүртэл өсөх

боломжтой, ялангуяа зуны улиралд. Энэ нь дулааны тэнцвэргүй байдал үүсгэж, дата центрүүдийн найдвартай байдлыг алдагдуулна.

Үүнийг шийдэхийн тулд Hot/cold aisle аргыг хэрэглэх нь зүйтэй. Hot aisle containment нь дулааны үр ашиг, ослын үед (ride-through) илүү сайн гүйцэтгэл үзүүлдэг бөгөөд дата центрүүдийн найдвартай байдлыг дээшлүүлдэг.

Нарны панел

НПС лабораторид нарны панел ашиглах нь эрчим хүчний хэрэглээг бууруулж, тогтвортой байдлыг хангах чухал шийдэл юм. Нарны эрчим хүчийг ашигласнаар цахилгааны үндсэн сүлжээнээс хамаарал багасч, зардлыг урт хугацаанд бууруулах боломжтой. Монголын уур амьсгал, жилийн турш олон цагийн нарлаг нөхцөл нь нарны системийг үр ашигтай ажиллуулах таатай нөхцөл бүрдүүлдэг. Жишээлбэл, нийт хэрэглээний 30 орчим хувийг нарны эрчим хүчээр хангаж чадвал жилд ойролцоогоор 8–10 сая төгрөгийн цахилгааны зардлыг хэмнэх боломжтой. Нарны систем нь эхний хөрөнгө оруулалт өндөртэй боловч 4–6 жилийн дотор өөрийн өртгөө нөхдөг. Үүний дараа үйлдвэрлэх эрчим хүч нь үндсэндээ үнэ төлбөргүй болж, лабораторийн тогтвортой ажиллагааг дэмжинэ. Мөн нүүрстөрөгчийн ялгарлыг бууруулж, байгаль орчны эерэг нөлөө үзүүлдэг. Нарны эрчим хүчийг UPS болон батерейны системтэй уялдуулбал тасралтгүй ажиллагааг хангах давуу талтай. Энэ нь ялангуяа цахилгааны тасалдал гарах эрсдэлтэй нөхцөлд лабораторийн серверүүдийг хамгаална. Иймд нарны панел ашиглах нь эдийн засгийн хувьд үр ашигтай, байгальд ээлтэй, тогтвортой хөгжлийн бодлогод нийцсэн шийдэл юм.

НОТ/COLD AISLE БОЛОН НАРНЫ ПАНЕЛ АШИГЛАЛТЫН ХЭМНЭЛТ

4-Р ХҮСНЭГТ.

Хугацаа	Hot/Cold aisle (25%) хэмнэлт (₮)	Нарны панел (30%) хэмнэлт (₮)
Цаг	3,640	910
Өдөр	87,360	21,840
Сар	2,657,200	664,300
Улирал	7,978,880	1,994,720
Жил	31,886,400	7,971,600

ДҮГНЭЛТ

Судалгааны үр дүнгээс үзэхэд НПС лабораторийн цахилгаан эрчим хүчний хэрэглээ өндөр байгаа нь дэд бүтцийн үр ашиггүй зохион байгуулалттай шууд холбоотой байв. Нийт хэрэглээний 71.7 хувь нь IT

төхөөрөмжөөс, 27.49 хувь нь хөргөлтийн системээс шалтгаалж байсан нь сайжруулах боломж байгааг харууллаа. Ракийг буруу байршуулсан, халуун ба хүйтэн агаарыг тусгаарлаагүй зэрэг нь хөргөлтийн үр ашгийг бууруулж байна. Hot/cold aisle containment хэрэгжүүлснээр 10–30 хувийн эрчим хүчний хэмнэлт гаргах боломжтойг тооцоолсон. Мөн CRAC-ийн температурын тохиргоог 1–3°C-аар өсгөхөд хөргөлтийн зардал 3–5 хувиар буурах боломжтой.

Сэргээгдэх эрчим хүчний эх үүсвэр болох нарны панелийг нэвтрүүлснээр хэрэглээний 20–40 хувийг хангах боломжтой. Энэ нь жилд ойролцоогоор 8–10 сая төгрөгийн зардал хэмнэхээс гадна нүүрстөрөгчийн ялгарлыг бууруулна. Нарны системийн анхны хөрөнгө оруулалт 4–6 жилийн дотор нөхөгдөж, дараа нь үнэ төлбөргүй эрчим хүч нийлүүлэх боломж бүрдэнэ.

MOBICOM CORPORATION бол ашгийн байгууллага учраас цахилгаан зарцуулалтаа маш сайн хянадаг. Гэтэл MХТС нь ашгийн бус байгууллага учраас цахилгаан зарцуулалтдаа хяналт тавьж ажилладаггүй. Хамгийн чухал нь эрчим хүч бол хязгаарлагдмал нөөц учраас байгууллага бүр серверт зарцуулах цахилгаанаа хянаж ажиллаваас ирээдүйд бид тог цахилгааны хомсалд орохгүй байх боломжтой.

Хөргөлтийн систем, эрчим хүчний удирдлагыг технологитой уялдуулах нь ирээдүйн үр ашигтай шийдэл болохыг судалгаа харууллаа. Дээрх арга хэмжээг шат дараатай хэрэгжүүлснээр лабораторийн ажиллагааны найдвартай байдал, үр ашиг сайжирна. Цаашид цаг тутмын энерги мониторинг, PUE-ийн нарийвчилсан хяналтыг нэвтрүүлэх шаардлагатай. Ингэснээр НПС лаборатори нь тогтвортой, байгальд ээлтэй, эдийн засгийн хувьд үр ашигтай систем болж хөгжих бүрэн боломжтой юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Mobicom Corporation. (n.d.). Мобиком Корпораци. Retrieved October 28, 2025,
 [2] OpenAI, ChatGPT (GPT-5), Large language model, 2025. [Online].
 [3] xAI, Grok (AI chatbot), Large language model, 2025. [Online].
 [4] R. Buyya, C. Vecchiola, and S. Selvi, Mastering Cloud Computing: Foundations and Applications Programming. Amsterdam, The Netherlands : Elsevier, 2013 он
 [5] BT. V. Heddeghem, “Trends in BworldBride ICT electricity consumption from 2007 to 2012,” Comput. Commun., vol. 50, pp. 64–76, Sep. 2014 он.

