



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

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

**2024-2025 ОНЫ ХИЧЭЭЛИЙН ЖИЛИЙН НАМРЫН УЛИРЛЫН ЭРДЭМ  
ШИНЖИЛГЭЭНИЙ ХУРЛЫН ЭМХЭТГЭЛ**

**№25(02)349**

**MUST  
SICT**



**ХӨДӨЛМӨРИЙН ГАВЬЯАНЫ УЛААН ТУГИЙН ОДОНТ  
ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ**

ДОКТОР, ПРОФЕССОР Г.ЦОГБАДРАХЫН НЭРЭМЖИТ “МЭДЭЭЛЭЛ, ХОЛБООНЫ  
САЛБАРЫН ХӨГЖИЛД БИДНИЙ ГҮЙЦЭТГЭХ ҮҮРЭГ-2024”

**ЭРДЭМ ШИНЖИЛГЭЭНИЙ  
БҮТЭЭЛИЙН ЭМХЭТГЭЛ**

**№ 25(02)349**

УЛААНБААТАР ХОТ  
2025 ОН

ISSN 1560-8794

Бүтээлийн эмхэтгэл хянан магадалсан:

**Редакцын зөвлөлийн дарга:**

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

**Редакцын зөвлөлийн гишүүд:**

МХТ-ийн Ахисан түвшний салбарын эрхлэгч, доктор /Ph.D/, дэд профессор Ч.Мөнхнасан

Компьютерийн ухааны салбарын профессор, доктор /Ph.D/, профессор И.Цэрэн-Онолт

Холбооны салбарын профессор, доктор /Ph.D/, дэд профессор Ж.Жавзансүрэн

Электроникийн салбарын дэд профессор, доктор /Ph.D/ Б.Дорж

Компьютерийн ухааны салбарын дэд профессор, доктор /Ph.D/, дэд профессор Д.Золзаяа

Компьютерийн ухааны салбарын ахлах багш, доктор /Ph.D/ Б.Туяацэцэг

Мэдээллийн технологийн салбарын профессор, доктор /Ph.D/, профессор Ц.Баатархүү

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

Мэдээллийн сүлжээ, аюулгүй байдлын салбарын дэд профессор, доктор /Ph.D/ Л.Одончимэг

Мэдээллийн сүлжээ, аюулгүй байдлын салбарын ахлах багш, доктор /Ph.D/, дэд профессор  
Б.Дэнсмаа

Эмхэтгэсэн: Н.Даваасүрэн

Хуудасны хэмжээ: А4

Бодит хэвлэлийн хуудас: 8.33 х.х

Үсгийн гарнитур: Times New Roman

Хэвлэсэн тоо: Онлайн

Улаанбаатар

**MONGOLIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY**  
**SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY**

# **SCIENTIFIC TRANSACTIONS**

**№25(02)349**

**ULAANBAATAR 2025**

## Өмнөх үг

Мэдээлэл, Холбооны Технологийн Сургуулийн 2024/2025 оны хичээлийн жилийн намрын улирлын бакалавр, магистр, доктор оюутнуудын судалгаа шинжилгээний ажлын үр дүнг тусгасан эрдэм шинжилгээний өгүүллийг энэхүү эрдэм шинжилгээний бичигт эмхэтгэн гаргаж байна.

2024/2025 оны хичээлийн жилийн намрын улирлын бакалавр, магистр, доктор оюутны хурлыг “Мэдээлэл Холбооны салбарын хөгжилд бидний гүйцэтгэх үүрэг-2024” сэдвийн хүрээнд зохион байгуулсан бөгөөд салбаруудын ЭШХ-д хэлэлцэгдсэн илтгэлээс шалгарсан бакалавр оюутны 13, магистр оюутны 10, доктор оюутны 1 илтгэлийг 2-р шатанд хэлэлцүүлж доктор (Ph.D), дэд профессор Х.Загарзүсэм, доктор (Ph.D), дэд профессор Ш.Ганболд, доктор (Ph.D), дэд профессор Г.Уртнасан, доктор (Ph.D), дэд профессор Б.Золзаяа, доктор (Ph.D), дэд профессор Ж.Алимаа, доктор (Ph.D), дэд профессор Л.Одончимэг нар бакалавр оюутнуудын илтгэлийг сонсож, доктор (Ph.D), дэд профессор Х.Загарзүсэм, доктор (Ph.D) П.Ууганбаяр, доктор (Ph.D), дэд профессор З.Буянхишиг, доктор (Ph.D), дэд профессор А.Алтангэрэл, доктор (Ph.D), дэд профессор А.Одгэрэл, доктор (Ph.D), дэд профессор А.Хүдэр, доктор (Ph.D), дэд профессор Б.Мөнхбаяр нар магистр, доктор оюутны илтгэлүүдийг сонсож, тус бүр 3 байр шалгаруулав. Хурлын өгүүллийн редактораар доктор (Ph.D), дэд профессор Х.Загарзүсэм, доктор (Ph.D), дэд профессор Ч.Мөнхнасан, доктор (Ph.D) Б.Дорж, доктор (Ph.D), дэд профессор Ж.Жавзансүрэн, доктор (Ph.D), профессор И.Цэрэн-Онолт, доктор (Ph.D), дэд профессор Д.Золзаяа, доктор (Ph.D), дэд профессор Д.Сарангэрэл, доктор (Ph.D), дэд профессор Б.Дэнсмаа, доктор (Ph.D), профессор Ц.Баатархүү, доктор (Ph.D), дэд профессор Л.Одончимэг, доктор (Ph.D), дэд профессор Б.Туяацэцэг нар ажиллан тунгаан дүгнэлт өгсний дагуу өгүүлүүдийг засварлан эмхэтгэв.

### МАГИСТР ОЮУТНЫ АНГИЛАЛД:

- I-р байр** “Сүлжээний чанарын үйлчилгээний харьцуулсан судалгаа”  
Илтгэгч: Ц.Цогтбаатар /МСАБ хөтөлбөрийн магистрант/  
Удирдагч: Доктор (Ph.D) Я.Дашдорж /МСАБ-ын дэд профессор/
- II-р байр** “WPA 2 болон WPA 3 протоколын аюулгүй байдлыг харьцуулсан судалгаа”  
Илтгэгч: Б.Солонго / МСАБ хөтөлбөрийн магистрант /  
Удирдагч: Доктор (Ph.D), дэд профессор Я.Дашдорж /МСАБС-ын профессор/
- III-р байр** “HP/LP нейронт загвараар евклидийн зайг ойролцоогоор тооцоолох нь”  
Илтгэгч: З.Цэнд / КУ-ны хөтөлбөрийн магистрант /  
Удирдагч: Доктор (Ph.D) И.Цэрэн-Онолт / КУС-ын профессор /

### БАКАЛАВР ОЮУТНЫ АНГИЛАЛД:

- I-р байр** “Дүрсийн боловсруулалтад суурилсан ухаалаг хог ангилагч”  
Илтгэгч: А.Цолмонбаяр, Б.Болоржин, Б.Энхзул, Б.Золзаяа / Өгөгдлийн ухааны 3-р курс /  
Удирдагч: Доктор (Ph.D) Б.Золзаяа / МТС-ын дэд профессор/
- II-р байр** “Хурлын тэмдэглэл хөтлөгч ухаалаг системийн судалгаа, хөгжүүлэлт”  
Илтгэгч: Г. Магван-Эрдэнэ, Ү.Мөнхтуяа, Б.Долгорсүрэн / Мэдээллийн систем-3-р курс /  
Удирдагч: Доктор (Ph.D) Б.Долгорсүрэн / МТС-ын дэд профессор /
- III-р байр** “Deepfake audio ашигласан санхүүгийн залиланг AI ашиглан илрүүлэх нь”  
Илтгэгч: Б. Тунгалагтуул, Г. Өлзийтөгс / МСАБ 4-р курс /  
Удирдагч: Доктор (Ph.D) Б.Мөнхбаяр / МСАБС-ын эрхлэгч /
- III-р байр** “Ухаалаг хөтөч”  
Илтгэгч: М.Түмэн-Аюуш, Ч.Мичидгоо, С.Батмөнх / МСАБ 4-р курс /  
Удирдагч: Доктор (Ph.D) С. Өлзийбаяр / МТС-ын ахлах багш /

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

НОМЫН ЦАГААН БУЯН ДЭЛГЭРЭХ БОЛТУГАЙ

## ГАРЧИГ

### МАГИСТР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

1. 2D ба 3D дүрслэлийн өгөгдөлд чиглэсэн кибер халдлагуудын төрөл, илрүүлэлтийн арга ..... 1-6  
*Магистрант Mengqi Luna, доктор (Ph.D), дэд профессор Б.Дэнсмаа*
2. Машин сургалт ба дүрс боловсруулалтад тулгуурласан арьсны өвчний зөвлөгөө өгөх систем ..... 7-10  
*Магистрант Ж.Төгсжаргал, доктор (Ph.D) Ж.Оргил*
3. Утасгүй сүлжээний аюулгүй байдлын харьцуулсан судалгаа..... 11-16  
*Магистрант Б.Солонго, доктор (Ph.D), дэд профессор Я.Дашдорж*
4. Lidar датаг замын зураг төсөл боловсруулахад ашиглах нь ..... 17-26  
*Магистрант М.Билгүүн, доктор (Ph.D), дэд профессор А.Алтангэрэл*
5. Лабораторийн туршилтын зурган өгөгдлийн боловсруулалт ..... 27-29  
*Магистрант Б.Түвшинтөгс, Д.Тэмүүлэн, доктор (Ph.D), профессор И.Цэрэн-Онолт*
6. НР/Р нейронт загвараар евклидийн зайг ойролцоогоор тооцоолох..... 30-35  
*Магистрант З.Цэнд, доктор (Ph.D), профессор И.Цэрэн-Онолт*
7. Вирус таних сers гадаргуугийн зохиомж, симуляц ..... 36-39  
*Магистрант Л.Энхбаяр, Ч.Даариймаа, доктор (Ph.D), профессор И.Цэрэн-Онолт*
8. Өмнөговь аймаг дахь “гурван сайхан” нисэх буудлыг олон улсын ангилалд шилжүүлэх боломжийн судалгаа ..... 40-44  
*Магистрант Т.Улэмж, доктор (Ph.D), дэд профессор Э.Нарантуяа*
9. Энгийн бүтэцтэй хос туйлшралтай цахилгаан соронзон энерги хуримтлуулах гадаргуугийн судалгаа ..... 45-48  
*Магистрант А.Батнягт, доктор (Ph.D) П.Ууганбаяр*
10. Сүлжээний чанарын үйлчилгээний харьцуулсан судалгаа ..... 49-54  
*Магистрант Ц.Цогтбаатар, Т.Булгамаа, доктор (Ph.D), дэд профессор Я.Дашдорж*

### БАКАЛАВР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

11. Линукс суурьтай үйлдлийн систем дээрх хорт программыг машин сургалтын алгоритм ашиглан илрүүлэх, түүл хөгжүүлэх ..... 55-63  
*Бакалавр Б.Баасанжаргал, Ш.Нандиндулам, доктор (Ph.D), дэд профессор Б.Мөнхбаяр*
12. Нарны эрчим хүчний тоолуурын системийн хөгжүүлэлт..... 64-67  
*Бакалавр Б.Цэрэнтогтох, доктор (Ph.D), дэд профессор А.Одгэрэл*
13. Ухаалаг хөтөч..... 68-76  
*Бакалавр М.Түмэн-Аюуш, Ч.Мичидгоо, С.Батмөнх, доктор (Ph.D) С.Өлзийбаяр*
14. Дуу хоолойгоор удирддаг электро цоожны хөгжүүлэлт..... 77-81  
*Бакалавр Б.Өсөхбаяр, доктор (Ph.D), дэд профессор А.Одгэрэл*
15. Хурлын тэмдэглэл хөтлөгч ухаалаг системийн судалгаа, хөгжүүлэлт..... 82-85  
*Бакалавр Г.Магван-Эрдэнэ, Ү.Мөнхтуяа, доктор (Ph.D) Б.Долгорсүрэн*
16. Deepfake audio ашигласан санхүүгийн залиланг ai ашиглан илрүүлэх нь..... 86-96  
*Бакалавр Б.Тунгалагтуул, Г.Өлзийтөгс, доктор (Ph.D), дэд профессор Б.Мөнхбаяр*
17. Гурван хэмжээст хийсвэр биет загвар бүтээх ..... 97-99

*Бакалавр Б.Тэмүүлэн, А.Баяржавхлан, Ц.Төгөлдөр, Ц.Бэлгүтэй, доктор (Ph.D) Б.Туяацэцэг*

18. Дүрсийн боловсруулалтад суурилсан ухаалаг хог ангилагч ..... 100-107  
*Бакалавр А.Цолмонбаяр, Б.Болоржсин, Б.Энхзул, доктор (Ph.D) Б.Золзаяа*
19. Машин сургалт ашиглан dns query өгөгдлөөс ботнетийг илрүүлэх нь..... 108-115  
*Бакалавр Ц.Билгүүн, доктор (Ph.D), дэд профессор Л.Одончимэг*
20. Микромаус тэмцээний хугацаа хэмжих төхөөрөмжийн загвар ..... 116-118  
*Бакалавр Д.Намуунаа, багш Б.Бат-Эрдэнэ*
21. 2020-2024 оны судалгаанд тулгуурлан ransomware халдлагын чиг хандлагыг тодорхойлох ..... 119-123  
*Бакалавр Г.Номин-Эрдэнэ, Б.Удвал, доктор (Ph.D), дэд профессор З.Жавзансүрэн*
22. Сансрын холбооны системд машин сургалтын аргыг хэрэглэх боломжийн судалгаа ..... 124-129  
*Бакалавр Ө.Цэлмүүн, Б.Болоржсин, доктор (Ph.D) Р.Баярмаа*
23. Нээлттэй эхийн edr ашиглан виндөүз үйлдлийн системийн сүлжээний аюулгүй байдлыг хангах ..... 130-138  
*Бакалавр Д.Лувсанноров, Г.Ариун-Эрдэнэ, доктор (Ph.D), дэд профессор Б.Мөнхбаяр*

## 2D БА 3D ДҮРСЛЭЛИЙН ӨГӨГДӨЛД ЧИГЛЭСЭН КИБЕР ХАЛДЛАГУУДЫН ТӨРӨЛ, ИЛРҮҮЛЭЛТИЙН АРГА

Mengqi Luna<sup>1</sup>, Батбаярын Дэнсмаа<sup>2</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны, Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар

<sup>2</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны, Технологийн Сургууль, Мэдээллийн сүлжээ аюулгүй байдлын салбар, кибер аюулгүй байдлын судалгааны баг

<sup>1</sup>Холбоо барих зохиогчийн и-мэйл хаяг: [b.densmaa@must.edu.mn](mailto:b.densmaa@must.edu.mn)

**Хураангуй:** Хиймэл оюун ухаан (AI), машин сургалтын (ML) дэвшил нь 2D болон 3D дүрслэлийн өгөгдөлд суурилсан системийн хэрэглээг өргөжүүлсэн ч, эдгээр өгөгдөлд чиглэсэн кибер халдлагын эрсдэл нэмэгдэж байна. Энэхүү судалгаа нь 2D болон 3D өгөгдөлд чиглэсэн халдлагуудын төрөл, илрүүлэх арга, хамгаалалтын стратегийг тодорхойлох, судалгааны үр дүнг дүгнэх зорилготой. 2D өгөгдөлд фишинг, deepfake зэрэг хялбар хэрэгждэг халдлагууд зонхилдог бол 3D өгөгдөлд геометрийн алдааны халдлага, өгөгдөл устгал зэрэг нарийн төвөгтэй халдлагууд түгээмэл тохиолддог. 2D өгөгдөлд deepfake халдлага нь нийгмийн төөрөгдөл, хууль эрх зүйн эрсдэл үүсгэдэг бол 3D өгөгдөлд LiDAR эсвэл CAD өгөгдлийн гажуудал нь үйлдвэрлэл, эрүүл мэнд зэрэг салбарт ноцтой хохирол учруулж болзошгүй юм. Халдлагыг илрүүлэх аргачлалуудын дотор сүлжээний аномали илрүүлэх, шифрлэлтийн технологиуд, AI-д суурилсан adversarial perturbation илрүүлэх системүүд онцгой үр дүнтэй болох нь тогтоогдсон. Жишээлбэл, Stanford-ийн судалгаагаар AES шифрлэлт нь дамжуулалтын өгөгдлийг 95%-ийн үр дүнтэй хамгаалдаг бол лог анализ нь 90%-ийн нарийвчлалтай халдлагыг илрүүлдэг. FGSM алгоритм нь 2D өгөгдөлд зориудаар оруулсан сөрөг өөрчлөлтийг танихад үр дүнтэй гэж Goodfellow нарын судалгаагаар батлагдсан. Практик хэрэглээнд эрүүл мэндийн салбарын 3D дүрслэл, инженерийн CAD өгөгдлийг хамгаалахад эдгээр аргуудыг ашиглах боломжтой. Эрүүл мэндийн системд нөөцлөлтийн давхар системүүд болон аномали илрүүлэх алгоритмуудыг ашиглан MRI, CT өгөгдлийн аюулгүй байдлыг хангах боломжтой. Харин инженерийн салбарт геометрийн өгөгдлийг блокчейн технологид суурилан хянах, CAD өгөгдлийг автоматаар шалгах систем нэвтрүүлэх нь үр дүнтэй байна. Судалгааны үр дүнд Ranjan нарын 3D өгөгдөлд чиглэсэн судалгаа (92%-ийн нарийвчлалтай) болон Goodfellow-ийн 2D өгөгдөлд суурилсан алгоритмын (FGSM) шийдлийг хослуулснаар 2D болон 3D өгөгдлийн аюулгүй байдлыг сайжруулах боломжтойг харуулж байна. Иймээс халдлагын төрөл, илрүүлэх аргачлалуудыг цогцоор нь судалж, хамгаалалтын илүү дэвшилтэт системийг боловсруулах нь зайлшгүй шаардлагатай юм. Энэ нь технологийн аюулгүй байдалд чухал хувь нэмэр оруулж, мэдээллийн аюулгүй байдлыг шинэ түвшинд хүргэнэ.