БИО-АНАГААХЫН РАДИО ДОЛГИОН ДЭЭР ЭЛЭГНИЙ ХОРТ ХАВДРЫГ ИЛРҮҮЛЭХ МЭДРҮҮР АНТЕНЫ СУДАЛГАА

Хүрэлсүх ЕСӨН-ЭРДЭНЭ¹, Батбаатар ЗАГАРСҮРЭН¹, Баярсайхан ПҮРЭВЦЭРЭН², Пүрэвдорж УУГАНБАЯР²

^{1,2}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Холбооны инженерчлэлийн ТЭНХИМ

Холбоо барих зохиогчийн и-мэйл хаяг: zagarsuren0109@gmail.com¹

Хураангуй— Элэгний хорт хавдрыг бичил долгионы техникийг ашиглаж илрүүлэх бага оврын урвуу F антенны загварыг танилцууллаа. Антен нь 401-406 МГц-ийн эмнэлгийн төхөөрөмж (Medradio)-ийн зурваст загварчлагдсан. Санал болгож буй антенны ойлтын коэффициентын симуляцын үр дүнгээс харахад резонансны давтамжийн шилжилтээр хорт хавдартай биеийг эрүүл биеэс ялгаж мэдрэхээс гадна хавдрын өөр өөр үе шатуудад антенны ойлтын коэффициентын утга - 27.4 дБ-с -29дБ хооронд өөрчлөгдөж байгаа учир тус антенны тусламжтайгаар хорт хавдрын үе шатуудыг ялгаж чадаж байна.

Түлхүүр үг—Элэгний эсийн хорт хавдар, хавтгай урвуу F антен

I. ОРШИЛ

Элэгний эсийн хорт хавдар (НСС) нь дэлхий даяар тохиолддог тав дахь хамгийн түгээмэл неоплазм (хэвийн бус эдийн өсөлт) бөгөөд зарим бүс нутагт хорт хавдартай холбоотой нас баралтын үндсэн шалтгаан болдог [1]. Элэгний хорт хавдарт холангиокарцинома (cholangiocarcinoma), ангиосаркома (angiosarcoma), элэгний эсийн хорт хавдар (hepatocellular carcinoma) гэсэн төрлүүд байдаг ба эдгээрээс хамгийн түгээмэл нь элэгний эсийн хорт хавдар юм [2]. Эдгээр төрлийн хорт хавдрууд нь бүх насанд тохиолддог бөгөөд хүний биед хөнөөлтэй тул эрт илрүүлэх шаардлагатай байдаг. Элэгний эсийн хорт хавдрыг цусны дээжийн шинжилгээ, компьютер томограф (СТ), соронзон резонансын дүрслэл (MRI), хэт авианы дүрслэл (US) зэрэг аргуудаар оношилж болно [3]. Мөн элэгний биопсигоор тухайн хүний элэгнээс дээж авч микроскопоор ажиглах, туршилт зэргийг гүйцэтгэж хавдрыг оношилно. Эдгээр бүх хавдрыг илрүүлэх аргууд нь хүний биеийн бүхий л хэсэгт гүйцэтгэгдэх боломжтой ба нарийн шинжилгээ хийгддэг. Гэвч эдгээр нь өртөг өндөртэй, олон удаа шинжилгээнд орох боломжгүй байдаг сул талуудтай.

Сүүлийн жилүүдэд антенаар хорт хавдар илрүүлэх аргууд түгээмэл судлагдаж байна [5], [6]. Бичил долгионы дүрслэл, давтамжийн шилжилт зэрэг аргууд нь хямд, нарийвчлал сайн олон удаа шинжилгээнд хамрагдах боломжийг үүсгэдэг нь гол давуу тал болж байна. Мэдрэгч антен нь давтамжийн шилжилт, цацрагийн өөрчлөлт, тусгай шингээлтийн харьцаа (SAR) зэрэг шинж чанарын өөрчлөлтөөр температур, даралт, глюкоз, чийг зэрэг мэдрэхэд хүнд зүйлсийг мэдрдэг [7]. Энэхүү өгүүлэлд элэгний хорт хавдрыг илрүүлэхэд зориулсан хавтгай урвуу F антенныг 404 МГц-ийн давтамж дээр загварчилсан. Антенныг хүний биеийн модель Густаво дээр 2 мм зайд байрлуулж үзүүлэлтүүдийг харууллаа. Ингэхдээ хавдрын 4 үе шат дээр тус тусад нь симуляцийг хийж гүйцэтгэлээ.

II. ЭЛЭГНИЙ БИЕИЙН ЗАГВАР БА ЭЛЭГНИЙ ХОРТ ХАВДАР

A. Элэгний хорт хавдар

Дэлхийн эрүүл мэндийн байгууллага (WHO) мэдээлснээр хорт хавдар нь хэвийн бус эсийн өсөлтөөс үүсдэг. Барселона клиникийн элэгний хорт хавдрын системээс (BCLC) тогтоосон стандартаар элэгний эсийн хавдрын үе шатыг тодорхойлдог. Элэгний хорт хавдрын үе шатуудад дараах зүйлс орно.

- I үе: Элэгэнд 2 см-ээс бага хэмжээтэй хавдрын эсүүд үүссэн байна. Энэ үед цусны шинжилгээнд хавдаргүй гэж гардаг.
- II үе: Элэгний эдэд 5 см ба түүнээс бага хэмжээтэй ганц хавдартай эсвэл 3 см-ээс бага хэмжээтэй нэгээс олон хавдрын голомттой. Хавдар цусаар дамжин судсанд тархсан байж магадгүй. Иймээс цусны шинжилгээнд илэрнэ.
- III үе: Энэ үе шатанд нэгээс олон хавдар тархсан ба /эсвэл 5 см-ээс дээш хэмжээтэй хавдартай байж болно/. Хавдар лимфийн зангилаа, том судас эсвэл өөр эрхтэн рүү тархсан /метастаз/ байж магадгүй.
- IV үе: Хорт хавдар нь таны уушги, яс, тунгалгийн булчирхай зэрэг биеийн бусад хэсэгт тархсан.