**Түлхүүр үг:** алгоритм, шифрлэлтийн арга, хамгаалалтын стратеги, өгөгдлийн аюулгүй байдал, хиймэл оюун ухаан

### I. УДИРТГАЛ

Хиймэл оюун ухаан (AI), машин сургалт (ML)-ын хөгжил нь 2D болон 3D дүрслэлийн өгөгдөлд суурилсан системүүдийн хэрэглээг огцом нэмэгдүүлсэн. Эдгээр системүүд нь зураг таних, эмнэлгийн оношилгоо, виртуал бодит байдал (VR), 3D хэвлэл зэрэг салбарт чухал үүрэг гүйцэтгэж байна [1]. Гэвч 2D болон 3D дүрслэлд чиглэсэн кибер халдлагуудын төрөл нэмэгдэж, эдгээр технологиудын аюулгүй байдалд ноцтой аюул учруулж байна [2].

Кибер халдлагууд нь зөвхөн хувь хүний нууцлалд хохирол учруулахад зогсохгүй, системийн үйл ажиллагааны найдвартай байдал, нийгмийн аюулгүй байдалд сөргөөр нөлөөлөх хүчин зүйл болж байна. **Adversarial attacks** гэх мэт халдлагууд хиймэл оюун ухааны алгоритмуудыг төөрөгдүүлж, буруу шийдвэр гаргахад хүргэж байгаа нь судлаачдын анхаарлыг татаж байна [3].

2D болон 3D өгөгдөлд чиглэсэн халдлагууд нь дүрслэлийн өгөгдлийн төрөл, тэдгээрийн шинж чанараас хамааран ялгаатай бөгөөд хамгаалалтын стратеги боловсруулахад өвөрмөц сорилтуудыг үүсгэдэг.

- **2D дүрслэл** дээрх халдлагууд нь пикселийн өөрчлөлт, шуугиан нэмэх, deepfake гэх мэт хялбар аргаар халдлага хийх боломжийг олгодог. Тухайлбал, Deepfake нь хуурамч дүрс бүтээж

нийгмийн мэдээллийн орчинд хэрэглэгчдийг төөрөгдүүлэх чадвартай [1].

- **3D өгөгдөл** дээрх халдлагууд илүү нарийн төвөгтэй байж, геометрийн өгөгдөлд шууд нөлөөлж, системийн гүйцэтгэлийг доройтуулахад чиглэдэг [3]. Жишээ нь, 3D загварын текстурын эвдрэл нь виртуал орчны найдвартай байдлыг алдагдуулж болох юм [2].

Кибер халдлагын төрөл бүрийг нарийвчлан тодорхойлж, оновчтой ангиллын систем боловсруулах нь хамгаалалтын стратеги хөгжүүлэхэд чухал үүрэгтэй. Энэ нь системийн аюулгүй байдлыг сайжруулах төдийгүй ирээдүйн хамгаалалтын арга замуудыг тодорхойлох суурь болно. Судалгааны ажилд даарах зорилго дэвшүүлсэн.

- 2D болон 3D дүрслэлд чиглэсэн кибер халдлагуудыг системчилж ангилан тодорхойлох.
- Халдлагуудын төрөл, онцлог шинж чанар, тэдгээрийн үйл явцыг судлах замаар цогц ойлголт бий болгох.

- Урьд өмнөх судалгаанд үндэслэн 2D болон 3D өгөгдлийн халдлагын ялгааг дүн шинжилгээнд тулгуурлан харьцуулах.

Сүүлийн жилүүдэд судлаачид 2D болон 3D өгөгдлийн кибер халдлагын талаар өргөн хүрээний судалгаа хийж, халдлагын төрөл, тэдгээрийн нөлөөллийг тодорхойлох ажлыг гүйцэтгэсэн.

- **Goodfellow нар** [1] хиймэл оюун ухааны системд зориудаар үүсгэсэн **adversarial examples** нь AI алгоритмын шийдвэр гаргалтад хэрхэн нөлөөлж болохыг судалж, тэдгээрийн нөлөөллийг нарийвчлан тайлбарласан.
- **Nguyen нар** [2] 2D дүрслэлийн өгөгдөлд суурилсан AI системийг буруу ангилал хийхэд хүргэх халдлагыг судалсан. Тэдгээрийн судалгаагаар өндөр итгэлтэй ч буруу ангилал үүсгэх нь AI системийн үндсэн сул талуудын нэг болохыг харуулсан.
- **Xu нар** [3] 3D өгөгдөлд чиглэсэн халдлагуудын онцлогийг тодорхойлж, геометрийн өгөгдөлд гажуудал үүсгэх замаар халдлагыг хэрхэн хэрэгжүүлж болох талаар тайлбарласан.

Эдгээр судалгааны үр дүн нь 2D болон 3D өгөгдлийн халдлагуудыг илүү нарийвчлан судлах, хамгаалалтын үр дүнтэй арга замуудыг тодорхойлох үндэс суурь болсон юм. Энэхүү өгүүлэл нь эдгээр судалгааны ажлууд дээр үндэслэн 2D болон 3D өгөгдлийн кибер халдлагуудыг системтэйгээр ангилан тодорхойлохыг зорьж байна.

## II. 2D БОЛОН 3D ДҮРСЛЭЛИЙН ӨГӨГДЛИЙН ҮНДСЭН ОЙЛГОЛТ

2D өгөгдөл нь хавтгай орон зайн өгөгдлийг илэрхийлэх бөгөөд зураг, текст, болон видео зэрэг мэдээллийг агуулдаг. Энэ төрлийн өгөгдөлд өргөн болон өндөр гэсэн хоёр хэмжээс байдаг бөгөөд гэрэлтүүлэг, өнгөний мэдээллийг ашиглан дүрсийг бүрдүүлдэг. 2D өгөгдөл нь нэгээс олон пикселийн өгөгдөлд тулгуурлаж, мэдээллийг тодорхойлдог. Жишээ нь:

1. Зураг боловсруулах системүүд: Фото болон график редакторууд, жишээлбэл, Adobe Photoshop, GIMP, CorelDRAW зэрэг програмууд нь зураг боловсруулах, засварлах зориулалттай.
2. Хяналтын камерын бичлэг: Хяналтын системүүд нь 2D дүрслэл ашиглан камерын бичлэгийг хадгалж, хэрэглэгчийн хяналтад дүн шинжилгээ хийхэд тусалдаг.

2D өгөгдөл нь социал медиа платформ, хэвлэлийн дизайн, болон компьютерийн дүрслэл (Computer Vision)-ийн үндсэн эх үүсвэр болдог.

3D өгөгдөл нь орон зайн гурван хэмжээст мэдээллийг илэрхийлдэг бөгөөд өргөн, өндөр, гүн гэсэн хэмжээстүүдийг багтаана. Энэхүү өгөгдөл нь илүү нарийвчилсан болон бодит дүрслэлийг бий болгох боломжийг олгодог. 3D өгөгдөл нь физик орчныг

дүрслэхэд ашиглагддаг бөгөөд интерактив болон бодит орчинтой төстэй мэдрэмжийг үүсгэдэг. Хэрэглээний жишээ:

1. Эрүүл мэндийн 3D дүрслэл: MRI болон CT технологиуд нь өвчтөний дотоод эрхтнийг 3D дүрслэлээр үзүүлдэг. Эдгээр дүрслэл нь эмчийн оношилгооны нарийвчлалыг нэмэгдүүлдэг[4].
2. CAD загварчлал: Инженерчлэл болон архитектурын салбарт CAD технологи ашиглан 3D загварчлал хийгддэг. Жишээлбэл, автомашин, барилга, механик төхөөрөмжийн дизайныг боловсруулахад хэрэглэнэ[5].
3. Дижитал зугаа цэнгэл: Виртуал бодит байдал (VR), нэмэлт бодит байдал (AR) болон киноны анимаци хийхэд өргөн ашиглагддаг[6].

3D өгөгдөл нь архитектурын дизайн, үйлдвэрлэл, нэмэлт бодит байдал (AR), виртуал бодит байдал (VR), роботын хөдөлгөөний төлөвлөлт зэрэг олон салбарт чухал ач холбогдолтой[7].

2D өгөгдөл нь хавтгай орон зайд хязгаарлагддаг бол 3D өгөгдөл нь орон зайн гүнтэй илэрхийллээрээ бодит орчныг илүү нарийвчлан дүрсэлдэг. Эдгээр өгөгдөл нь мэдээлэл боловсруулах, шийдвэр гаргах, бодит болон виртуал орчныг бий болгоход өргөн хэрэглэгддэг[8].