Зураг.1-т элэгний хорт хавдрын үе шатуудыг үзүүлэв.



1-р зураг. Элэгний хорт хавдрын үе шат

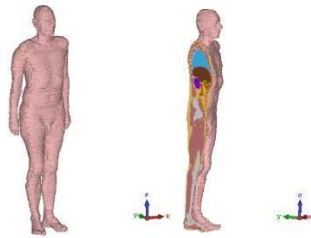
Энэхүү судалгаанд хүний биед тохиолддог хамгийн түгээмэл хавдар болох элэгний эсийн хавдрыг авч үзсэн. [12]-т буй эрэгтэй 65 настай элэгний эсийн хорт хавдартай өвчтөний

мэдээллийг ашигласан.

В. Элэгний загвар

Антен элэгний эс хоорондох үзүүлэлтийг үндэслэн нотлохын тулд CST Studio Suite программ хангамжид зураг.2-т буй хүний биеийн модель болох Густавог ашигласан. Густаво нь CST Studio suite программ хангамжид нээлттэй байдаг. Эдгээр эдийг үүсгэхдээ хүний биед бодитоор тохиолддог диэлектрик шинж чанаруудыг ашигласан [8]. Симуляцийг гүйцэтгэхдээ

моделийн хэвлийн дээд хэсгийг сонгон авч симуляцийг гүйцэтгэсэн.



2-р зураг. Хүний биеийн 3D модель Густаво

1-Р ХҮСНЭГТ. ЭЛЭГНИЙ ЗАГВАРТ АШИГЛАСАН ДИЭЛЕКТРИК ШИНЖ ЧАНАР

Шинж чанар \ Эд	Арьс	Өөх	Булчин	Элэг	Хавдрын эс
Нэвтрүүлэх чадвар	46.7	11.6	57.1	51.2	59.89
Цахилгаан дамжуулалт [C/м]	0.69	0.08	0.79	0.65	0.65
Нягт [кг/м ³]	1109	911	1090.4	1078.7	~
Дулааны дамжуулалт [Вт/°C/м]	0.37	0.21	0.49	0.51	~
Дулааны багтаамж [кЖ/К/кг]	3390.5	2348.3	3421.2	3540.2	~

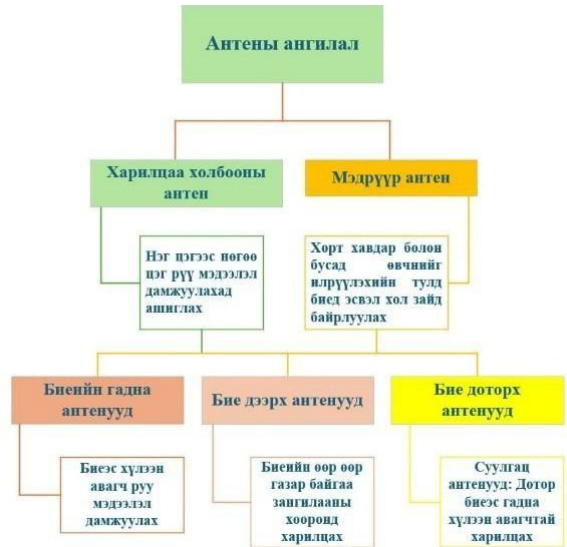
I. АНТЕНЫ ЗАГВАРЧЛАЛ

Хавдрыг илрүүлэх антенууд нь голчлон хавдрын эсийг мэдрэх болон дүрслэл хийх зорилготой бүтээгддэг. Нөгөө талаас холбооны антенуудыг эмнэлгийн төхөөрөмж, мэдрэгч, суулгац эсвэл зүүж болох төхөөрөмжүүдийн хооронд утасгүй холболт хийх зорилгоор био-анагаахын хэрэглээнд ашигладаг [4]. Зураг.3-т эдгээрийн төрлийг харуулав.

Хавдрыг илрүүлэхэд илүү бага давтамжийн зурвасыг ашиглахыг илүүд үздэг. Учир нь нам давтамжууд нь эд эсэд илүү амархан нэвтрэх чаддаг гэдгийг нэвтрэлтийн гүний тэгшитгэлд дурдсан байдаг [10]. Антен бүтээхэд долгионы уртаас хамаарч антенны загварчилдаг. Ихэвчлэн антенууд нь долгионы уртын хагастай тэнцүү хэмжээтэй байдаг [11]. Иймд антен нь

хэмжээний хувьд том болох тул антенны хэмжээг багасгах маш том асуудал үүсдэг.

3-р зураг. Био-Анагаахын антенны төрлүүд



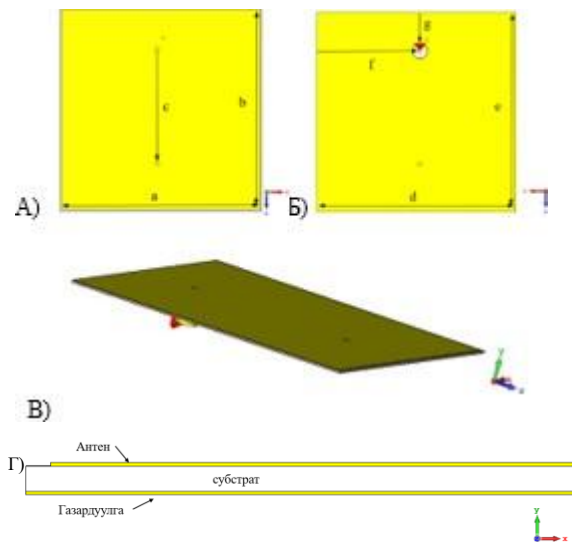
Тиймээс антен жижгэрүүлэхийн тулд өндөр диэлектрик тогтмолтой материал ашиглах, хагас долгионы антен, слот арга гэх мэт антен жижгэрүүлэх аргуудыг ашигласан [9].