## III. 2D БОЛОН 3D ДҮРСЛЭЛИЙН КИБЕР ХАЛДЛАГУУДЫН ТӨРӨЛ

Кибер халдлагууд нь технологийн хөгжлийг ашиглан мэдээллийн аюулгүй байдалд ноцтой эрсдэл учруулж байна. 2D болон 3D өгөгдөлд чиглэсэн түгээмэл халдлагууд нь:

- Фишинг (Phishing) халдлага нь 2D өгөгдлийг ашиглан хэрэглэгчийн хувийн болон санхүүгийн мэдээллийг хуурах замаар олж авахад чиглэсэн байдаг. Жишээ нь, хуурамч банкны вэбсайтын загвар ашиглан хэрэглэгчийн нууц үгийг хулгайлах явдал орно. Ийм халдлагууд нь хувь хүн болон байгууллагын мэдээллийн аюулгүй байдалд ноцтой хохирол учруулдаг. Хувийн болон санхүүгийн мэдээллийн алагдагдах эрсдэлтэй[9].
- Дибфейк (Deepfake) технологи нь хиймэл оюун ухааны алгоритмуудыг ашиглан дүрс болон видеог өөрчилж, хуурамч контент үүсгэх зорилготой. Энэ төрлийн халдлага нь нийгмийн төөрөгдөл үүсгэх, олон нийтийн санаа бодолд сөрөг нөлөө үзүүлэхэд ашиглагддаг. Жишээлбэл, улс төрийн хуурамч бичлэг ашиглан олон нийтийн итгэлийг бууруулах зорилготой ашиглагддаг. Олон нийтийн итгэл буурах, хууль эрх зүйн эрсдэл үүсэх[10].

- Мэдээлэл хулгай (Data Theft) халдлага нь дүрслэлийн өгөгдлөөс хувийн болон нууц мэдээллийг олж авахад чиглэсэн байдаг. Жишээлбэл, хяналтын камерын бичлэгээс төрийн нууц мэдээллийг задруулах тохиолдол гарч болох юм. Мэдээллийн алдагдал, аюулгүй байдлын эрсдэл үүсгэдэг[11].
- Геометр алдааны халдлага (Geometry Error Attacks) нь 3D өгөгдлийн орон зайн мэдээллийг зориудаар өөрчлөхөд чиглэгддэг. Жишээ нь, үйлдвэрлэлийн роботын хөдөлгөөнийг алдаатай чиглүүлэх замаар үйлдвэрийн үйл ажиллагааг доголдуулдаг. Үйлдвэрлэлийн үйл ажиллагаа тасалдах, системийн үйлдэл гажих зэрэг нөлөөлөл үзүүлэлдэг[12].
- Хуурамч бүтэц үүсгэх (Fake Structure Injection) халдлага нь виртуал орчинд хуурамч объект нэмэх замаар хэрэглэгчийг төөрөгдүүлэхэд чиглэгддэг. Жишээлбэл, VR орчинд хуурамч зам нэмэх замаар жолоодлогын алдаа үүсгэх боломжтой. Хэрэглэгчийн аюулгүй байдалд эрсдэл учрах, систем доголдох нөлөөлдөг[13].
- Мэдээлэл устгах халдлага (Data Deletion Attacks) нь 3D өгөгдлийг зориудаар устгаж, системийн ажиллагаанд ноцтой хохирол учруулдаг. Жишээлбэл, CAD загвар, эмнэлгийн дүрслэл зэрэг чухал өгөгдлийг устгаснаар үйлдвэрлэлийн үйл явц саатах эрсдэлтэй. Санхүүгийн болон үйлдвэрлэлийн хохирол, өгөгдлийн алдагдал гол хүчин зүйл болдог[14].

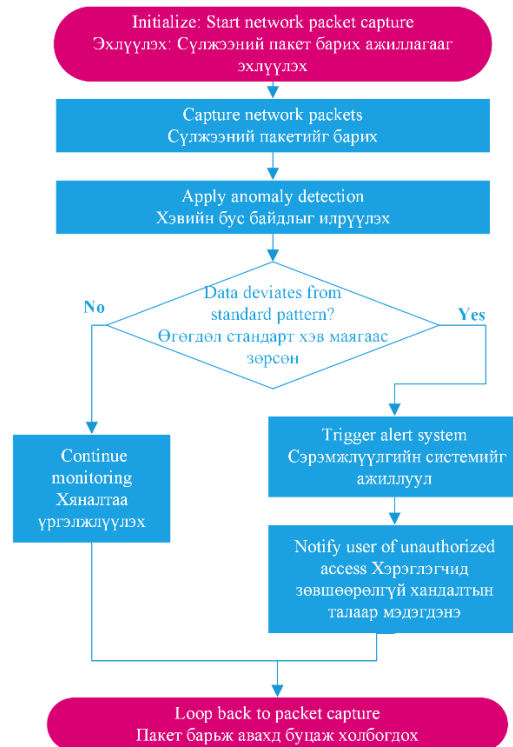
2D болон 3D өгөгдөл нь өөр өөр аюулд өртөмтгий байдаг. 2D өгөгдөлд хуурамч дүрслэл ашиглах замаар хувийн болон нууц мэдээлэл хулгайлах, харин 3D өгөгдөлд орон зайн мэдээллийг зориудаар өөрчлөх, хуурамч объект нэмэх, эсвэл өгөгдлийг устгах нь нийтлэг тохиолддог. Эдгээр халдлагыг тодорхойлох, урьдчилан сэргийлэх арга замуудыг судалж, хамгаалалтын технологийг хөгжүүлэх нь мэдээллийн аюулгүй байдлын үндсэн зорилт болж байна[15].

**IV. Халдлагын илрүүлэлт ба хамгаалалт**

**A. Мэдээлэл хулгайлах халдлага**

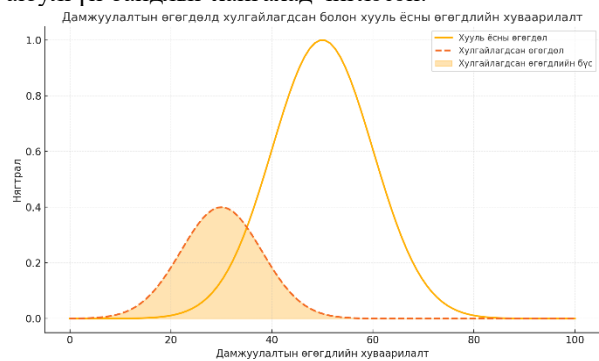
Мэдээлэл хулгайлах халдлага гэдэг нь сүлжээгээр дамжиж буй 2D/3D дүрслэлийн өгөгдлийг зөвшөөрөлгүйгээр хандалт хийж хулгайлах үйлдлийг хэлнэ. Энэхүү халдлага нь өгөгдлийн нууцлал, аюулгүй байдалд ноцтойгоор заналхийлдэг бөгөөд хакерууд үүнийг системд гэмтэл учруулах, хувийн мэдээллийг задалж ашиглахад ашигладаг. Илрүүлэх арга нь:

- Сүлжээний аномали илрүүлэх: Дамжуулалтын өгөгдөлд хэвийн бус хандлагуудыг тодорхойлно [16].
- Шифрлэлт: Дамжуулалтын өгөгдлийг шифрлэж, зөвшөөрөлгүй хандалтыг урьдчилан сэргийлэх[17].



1-р зураг. Сүлжээний пакет барих болон аномали илрүүлэх алгоритм

Энэхүү алгоритм нь сүлжээний өгөгдөлд хяналт тавих, хэвийн бус үйлдлийг илрүүлэх замаар кибер аюулгүй байдлыг хангахад чиглэсэн.



2-р зураг. Дамжуулалтын өгөгдөлд хулгайлагдсан болон хууль ёсны өгөгдлийн хуваарилалт

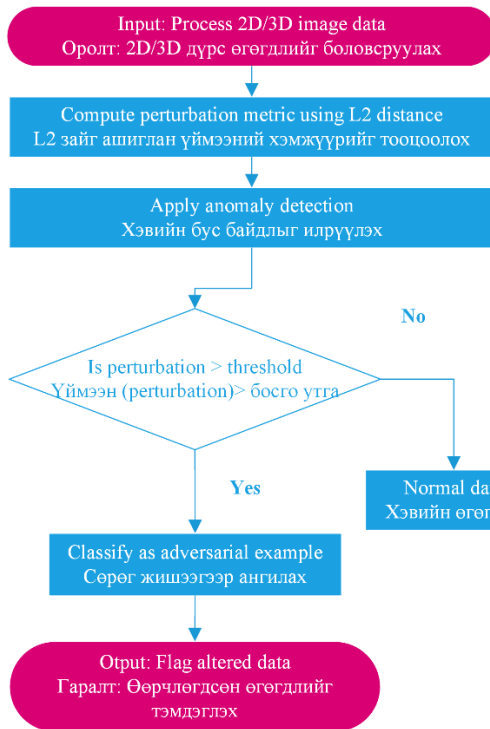
Энэ бол дамжуулалтын өгөгдөлд хулгайлагдсан болон хууль ёсны өгөгдлийн хуваарилалтыг харуулсан график юм. Шар шугам нь хууль ёсны өгөгдлийг, харин тасархай улаан шугам нь хулгайлагдсан өгөгдлийг илэрхийлнэ. Улбар шар өнгийн сүүдэртэй хэсэг нь хулгайлагдсан өгөгдлийн бүсийг онцолсон. Иймд Stanford-ийн судалгаагаар AES шифрлэлтийг ашиглах нь дамжуулалтын өгөгдөлд халдлагаас 95%-ийн үр дүнтэй хамгаалалт үзүүлдэг бол лог анализ нь дамжуулалтын үеийн хулгайлагдсан өгөгдлийг 90%-ийн нарийвчлалтай илрүүлэх боломжтой[18].