2-Р ХҮСНЭГТ: ХАВТГАЙ УРВУУ F АНТЕННЫ ТЭМДЭГЛЭЭ БА ХЭЖЭЭС

Иймээс хавтгай урвуу F антенныг 401-406 МГц-ийн эмнэлгийн төхөөрөмж (Medradio)-ийн зурваст загварчилсан. Дээд болон доод хязгаар давтамжийг 0

Тэмдэглэгээ	Хэмжээ(мм)
Антенны урт, a	45.5
Антенны өргөн, b	45.5
Тэжээл слотын хоорондох зай, c	46
Газардуулгын урт, d	46
Газардуулгын өргөн, e	26
Тэжээлийн урт, f	22
Тэжээлийн өргөн, g	9

МГц-ээс 800 МГц гэж сонгосон. Антен газардуулга хоорондох материалыг Rogers 6010 гэсэн материалаар сонгож симуляци хийсэн. Материалын зузаан 0.254 мм, зэсийн зузаан 0.035 мм.

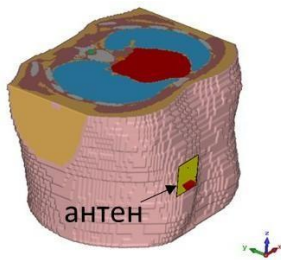


4-р зураг. Хавтгай урвуу F антен (а- нүүр, б- ар тал, в- 3D, г- хэвтээ)

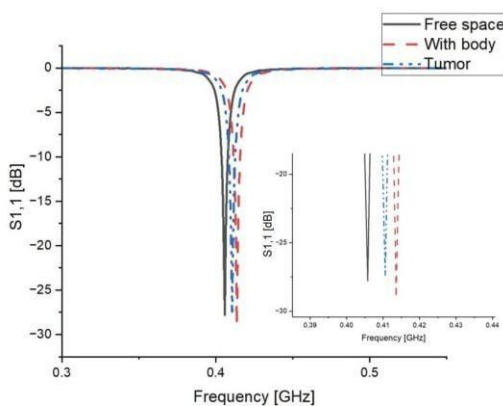
Хавтгай урвуу F антенны 3D загварыг зураг.4-т үзүүлэв. Мөн хүснэгт. II нь хавтгай урвуу F антенны тэмдэглэгээ ба хэмжээсийг харуулав.

III. СИМУЛЯЦИЙН ҮР ДҮН

Антен жижгэрүүлэх аргуудыг ашиглаж элэгний хорт хавдар илрүүлэхэд зориулсан антенныг 16 дахин жижгэрүүлсэн. Хүний биеийн модель антенны симуляцийг CST Studio Suite программын тусламжтай хийж гүйцэтгэв.



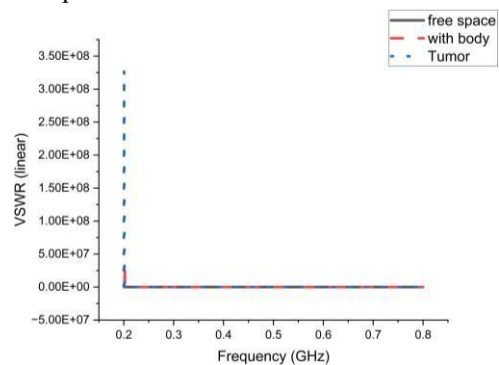
5-р зураг: Хүний биеийн цээжин хэсэгт антен байрлах байрлал



6-р зураг: Антенны ойлтын коэффициент

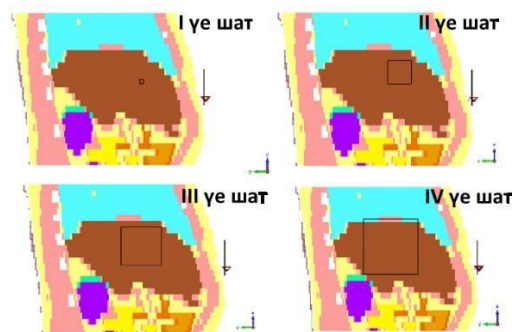
Зураг.4-т санал болгож буй антенныг хүний биеийн элэг байрладаг хэсэгт хэрхэн байрлуулахыг харуулж байна.

Антен нь хүний биед 2 мм зайтай байрлаж хавдрын шинжилгээг хийх ба энгийн дүрс оношилгоотой харьцуулахад хавдрын эсийг хавдрын эхэн үе шатанд нь мэдрэх чадвартайгаа онцлог юм. Өөрөөр хэлбэл маш бага хэмжээтэй хавдрын үүслийг цаг алдалгүй илрүүлэх боломжтой. Зураг.6-т антенныг чөлөөт орон зайд байрлуулсан, эрүүл хүний биед байрлуулсан, элэгний хорт хавдартай биед байрлуулсан зэрэг 3 ялгаатай нөхцөлд түүний ойлтын коэффициент хэрхэн өөрчлөгдөж, давтамж шилжиж байгааг үзүүлэв. Эндээс хавдар байгаа үед резонансны давтамж шилжиж антен мэдрүүр байдлаар амжилттай ажиллаж байгааг харж болно.



7-р зураг. Ялгаатай нөхцөлд антенны VSWR

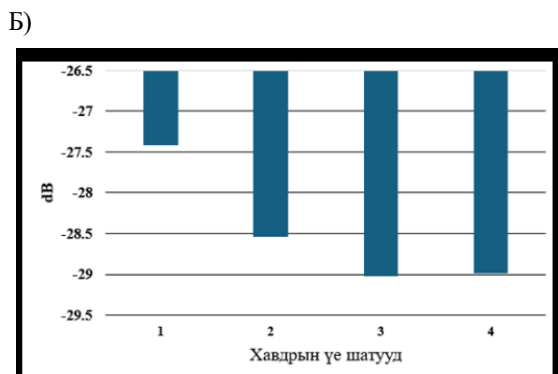
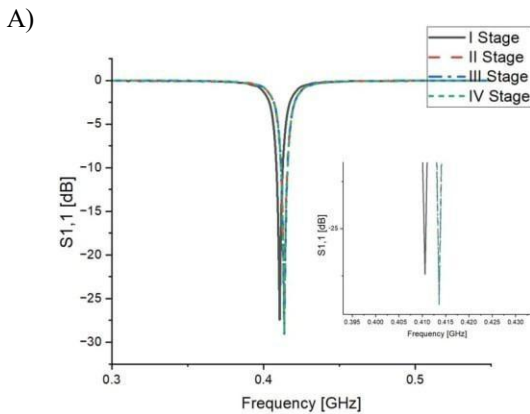
Зураг 7-оос харахад антенныг чөлөөт орон зайд байрлуулсан, эрүүл хүний биед байрлуулсан, элэгний хавдартай биед байрлуулсан зэрэг 3 ялгаатай нөхцөлд VSWR үзүүлэлт тогтвортой байгаа бөгөөд эндээс бид гадны физик шалтгааны улмаас антенны мэдрэх чадвар өөрчлөгдөхгүй тогтвортой байж чадна гэдгийг баталж болно.