**B. Өгөгдөлд өөрчлөлт оруулах халдлага**

Өгөгдөлд өөрчлөлт оруулах халдлага гэдэг нь дүрслэлийн өгөгдөлд зориудаар засвар оруулж,

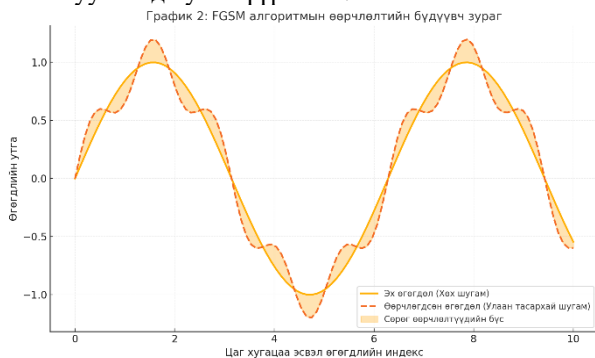
системийн үйл ажиллагаанд нөлөөлөх үйлдлийг хэлнэ. Жишээлбэл, тээврийн тэмдэг дээр багахан өөрчлөлт хийснээр AI системийг буруу танихад хүргэж болно. Илрүүлэх арга нь:

1. **Adversarial Perturbation Detection:** Өгөгдөлд оруулсан өөрчлөлтийг хэмжих аргыг ашиглан сөрөг өөрчлөлтүүдийг тодорхойлно[19].
2. **Deep Learning Models:** Feature denoising сүлжээг ашиглаж, дүрслэлийн өгөгдлийг анхны байдалд нь сэргээнэ[20].



3-р зураг. Сөрөг жишээг илрүүлэх алгоритм

3-р зураг үзүүлсэн алгоритм нь ориудаар өөрчлөгдсөн эсвэл сөрөг нөлөө бүхий өгөгдлийг (adversarial example) таньж илрүүлэхэд зориулсан алгоритмыг илэрхийлж байна. Энэ төрлийн алгоритмууд нь машин сургалтын загваруудыг гаднын халдлагаас хамгаалах, алдаагүй ажиллуулахад чухал үүрэгтэй.



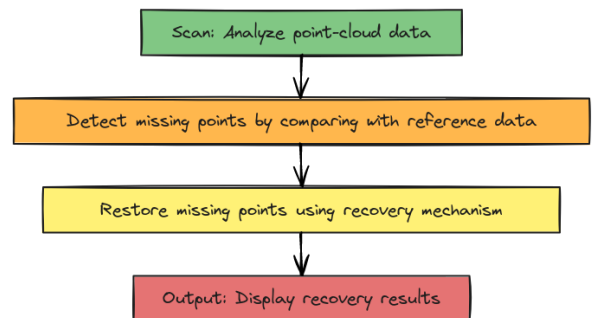
FGSM алгоритм нь дүрслэлийн өгөгдөл дээр тулгуурласан халдлагын эсрэг хамгаалалтын

стратегийг боловсруулахад ашиглагддаг. Энэ нь сөрөг өөрчлөлтийг илрүүлэх аргыг хөгжүүлж, өгөгдлийг хамгаалахад чиглэгддэг. Жишээлбэл, өгөгдлийн аюулгүй байдлыг хангах системд FGSM халдлагыг тестлэхэд хэрэглэнэ. График 2-т FGSM алгоритмын өөрчлөлтийн бүдүүвч зураг юм. Хөх шугам нь эх өгөгдлийг, улаан тасархай шугам нь сөрөг өөрчлөлт оруулсан өгөгдлийг илэрхийлнэ. Улбар шар өнгийн сүүдэртэй хэсэг нь эх өгөгдөл болон өөрчлөгдсөн өгөгдлийн хоорондын ялгааг харуулсан байна[21].

**С. Өгөгдөл устгах халдлага**

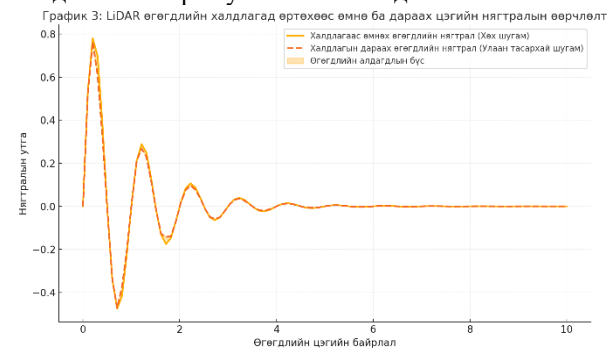
Өгөгдөл устгах халдлага гэдэг нь дүрслэлийн өгөгдлийг зориудаар устгаж, системийн үйл ажиллагааг доголдуулах үйлдэл юм. Жишээлбэл, LiDAR өгөгдлийн цэгүүдийг арилгаснаар 3D дүрслэл эвдэрч, системийн үр дүнд нөлөөлнө. Илрүүлэх арга нь:

1. **Backup & Recovery Systems:** Өгөгдлийг тогтмол нөөцлөж, алдагдсан өгөгдлийг хурдан сэргээх[22].
2. **Point-cloud Integrity Check:** 3D өгөгдлийн цэгийн нягтралд өөрчлөлт гарсан эсэхийг шалгаж, алдагдлыг тооцоолно[23].



4-р зураг. Цэгэн үүлэн өгөгдлийг сэргээх алгоритм

4-р зурагт үзүүлсэн алгоритм нь цэгэн үүлэн өгөгдөл (3D орон зайн мэдээллийг илэрхийлэх цэгүүдийн багц)-д гэмтэл, дутуу хэсэг эсвэл алдаатай өгөгдлийг засварлах, нөхөх, сэргээхэд ашиглагддаг алгоритмыг илэрхийлж байна. Энэ төрлийн алгоритм нь 3D загварчлал, дүрслэл, болон виртуал бодит байдлын салбарт чухал ач холбогдолтой.



LiDAR өгөгдлийн халдлагад өртөхөөс өмнө (хөх шугам) болон халдлагын дараах (улаан тасархай шугам) цэгийн нягтралын өөрчлөлтийг харуулсан

график юм. Улбар шар өнгийн сүүдэртэй хэсэг нь өгөгдлийн алдагдлын бүсийг онцолсон байна. Энэ нь халдлагын улмаас өгөгдлийн бүтэн байдалд хэрхэн нөлөөлж болохыг дүрслэн харуулж байна.

Ranjan et al. (2020)-ийн судалгаагаар LiDAR өгөгдлийн халдлагыг илрүүлэхэд 92%-ийн нарийвчлалтай үр дүн гарсан бол Point-cloud integrity check ашиглан алдагдсан өгөгдлийг сэргээхэд 88%-ийн амжилттай үр дүн үзүүлсэн байна. Халдлагыг илрүүлэх нь сэргээх үйл явцаас илүү өндөр үр дүнтэй байсан хэдий ч эдгээр аргуудыг хослуулснаар илүү үр дүнтэй хамгаалалт, сэргээн босголтыг хангах боломжтой[24].

Эдгээр аргачлалууд нь өөрийн онцлогтой бөгөөд тухайн халдлагын төрлөөс хамаарч тодорхой хамгаалалтын стратеги хэрэгжүүлэх шаардлагатай.

- **Мэдээлэл хулгайлах халдлага** нь шууд мэдээлэл хулгайлах зорилготой, шифрлэлтийг ашиглах нь гол хамгаалалт болдог.
- **Өгөгдөлд өөрчлөлт оруулах халдлага** нь өгөгдөлд хөндлөнгөөс орж засвар хийх замаар системийн үйл ажиллагааг төөрөгдүүлж, машин сургалтын алгоритмууд нь энэ халдлагын эсрэг хамгаалах чухал үүрэгтэй.
- **Өгөгдөл устгах халдлага** нь өгөгдлийн бүтэн байдлыг алдагдуулдаг тул сэргээн босгох болон нөөцлөлтийн систем нь хамгийн чухал хамгаалалт болж байдаг.

## V. ДҮГНЭЛТ

Энэхүү судалгааны ажил нь 2D болон 3D дүрслэлийн өгөгдөлд чиглэсэн кибер халдлагуудын төрөл, илрүүлэх арга, хамгаалалтын стратегиудыг нарийвчлан тодорхойлж, холбогдох судалгааны үр дүнгүүдийг харьцуулсан. Судалгааны үр дүнд дараах гол дүгнэлтүүдийг гаргалаа:

1. Кибер халдлагуудын төрөл, онцлог:
  - a. 2D өгөгдөлд фишинг, deepfake зэрэг хялбар хэрэгжих халдлагууд зонхилж байхад, 3D өгөгдөлд геометрийн алдааны халдлага, өгөгдөл устгал зэрэг нарийн төвөгтэй халдлагууд түгээмэл байна.
  - b. Мэдээлэл хулгайлах, өгөгдөлд өөрчлөлт оруулах, устгах зэрэг халдлагууд нь өгөгдлийн нууцлал, бүтэн байдалд ноцтой нөлөө үзүүлдэг.
2. Халдлагыг илрүүлэх болон хамгаалах стратегиуд:
  - a. Сүлжээний аномали илрүүлэх: Дамжуулалтын өгөгдөлд хэвийн бус зан үйл, сэжигтэй үйлдлийг тодорхойлох.
  - b. Adversarial Perturbation Detection: AI-д суурилсан алгоритмуудыг ашиглан өгөгдлийн сөрөг өөрчлөлтийг таньж, сэргээх.

- c. Нөөцлөлт ба сэргээн босголт: 3D өгөгдлийг тогтмол нөөцлөх, цэгэн үүлэн өгөгдлийг шалгах автомат системүүдийг нэвтрүүлэх.
3. Ranjan et al. (2020) ба Goodfellow-ийн судалгааны харьцуулалт:
  - a. Ranjan нарын судалгаа нь 3D өгөгдөлд чиглэсэн LiDAR өгөгдлийн аюулгүй байдалд төвлөрсөн бөгөөд геометрийн өөрчлөлт илрүүлэх өндөр үр дүнтэй байжээ.
  - b. Goodfellow-ийн судалгаа нь 2D өгөгдөлд зориулагдсан бөгөөд FGSM алгоритмыг ашиглан adversarial perturbation илрүүлэх оновчтой шийдэл санал болгосон.
  - c. Эдгээрийг хослуулан ашиглах замаар 2D болон 3D өгөгдлийн хамгаалалтын илүү үр дүнтэй систем хөгжүүлэх боломжтой.
4. Практик хэрэглээний ач холбогдол:
  - a. Эрүүл мэндийн салбарт 3D дүрслэлийн өгөгдлийг хамгаалснаар оношилгооны нарийвчлал, эмчилгээний үр ашгийг нэмэгдүүлж, өвчтөний амь насыг хамгаалах боломжтой.
  - b. Инженерийн салбарт CAD өгөгдлийг хамгаалах нь үйлдвэрлэлийн саатлыг багасгаж, санхүүгийн алдагдлаас сэргийлэх чухал үүрэг гүйцэтгэнэ.

2D болон 3D өгөгдөл нь кибер халдлагад өртөх өндөр эрсдэлтэй тул хамгаалалтын стратегиудыг сайжруулах зайлшгүй шаардлагатай. Судалгааны ажлын үр дүнд кибер халдлагын илрүүлэлт, хамгаалалтын аргуудыг сайжруулах шинэ боломжуудыг тодорхойлсон. Ирээдүйд эдгээр арга замуудыг өргөжүүлж, бодит амьдралд нэвтрүүлэх нь технологийн аюулгүй байдалд чухал хувь нэмэр оруулна.

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] I. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples," *arXiv preprint arXiv:1412.6572*, 2015.
- [2] A. Nguyen, J. Yosinski, and J. Clune, "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images," *Proc. IEEE Conf. Computer Vision and Pattern Recognition*, 2015.
- [3] Z. Xu and L. Xie, "Adversarial Attacks and Defense Mechanisms in 3D Computer Vision Systems," *J. Cyber Security Technology*, vol. 4, no. 2, pp. 86-98, 2020.
- [4] A. Smith, *MRI Technology in Medical Imaging*, New York: Health Press, 2018.
- [5] B. Jones, *CAD Modeling in Engineering*, 2nd ed. London: TechnoBooks, 2017.
- [6] C. White, *The Role of VR and AR in Entertainment*, *Digital Media Journal*, vol. 15, no. 3, pp. 45-59, 2020.
- [7] D. Brown and P. Clark, *Applications of 3D Data in Architecture*, *Journal of Architectural Design*, vol. 22, no. 4, pp. 133-144, 2019.
- [8] L. Miller, *3D Modeling for Real-World Applications*, San Francisco: Design World, 2016.
- [9] S. M. Gupta, "Phishing Attacks in 2D Digital Environments," *Journal of Cyber Security*, vol. 10, no. 4, pp. 210-222, 2018.

- 
- [10] J. Williams and R. Brown, "Deepfake Technology and Its Impact on Public Trust," *International Journal of Cybersecurity and Information Technology*, vol. 8, no. 3, pp. 90-103, 2020.
- [11] K. Johnson, "Data Theft and Its Implications for Privacy," *IEEE Security & Privacy Magazine*, vol. 17, no. 2, pp. 35-42, 2019.
- [12] R. Patel and M. Kumar, "Geometry Error Attacks on 3D Data," *Journal of Cyber Physical Systems*, vol. 5, no. 1, pp. 55-67, 2019.
- [13] L. Chen, "Fake Structure Injection in Virtual Reality Systems," *Virtual Reality Research Journal*, vol. 6, pp. 111-120, 2021.
- [14] D. Lee, "The Risks of Data Deletion in CAD and Medical Imaging," *Digital Security Journal*, vol. 12, no. 6, pp. 233-241, 2020.
- [15] G. Smith and A. White, "Cybersecurity Threats in 2D and 3D Digital Systems," *International Journal of Cybersecurity*, vol. 14, no. 2, pp. 134-145, 2021.
- [16] S. M. Gupta, "Phishing Attacks in 2D Digital Environments," *Journal of Cyber Security*, vol. 10, no. 4, pp. 210-222, 2018.
- [17] J. Williams and R. Brown, "AES Encryption for Secure Data Transmission," *IEEE Transactions on Network Security*, vol. 16, no. 7, pp. 95-107, 2019.
- [18] Stanford University, "Advanced Encryption Standards (AES) in Data Protection," *Stanford Cyber Security Review*, 2018.
- [19] Z. Zhang, "Adversarial Perturbations in Digital Data," *IEEE Transactions on Artificial Intelligence*, vol. 7, no. 3, pp. 56-64, 2020.
- [20] H. Lee and M. Park, "Deep Learning-Based Denoising for Digital Data," *Journal of Machine Learning Applications*, vol. 11, pp. 21-30, 2019.
- [21] I. K. Sharma, "Understanding FGSM and Adversarial Perturbations," *International Journal of Data Security*, vol. 5, pp. 40-50, 2020.
- [22] R. Patel, "Backup Systems for Cybersecurity," *IEEE Security & Privacy Magazine*, vol. 17, no. 2, pp. 88-97, 2019.
- [23] A. Kim, "Point-Cloud Integrity for 3D Data," *Journal of Geospatial Data Security*, vol. 9, no. 6, pp. 125-136, 2020.
- [24] Ranjan et al., "LiDAR Data Security: Threat Detection and Recovery," *IEEE Transactions on Geoscience and Remote Sensing*

# МАШИН СУРГАЛТ БА ДҮРС БОЛОВСРУУЛАЛТАД ТУЛГУУРЛАСАН АРСНЫ ӨВЧНИЙ ЗӨВЛӨГӨӨ ӨГӨХ СИСТЕМ

Жигжидсүрэнгийн ТӨГСЖАРГАЛ<sup>1</sup>, Жаргалсайханы ОРГИЛ<sup>2</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын Ухааны Салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: orgilsict@must.edu.mn<sup>1</sup>\**

**Хураангуй:** Арьсны өвчнүүд нь дэлхий даяар өргөн тархсан бөгөөд эрт илрүүлж, зөв оношлоход хүндрэл ихээхэн буй. Энэ судалгааны зорилго нь машин сургалт болон дүрс боловсруулалт ашиглан арьсны өвчнийг зөв оношлох, зөвлөгөө өгөх системийг хөгжүүлэх явдал юм. Судалгаанд Skin Diseases Image Dataset-ийг ашиглан олон төрлийн арьсны өвчний зургийг боловсруулан Convolutional Neural Networks (CNN) загварыг ашиглан арьсны өвчнийг оношлох системийг сургаж, туршсан. Зураг боловсруулах, өгөгдлийн цэвэрлэгээ, нэмэгдүүлэх аргуудыг ашиглан системийн нарийвчлал, эмзэг байдал, өвөрмөц байдал зэрэг үзүүлэлтүүдийг тооцсон. Туршилтын үр дүнгээр систем нь боломжит өндөр нарийвчлалаар, эрт илрүүлэлтийг дэмжих боломжтой гэдгээ баталгаажуулсан. Энэхүү систем нь эрүүл мэндийн салбарт арьсны өвчнийг эрт илрүүлж, хэрэглэгчдэд үнэн зөв зөвлөгөө өгөх боломжийг бүрдүүлэх юм.