Зураг. 8 Хавдрын 4 шат

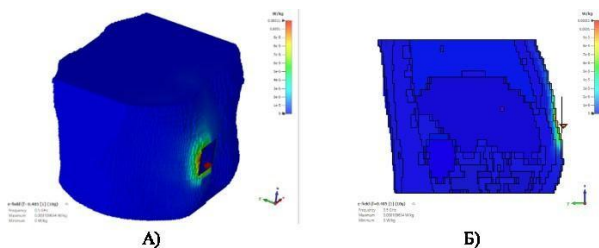
Зураг.8-т элэгний хавдрын I, II, III, IV шат дахь хэмжээний дагуу элгэнд хорт хавдрыг байршуулав. Эцсийн шатанд бусад эрхтэн лүү үсэрхийлсэн байдлаар байршуулсан. Хорт хавдрын тархалтыг дөрвөлжин хүрээгээр тэмдэглэн харуулсан бөгөөд симуляци хийх үед дөрвөлжин хүрээ доторх хэсгийг хавдар гэж үзээд ялгаатай диэлектрик нэвтрэх чадвартай материалаар

дүүргэсэн. Ийнхүү хавдрын ялгаатай үе шатуудыг загварчилснаар санал болгож буй антен хавдарт хэрхэн мэдрэг байгааг шинжлэх боломжтой болж байгаа юм.



9-р зураг. Хавдрын 4 үе шат дээрх ойлтын коэффициентийн өөрчлөлт

Үүний дараа хорт хавдрын үе шатуудад антенны ойлтын коэффициент хэрхэн өөрчлөгдөж буйг зураг.9а,б-д үзүүлэв. Зураг 9б-ээс харахад хавдрын өөр өөр үе шатуудад антенны ойлтын коэффициентийн утга - 27.4 дБ-29 дБ хооронд өөрчлөгдөж байгаа учир тус антенны тусламжтайгаар хорт хавдрын үе шатуудыг ялгах боломжтой гэж үзэж байна.



10-р зураг. Тусгай шингээлтийн харьцаа

Хүний биеийн тусгай шингээлтийн харьцааны (SAR) стандарт утга нь 1.6 Вт/кг байдаг бол санал болгож буй антенны хувьд Зураг 10-г үзүүлсэн симуляцийн үр дүнгээс харахад 0.00011 Вт/кг байгаа нь энэ антен нь хүний биед аюултай нөлөөгүй гэдгийг баталж байна.

3-Р ХҮСНЭГТ. НӨХЦӨЛ БҮР ДЭЭРХ ПАРАМЕТР ҮЗҮҮЛЭЛТҮҮД

Параметер	Чөлөөт орон зай	Хүний бие	Хавдар
S11(дБ)	-28.13	-10.09	-10.08
Өсгөлт(дБ)	1.27	1.25	1.23
VSWR	1.08	1.93	1.91

4-Р ХҮСНЭГТ. ТӨСӨӨТЭЙ ЗАГВАРУУДАЙ ХАРЬЦУУЛСАН БАЙДАЛ

Ном зүй	S11(дБ)	Хэмжээ(мм)	Ажлын давтамж (ГГц)
[5]	-27.48	20.5×14×1.6	3.35
[6]	-27	137×109×109	0.58-1.6
Энэ ажил	-27.78	46×46×0.324	0.403

ДҮГНЭЛТ

Энэхүү өгүүлэлд урвуу F хэлбэрийн антенныг 401-406МГц зурваст элэгний хорт хавдрыг эрт илрүүлэх оношилгоонд зориулж загварчиллаа. Санал болгож буй антенны ойлтын коэффициентийн симуляцийн үр дүнгээс харахад резонансны давтамжийн шилжилтээр хавдартай биеийг эрүүл биеэс ялгаж мэдрэхээс гадна хавдрын өөр өөр үе шатуудад антенны ойлтын коэффициентийн утга -

27.4 дБ-с -29дБ хооронд өөрчлөгдөж байгаа учир тус антенны тусламжтайгаар хорт хавдрын үе шатуудыг ялгах боломжтой гэж үзэж байна.

Санал болгож буй антенны гол давуу тал нь UHF био-радио давтамжийн зурваст буюу харьцангуй нам давтамжид антенны геометр хэмжээг хангалттай бууруулж 46мм×46мм×0.324мм болгож чадсан явдал юм.

НОМ ЗҮЙ

- [1] J. Bruix, L. Boix, M. Sala, and J. M. Llovet, "Focus on hepatocellular carcinoma," *Focus*, vol. 5, no. 3, pp. 201–219, Mar. 2004.
- [2] J. Baj, L. Brylinski, F. Wolinski, M. Granat, K. Kostelecka, and P. Duda, "Biomarkers and genetic markers of hepatocellular carcinoma and cholangiocarcinoma—What do we already know," *Cancers*, vol. 14, no. 6, p. 1493, 2022. [Online]. Available: <https://doi.org/10.3390/cancers14061493>
- [3] Yu, X.L., Li, A.H., Jiang, T.A., Chen, M.H., Zhao, B.Z., Zhou, X.D. and Wang, J.R., 2007. Comparison of contrast enhanced ultrasound and contrast enhanced CT or MRI in monitoring percutaneous thermal ablation procedure in patients with hepatocellular carcinoma: a multicenter study in China. *Ultrasound in medicine & biology*, 33(11), pp.1736-1749.
- [4] A. R. Chishti, M. A. Qureshi, M. N. Abbasi, S. S. Iqbal, and A. M. Algarni, "Advances in antenna-based techniques for detection and monitoring of critical chronic diseases: A comprehensive review," *IEEE Access*, published Sept. 18, 2023.
- [5] R. Islam, F. Mahbub, S. A. Al-Nahium, and M. I. Hossain Rabbi, "Design and performance analysis of monopole antenna for early-stage hepatocellular carcinoma (HCC) in human liver," in *Proc. IEEE Annu. Information Technology Conf.*, 2021.
- [6] S. A. Razaiech, A. Brankovic, A. S. Janani, B. Mohammed, A. Darvazeban, A. Zamani, G. A. Macdonald, and A. M. Abbosh, "Wearable electromagnetic belt for steatotic liver detection using multivariate energy statistics," *IEEE Access*, published Nov. 3, 2020.

- [7] M. E. Gharbi, R. Fernandez-Garcia, S. Ahyoud, and I. Gil, “A review of flexible wearable antenna sensors: Design, fabrication methods, and applications,” *Materials*, published Aug. 27, 2020..
- [8] IT’IS Foundation. Tissue Properties Database. Version 4.2 [Online]. Available: <https://itis.swiss/virtual-population/tissue-properties/database/dielectric-properties/>
- [9] N. A. Malik “ Design of implantable antennas for biomedical applications” Ph.D dissertation, Univ. of Bedfordshire pp. 10-12, 2022.
- [10] S. I. Alekseev and M. C. Ziskin, “Human skin permittivity determined by millimeter wave reflection measurements,” *Bioelectromagnetics*, vol. 28, no. 5, pp. 331–339, 2007
- [11] Antenna theory “The Dipole antenna” [Online]. Available: <https://www.antenna-theory.com/antennas/dipole.php>
- [12] A. Peyman, B. Kos, M. Djokic, B. Trotovek, C. Limbaeck-Stokin, G. Sersa, and D. Miklavcic “ Variation in dielectric properties due to pathological changes in human liver” *Bioelectromagnetics*, vol. 36, pp. 603-612, 2015

ГАР УДИРДЛАГАТ ДРОНН УНАГААХ ТӨХӨӨРӨМЖ

Түвшинтөгсийн АМАРТӨР¹, Энхболдын БАТЖАРГАЛ¹, Баярсайханы ПҮРЭВЦЭРЭН²

^{1,2}Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Холбооны инженерчлэлийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: B222300034@must.edu.mn

Хураангуй: Тус өгүүлэлд нисгэгчгүй нисэх төхөөрөмж болон түүний хууль бус хэрэглээ цэрэг дайны нөхцөлийн ашиглалтын сөрөг үр дагаваруудыг хязгаарлах чиг үүрэгтэй дагуу дроны сүлжээ унагаах төхөөрөмжийн загварчлалыг өгүүлнэ. Энэ төхөөрөмж нь өнөөгийн зах зээлд өндөр өртгөөр үйлдвэрлэгддэг бөгөөд технологийн шийдэл ашиглагдах зай болон ажиллах хугацаа нь тусгай зориулалтын хэрэглээнд нийцсэн байх ёстой. Үүний тулд хосолсон давтамжийн зурваст зэрэгцээ байрлалтай хос бичил туузан Яаги Уда антенныг өсгөлт, чиглэлийг хувьд өндөр үзүүлэлттэйгээр загварчилсанлан бөгөөд симуляцийн орчиндахь үр дүнг тусгасан, мөн бодит угсралтын демо загварыг гаргахын тулд гадар хэсгийг гурван хэмжээсээр загварчилж бусад бүрэлдэхүүн хэсгийн судалгааг хийж гүйцэтгэв.

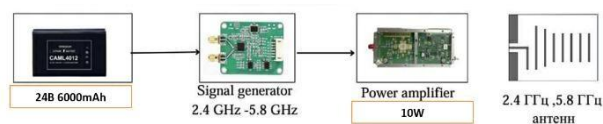
I. УДИРТГАЛ

Орчин үед алсын зайнаас удирддаг нисэх төхөөрөмж буюу дронууд ачаа бараа тээвэрлэх, зураг авах, бичлэг хийх, эрэн хайх аврах, цэрэг арми зэрэг олон салбарт хурдтай нэвтэрч байна. Гэвч хэрэглээ хурдацтай хөгжихийн хэрээр хууль бусаар бусдыг тагнах, амь насанд нь занал хийлэх зэргээр олон хор хөнөөл учруулж байна. Эдгээр эрсдэлээс сэргийлэх аргуудын нэг арга нь радио долгионоор дамжих дроны алсын удирдлагыг тасалдуулах технологи юм. Дийлэнх алсын удирдлага 2.4 ГГц, 5.8 ГГц-ийн ажлын давтамж дээр ажилдагтул давтамж тус бүр дээр ажиллах бичил туузан Яаги-Уда антенныг загварчилсан. Уг антэнн нь бичил туузан болон Яаги-Уда антеннуудын онцлог шинжийг агуулсан нийлмэл антэнн юм. Тус антэнн нь FR-4 материал дээр зэс ашиглан идэвхтэй элемент, ойлгогч, чиглүүлэгч гэсэн элементүүдээс бүрдсэн бөгөөд чиглэлийг 2.4 ГГц-ийн ажлын давтамжтай антэнн дээр 36.4° өсгөлт нь 11.3 дБ, 5.8 ГГц-ийн антэнны чиглэл 32.8° өсгөлтийг 11.6 дБ-ээр загварчилсан. Энэ нь өмнөх симуляцын үг дүнгүүдээс хамгийн боломжит шийдэл болж байна.