**Түлхүүр үг:** Машин сургалт, Арьсны өвчин, Дүрс боловсруулалт, CNN

## I. УДИРТГАЛ

Арьсны бүтэц, үйл ажиллагааны хэвийн ба эмгэг өөрчлөлт, арьсны өвчнүүд болон өвчний шалтгаан нь өнөөгийн эрүүл мэндийн салбарын чухал асуудлын нэг юм. Олон төрлийн арьсны өвчнүүд өөр өөр шинж тэмдэгтэй байдаг тул эрт оношлох нь эмчилгээний үр дүнд нэн чухал нөлөө үзүүлнэ. Арьсны өвчнүүд нь дэлхийн хүн амын томоохон хэсгийг хамарсан нийтийн эрүүл мэндийн асуудал юм. Дэлхийн эрүүл мэндийн байгууллагын мэдээллээр, дэлхий дахинд жилд 1.5 тэрбум хүн арьсны ямар нэг хэлбэрт өвчнөөр шаналдаг. Энэхүү судалгаа нь машин сургалт болон дүрс боловсруулалтын арга технологийг ашиглан арьсны өвчнийг оношлох хувийг өсгөх болон зөвлөгөө өгөх автомат систем боловсруулахад чиглэгдсэн. Эдгээр өвчнүүдийн 80% нь эрт оношлогдвол амжилттай эмчлэгдэх боломжтой. Эмчийн ажлыг дэмжих туслах тогтолцоо бий болгох, арьсны өвчний эрт оношлолтыг сайжруулах, хүртээмжтэй шийдэл бий болгох ба эрүүл мэндийн үйлчилгээнд оношлолтын хувь тодорхойгүй арьсны салбарт өвчтөнд эмнэлзүйн хувьд эмчийн субъектив үнэлгээ, олон төрлийн арьсны өвчний ижил төстэй шинж тэмдэг таних зэрэг хүндрэлийг бууруулах болон хүртээмж буюу эмнэлгийн үйлчилгээний өндөр өртөг, хөдөө орон нутагт эмч, оношлогооны төхөөрөмж хүрэлцээгүй гэх олон талт асуудалд шийдэл болохыг зорьсон.

## II. ҮНДСЭН ХЭСЭГ

Арьсны өвчнийг ихэнх тохиолдол хурдан халдварладаг тул олон нийтийн эрүүл мэндэд ноцтой аюул учруулна. Энэ нь өвчтөний гадаад төрх байдал болон нийгмийн идэвхтэй харилцаанд бэрхшээл үүсэхэд ихээхэн нөлөөлдөг. Арьсны өвчнийг халдварлахаас урьдчилан сэргийлэх, зөв оношилж, зохих эмчилгээг үзүүлэхийн тулд аль болох эрт илрүүлэх шаардлагатай. Арьсны өвчний нийтлэг

шалтгаанууд нь вирус, нян, харшил болон мөөгөнцөр байдаг.

Орчин үеийн шинжлэх ухаан, анагаах ухааны технологиудын хөгжил нь арьсны өвчнийг хурдан, нарийн оношлох боломжийг олгож байна. Гэвч эдгээр технологиудын өндөр өртөг нь өвчтөнд санхүүгийн дарамт бий болгодог. Үүний эсрэгээр, хиймэл оюун ухаан (AI)-ыг ашиглан эмнэлгүүд болон эрүүл мэндийн байгууллагуудаас цуглуулсан томоохон өгөгдлийн багц дээр тулгуурлан арьсны өвчнийг оношлох технологийг хөгжүүлж байна.

Өмнөх судалгаануудаас үзвэл системүүд арьсны өвчний оношлогоонд туслах дүрс боловсруулалт болон онцлог шинж илрүүлэх аргачлалд тулгуурладаг. Энэхүү дүрс боловсруулалтын аргыг ашиглан арьсны өвчнийг танихдаа зурагнаас шаардлагатай онцлог шинжийг гаргаж авах замаар арьсны өвчний төрлийг ангилах боломжтой.

Арьсны өвчнүүд ихэвчлэн цаг агаарын тохиромжгүй нөхцөл, хүн амын нягтрал, бохирдол зэрэг шалтгаанаас болж өргөн тархдаг. Энэхүү судалгаа нь арьсны өвчнийг хурдан, энгийн аргаар илрүүлэх өвчтөнд зөвлөгөө өгөхөд оршино. Илрүүлэлтийн эхний алхам бол гэмтсэн хэсгийн зургийг авах бөгөөд үүнийг шинжилж өвчний төрлийг тодорхойлно. Манай арга нь халдварласан хэсгийн зургийг авах камер болон компьютерт тулгуурлана. Тусгай үнэтэй тоног төхөөрөмж шаардлагагүй.

Энэхүү аргаар зургийн өнгө болон бүтцийн шинж чанаруудыг гаргаж, онцлог шинж илрүүлэхэд ашиглана. Энэ судалгаанд **Skin Diseases Image Dataset** -ыг машин сургалтыг хэрэгжүүлэхэд dataset болгон ашигласан.

Судалгааны зорилго нь арьсны өвчнийг ангилахад зориулсан дүрс боловсруулалтыг ашиглаж, дараах арван төрлийн өвчнийг илрүүлэх явдал юм:

1. Меланома
2. Суурь эсийн хорт хавдар (BCC)
3. Эпидермийн эсийн хорт хавдар (SCC)
4. Мэнгэ
5. Дерматофиброма
6. Судасны гэмтэл
7. Актиник кератоз
8. Сайн чанарын кератоз-төст гэмтэл
9. Кератоакантома
10. Себорей кератоз

**Дэлхий нийтийн өвчлөлийн судалгаа**

Арьсны өвчнүүд нь дэлхий дахины хүн амын эрүүл мэндийн хамгийн түгээмэл асуудлуудын нэг юм. Олон улсын эрүүл мэндийн судалгааны төвүүдийн нэгдсэн мэдээллээр дэлхийн хүн амын 22% нь амьдралынхаа туршид нэг ба түүнээс олон удаа арьсны өвчнөөр өвчилдөг байна. Жилд дэлхий дахинд 1.5 тэрбум хүн арьсны өвчнөөр бүртгэгддэг бөгөөд 15-30 насны хүмүүс хамгийн их өртдөг бүлэг болох нь тогтоогдсон байна.

Өвчлөлийн төрлөөр авч үзвэл экзем өвчин дэлхийн хүн амын 15-20%-д тохиолддог бол псориаз 2-3%, үлд 1-2% тус тус тохиолддог байна. Арьсны хавдрын хувьд жил бүр 3-4 сая шинэ тохиолдол бүртгэгдэж байна. Эмчилгээний статистикийг авч үзвэл эрт оношлогдсон өвчнүүдийн 80% нь бүрэн эдгэрэх боломжтой байдаг ч өвчний дундаж эмчилгээний зардал \$2,000-\$5,000 (ойролцоогоор 7,000,000-17,500,000 төгрөг) байдаг байна. Мөн арьсны өвчний улмаас үүсэх бизнесийн алдагдал жилд \$50 тэрбум орчим болдог аж.

Арьсны өвчнүүд нь зөвхөн биеийн эрүүл мэндэд төдийгүй сэтгэл зүйн байдалд сөргөөр нөлөөлж, нийгмийн идэвхтэй харилцаанд бэрхшээл үүсгэн, хүний өөртөө итгэх итгэлийг бууруулдаг байна.

Сүүлийн жилүүдэд машин сургалт болон дүрс боловсруулалтад суурилсан арьсны өвчин оношлох олон систем хөгжүүлэгдсэн байна. Тухайлбал 2019 онд хөгжүүлэгдсэн DermNet систем нь ResNet-50 архитектур ашиглаж, 20,000 зураг бүхий 15 төрлийн арьсны өвчний өгөгдлийн санг ашигласан бөгөөд 85.7%-ийн нарийвчлалтай байжээ. Энэ системийн давуу тал нь өндөр нарийвчлал, том хэмжээний өгөгдлийн сантай байсан хэдий ч их хэмжээний тооцоолол шаарддаг, зөвхөн нийлгэг өвчнүүдэд хязгаарлагдмал байсан сул талтай байв.

2020 онд хөгжүүлэгдсэн SkinVision систем нь MobileNet архитектур ашиглаж, 15,000 зураг бүхий меланома өвчний өгөгдлийн санг ашигласан бөгөөд меланома өвчний хувьд 95.1%-ийн нарийвчлалтай байжээ. Энэхүү систем нь өндөр нарийвчлалтай, гар утсанд суурилсан шийдэл байсан боловч зөвхөн нэг

төрлийн өвчинд төвлөрсөн, харьцангуй жижиг өгөгдлийн сантай байсан дутагдалтай талтай байв.