II. ДРОНН УНАГААГЧ ТӨХӨӨРӨМЖИЙН БҮТЭЦ, ҮЙЛ АЖИЛЛАГААНЫ ЗАРЧИМ

Алсын удирдлагыг тасалдуулах технологи нь үндсэн дөрвөн бүрдэл хэсгээс бүтнэ. Нэгдүгээрт гэжээлийн үүсгүүр буюу батарей хэсэг нь төхөөрөмжийг зай тэжээлээр хангах үндсэн үүрэгтэй. Хоёрдугаар бүрдэл хэсэгт радио долгионы өрнүүлгийн систем энэ нь гол өрнүүлэгч хэсэг юм. Гуравт антэнны хэсэг буюу долгионы давтамжийн цацаргагч хэсэг бөгөөд дөрөв дэхь нь бүрхүүл буюу гадаргуу юм. Тухайлбал, бусад гурван бүрэлдэхүүн хэсгийнхээ гадна талаар байрлах бөгөөд дотоод схемийг хамгаалах эх бие, бариул, ил хараа,

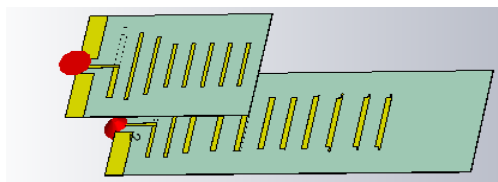
антенныг хамгаалах хэсэг, гэсэн хэд хэдэн хэсгээс бүрдэнэ.



1-р зураг. Дронны алсын удирдлагыг тасалдуулах технологийн дотоод бүтэц

III. АНТЕНН БОЛОН ЭХ БИЕЙН ЗАГВАРЧЛАЛ

Антенны хувьд FR-4 гэх диэлектрик шинж чанартай хэт халалтад тэсвэртэй цахилгаан тусгаарлагч материал дээр зэс материал ашиглаж хийсэн. Тухайн антэнн нь Яаги-Уда антэнны нэг идэвхтэй элемент, нэг ойлгогч элемент, хэд хэдэн чиглүүлэгч элементүүдийг цахилгаан тусгаарлагч материал дээр бичил туузан хэлбэрээр байрлуулж хийсэн (Зураг 3-д үзүүлэв). Эх биеийн хувьд (Зураг 2-д үзүүлсэн). Эдгээр хэсгүүд нь дотоод схемийг хамгаалах эх бие, бариул, ил хараа, антэнныг хамгаалах хэсэг гэсэн бүрдэлтэй.



2-р зураг. Бичил туузан Яаги-Уда антэнны загварчилсан байдал



3-р зураг. Дронны алсын удирдлагийг тасалдуулах технологийн эх биеийн бүтэц

А. Бичил туузан Яаги-Уда антенны тооцоолол

Антенны геометр хэмжээсийг тооцоолход ажлын давтамж гол нөлөөлөгч хүчин зүйл юм. Ажлын давтамж (f) болон гэрлийн хурдны тогтмол (c)-г ашиглаж долгионы уртыг дараах тэгшитгэл 1-ээр тооцоолно [6] [7].

$$\lambda = \frac{c}{f} \quad (1)$$

Долгионы уртаас хамаарч элементүүдийн геометр хэмжээснүүд өөр хоорондоо яалгаатай байдаг.

Идэвхтэй элемент (D)-ийг дараах томъёогоор тодорхойлно:

$$D = 0.5\lambda \quad (2)$$

Ойлгогч элемент (R)-ийг дараах томъёогоор тодорхойлно:

$$R = 0.55\lambda \quad (3)$$

Чиглүүлэгч элемент (d)-ийг дараах томъёогоор тодорхойлно:

$$d = 0.45 - 0.48\lambda \quad (4)$$

Элементүүдийн хоорондын хэмжээ (S)-ийг дараах томъёогоор тодорхойлно:

$$S = 0.15 - 0.3\lambda \quad (5)$$

Бичил туузан Яаги-Уда антенныг CST STUDIO SUITE программ ашиглан загварчилсан.

1-Р ХҮСНЭГТ. БИЧИЛ ТУУЗАН ЯГИ-УДА АНТЕННЫ ПАРАМЕТР УТГУУД

Антенн	Параметр		
	Давтамж	5.8 ГГц	2.4 ГГц
Бичил туузан Яаги Уда антенн	Өсгөлт	11.3 дБ	11.6 дБ
	Чиглэл	32.2°	36.4°
	Урт, өргөн	20см,7см	40см,7см

Б. Зай тэжээлийн тооцоо

Тэжээлийн үүсгүүр буюу батарей нь төхөөрөмжийг зай, тэжээлээр хангах үндсэн зориулалттай. Алсын удирдлагыг тасалдуулах технологийг ашигтай урт хугацаанд ажиллуулхын тулд тохирох төрлийн зайг сонгон (Зураг 4-д үзүүлэв). Түүний энергийг (E)-ийг дараах томъёогоор тодорхойлно:

$$E = V * C \quad (6)$$



4-р зураг. Литум 24 В-ийн хүчдэлтэй 6 А-ийн багтаамжтай батарей

Энэхүү (Зураг 5-д үзүүлснээр) 24 Вольтын тогтмол хүчдэлээр алдагдалгүйгээр тасралтгүй ажиллах хугацааг тооцоолсон .

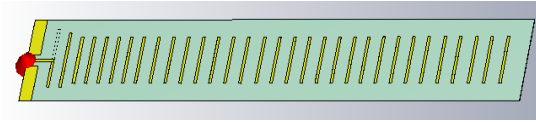


5-р зураг. Дронны алсын удирдлагийг тасалдуулах системийн тэжээлийн тооцоо

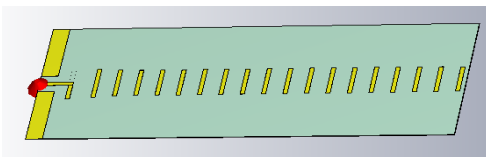
Тогтмол хүчдэл нь тогтворжсон тул үүнийг бага чадлийн тэжээлийн удирдлага ашиглан супер конденсаторт цэнэглэж бага чадлийн мэдрүүр болон микроконтроллер ажиллуулах боломжтой [5].

IV. БИЧИЛ ТУУЗАН ЯАГИ-УДА АНТЕННЫ ҮР ДҮН

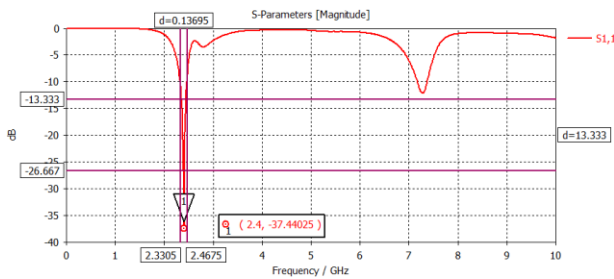
Судалгааны ажлын анхны зорилгын дагуу UHF давтамжын зурваст ажиллах цацаргагч фидер болон феррит цөмийг CST програм дээр тус тусад загварчилсан.



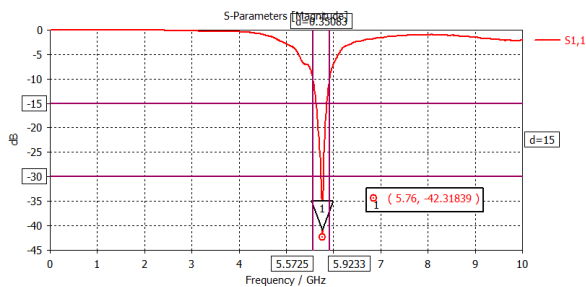
6-р зураг. Бичил туузан Яаги-Уда антенны 2.4 ГГц-ийн ажлын давтамж дээрх CST загварчлал



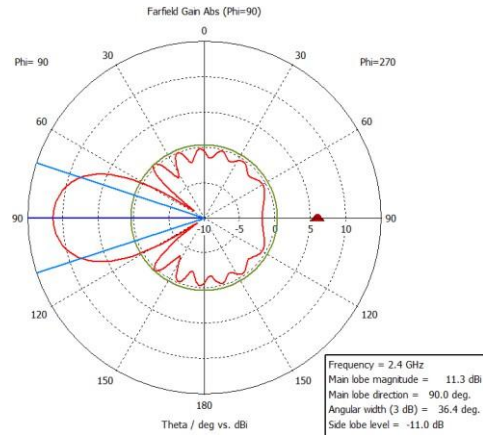
7-р зураг. Бичил туузан Яаги-Уда антенны 5.8 ГГц-ийн ажлын давтамж дээрх CST загварчлал



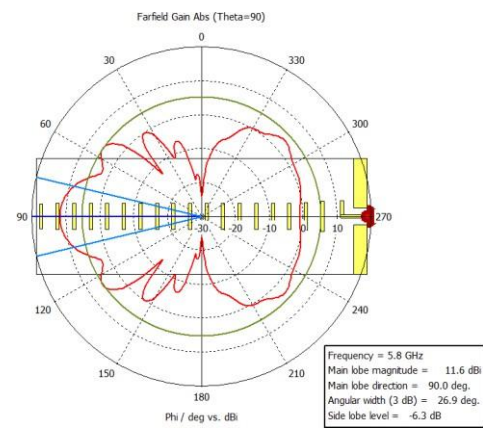
8-р зураг. 2.4 ГГц-ийн ажлын давтамж дээрх ойлтын коэффициентийн график



9-р зураг. 5.8 ГГц-ийн ажлын давтамж дээрх ойлтын коэффициентийн график

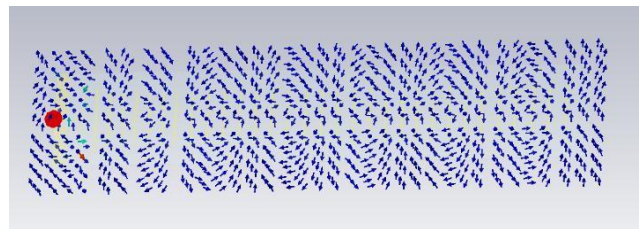


10-р зураг. 2.4 ГГц Антенны цацаргалтын диаграм

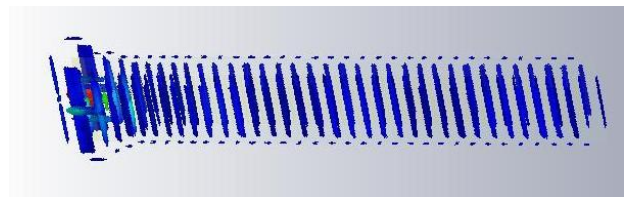


11-р зураг. 5.8 ГГц Антенны цацаргалтын диаграм

Цацаргагч фидер болон феррит цөм хэрхэн харилцан нөлөөлөлд орж байгааг Зураг 6-с харж болно. Энэ тохиолдолд шугамын тэжээлийн дохиог цацаргагч фидерт өгөөд феррит цөмд индукцлэлийн үзэгдлээр гүйдэл үүсч байгаа бөгөөд феррит цөмд үүссэн энергийг цааш шулуутган хэрэглэх боломжтой юм.



12-р зураг. Цахилгаан орны хүчлэг



14-р зураг. Гадаргуугийн гүйдэл

ДҮГНЭЛТ

Тус системийн хамгийн гол давуу тал нь ашиглахад хялбар, хөнгөн, овор багатай бөгөөд өндөр хүчин чадалтай, удаан хугацаанд тасралтгүй ажиллах боломжтой юм. Эдгээр үзүүлэлтүүд нь антенны загварчлалд чухал нөлөө үзүүлж, овор хэмжээ, антен хоорондын харилцан нөлөөлөл, давтамжийн өрнүүлэгийн эзэлхүүн зэрэг хүчин зүйлсийг оновчтой тодорхойлох шаардлагатайг харуулж байна. Мөн тэжээлийн хэсэг нь төхөөрөмжийн найдвартай ажиллагаа, үр ашигтай байдлын үндсэн хүчин зүйл бөгөөд (24 В, 6 mAh)-ийн батерей ашигласнаар ойролцоогоор 14.24 цаг тасралтгүй ажиллах боломжтой гэж тооцоолсон. Антенны үзүүлэлтүүд болох өсгөлт, чиглэл, давтамж нь нарийн чиглэлтэй бөгөөд өндөр өсгөлттэй байснаар бага чадлаар илүү хол зайд радио долгион нэвтрүүлэх, нарийн хүрээтэй бүрхэлт үүсгэх давуу талтай. Төхөөрөмжийн гадар бүтэц нь ус, чийг, доргионоос хамгаалагдсан байх шаардлагатай бөгөөд эргономик талаасаа цомхон, хөнгөн байдлаар загварчлагдсан.

АШИГЛАСАН МАТЕРИАЛ

- [1]. Antenna theory and design (2012)
- [2] Antenna handbook(vol1)
- [3]. Cst studio suite
- [4] Fusion 360 auto deck