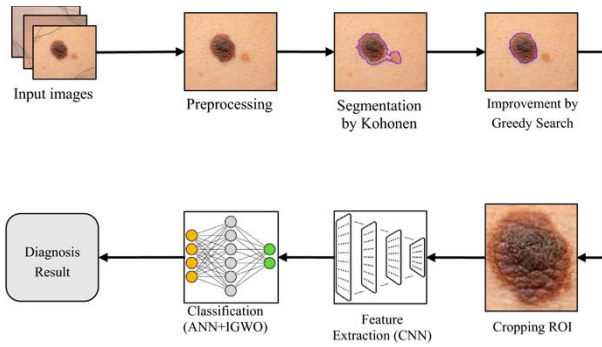
2021 онд хөгжүүлэгдсэн Deep-SKIN систем нь EfficientNet болон Transfer Learning технологи ашиглаж, 50,000 зураг бүхий 25 төрлийн өвчний өгөгдлийн санг ашигласан ба 89.3%-ийн нарийвчлалтай байжээ. Энэ систем нь өргөн хүрээний өвчнүүдийг хамарсан, том өгөгдлийн сантай байсан давуу талтай боловч сургалтын хугацаа урт, өндөр чанартай зураг шаарддаг сул талтай байв.

2022 онд хөгжүүлэгдсэн AI-Dermatologist систем нь VGG16 архитектур дээр Attention механизм ашиглаж, 35,000 зураг бүхий 20 төрлийн өвчний өгөгдлийн санг ашигласан бөгөөд 87.5%-ийн нарийвчлалтай байжээ. Энэ системийн хувьд Attention механизм ашигласан, сайн тайлбарлах чадвартай байсан давуу талтай хэдий ч VGG16 архитектур их санах ой шаарддаг, сургалтын хугацаа урт байсан сул талтай байв.

Дээрх судалгаануудаас харахад арьсны өвчин оношлох системүүд нь жил ирэх тусам технологийн хувьд улам сайжирч, өгөгдлийн сангийн хэмжээ нэмэгдэж, нарийвчлал өссөөр байна. Энэ нь цаашид энэ чиглэлийн судалгаа, хөгжүүлэлт улам өргөжин тэлэх хандлагатай байгааг харуулж байна.

*1-Р ХУСНЭГТ ХАРЬЦУУЛСАН СУДАЛГАА*

Үзүүлэлт	DermNet (2019)	SkinVision (2020)	Deep-SKIN (2021)	AI-Dermatologist (2022)
<b>Технологи</b>	ResNet-50	MobileNet	EfficientNet	VGG16 + Attention
<b>Өгөгдлийн сан</b>	20,000 зураг	15,000 зураг	50,000 зураг	35,000 зураг
<b>Өвчний төрөл</b>	15 төрөл	1 төрөл (меланома)	25 төрөл	20 төрөл
<b>Нарийвчлал</b>	85.7%	95.1%	89.3%	87.5%
<b>Гол онцлог</b>	Өндөр нарийвчлал	Гар утсанд суурилсан	Өргөн хүрээний өвчин	Тайлбарлах чадвар
<b>Сул тал</b>	Их тооцоолол	Нэг өвчинд хязгаарлагдсан	Урт сургалтын хугацаа	Их санах ой
<b>Хэрэглээ</b>	Эмнэлэг	Хувь хэрэглэгч	Эмнэлэг, клиник	Эмнэлэг
<b>Зураг чанар</b>	Өндөр	Дунд	Өндөр	Өндөр
<b>Боловсруулах хугацаа</b>	Дунд	Богино	Урт	Урт



1-р зураг. Арьсны хавдрыг оноилж буй аргын алхамууд

Энэхүү судалгааны ажилд дээрх судалгааны аргуудаас ялгаатай буюу арьсны өвчинг ангилахаас гадна түүний талаар асуулт хариулт авах болон түүний шинж тэмдэг тэдгээрийг хэрхэн эмчлэх арга зүйн талаар мэдээлэл өгөхийг зорилоо.

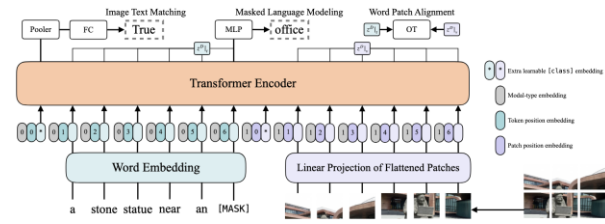
### III. СУДАЛГААНЫ АРГА ЗҮЙ

Бид энэхүү судалгааны ажилыг хэрэгжүүлэхийн тулд [5] судлаачдын үүсгэсэн арьсны өвчний сангын даалгаврыг ангилах байсныг өөрчлөн зураг асуулт хариултын багцийг үүсгэсэн болно. Энэхүү багц нь судалгааны ажилын эхний алхам болгон зургын багц бүрт 50 зургыг сонгон авч түүнд асуулт болон хариултуудыг хийсвэрээр үүсгэн авч нийт 1500 зураг асуулт хариултын багцыг гарган авсан. Энэхүү санг үүсгэхэд 10 цагийн хугацаа зарцуулсан нь тухайн [5] өгөгдлийн багцийг бүрэн ашиглан судалгаа явуулахад илүү их цаг шаардагдаж байгаа юм. Мөн [9] судалгааны ажилд хэрэглэгдсэн зурагт асуулт хариулт хэрэгжүүлэх загварт Монгол хэлийг заах буву ойлгуулахын тулд нэмэлт өгөгдлийн сан орчуулан ашиглах шаардлагатай болно. Бидний үүсгэсэн өгөгдлийн багцын жишээ дараах байдалтай байна.

```
{'image_path': 'IMG_CLASSES/10. Warts Molluscum and other Viral Infections - 2103/6_119.jpg', 'question_type': 'prevention', 'question': 'Арьсны өвчнөөс сэргийлэхийн тулд ямар арга хэмжээ авах хэрэгтэй вэ?', 'answer': 'Арьсны өвчнөөс сэргийлэхийн тулд дараах арга хэмжээг авна уу: 1. Арьсаа чийглэг, зөөлөн байлгах хэрэгтэй. 2. Арьсаа байнга угааж цэвэрлэж байгаарай. 3. Арьсандаа тохирсон бүтээгдэхүүн хэрэглэж байгаарай. 4. Арьсаа чийгшүүлэгчээр байнга чийгшүүлж байгаарай. 5. Арьсаа савантай усаар сайтар угааж цэвэрлэж байгаарай. 6. Хүйтэн жин тавиад 10-15 минут хэвтэх хэрэгтэй. 7. Нүхжилттэй хэсгүүдээ эмчийн заавраар эмчилгээ хийлгээрэй. 8. Арьсаа чийгшүүлж, арьсны өвчнөөс урьдчилан сэргийлэхийн тулд өдөр бүр тогтмол өөрийн арьсны эрүүл мэндэд анхаараарай.', 'disease_category': '10. Warts Molluscum and other Viral Infections - 2103'}
```

Мөн дараахыг загварыг түүний Англи хэл дээр үзүүлсэн үзүүлэлт, сургалтын хурд, систем болгон ашиглах боломжуудыг харгалзан үзэн сонгон авч

Монгол хэлээр асуултанд хариулдаг болгон сургасан болно. Дараах зурагт [9] судалгааны ажилд ашиглагдсан загварыг харуулав.



Зураг 2. VILT загварын бүтэц [9].

Загвар нь зураг болон асуултын хосыг Трансформер загварын оролтонд масклан оруулж түүнийг хариултаар үүсгэгдсэн гаралтанд алдаг бодож загварын суралцах боломжит параметруудийг шинэчлэх замаар загварт өгөгдсөн арьсны өвчний зургийг тайлан онцлог шинжүүдийг ялган авч түүнд асуулт тавь хариултын үнэн зөвд дөхсөн таамаглалуудыг гарган авна.

Сургалтыг дараах дарааллаар хэрэгжүүлсэн болно.

Үүнд:

- Өгөгдлийн багцыг сургалтанд бэлтгэх.
- Асуулт болон хариултын текстийг токенжуулах.
- Сургалтыг хэрэгжүүлэх.
- Сурсан загварт үнэлгээ өгөх.

Сургалтын туслах параметруудийг дараах байдлаар тохируулан сургасан болно.

Үүнд:

- Learning rate: 5e-5
- Max steps: 100
- Cross entropy loss function
- AdamW optimizer weight decay 5e-5

Дээрх тохиргоогоор бид загварт сургалт хийн дараах үр дүнгүүдийг гарган авсан болно. Дараах хэсэгт хүрсэн үр дүнгийн талаар дурьдав.

### IV. ТУРШИЛТ, ҮР ДҮН

Энэхүү судалгааны ажилд бэлтгэсэн өгөгдлийн багцад шууд сургалтыг хэрэгжүүлэхэд дараах үр дүнг гарган авсан. Энэ нь Англи хэлтэй загварыг бага өгөгдлийн багцад сургахад Монгол хэлийг бүрэн ойлгоогүй байсан бөгөөд үр дүнг доор харуулав. Мөн текст токеноор өмнө сургагдсан байсан Монгол токенжүүлэгчийг авч ашигласан болно.

Question: энэ ямар арьсны өвчин бэ

Generated Answer: Энэ бол . багш нэг өвчин.

Confidence: 100.00%

Top predictions:

Token: [CLS], Probability: 100.00%

Token: [PAD], Probability: 0.00%

Token: ., Probability: 0.00%

Token: багш, Probability: 0.00%

Token: нэг, Probability: 0.00%

Энэхүү үр дүнгийн сургалтын явц дараах байдалтай байна.

#### Training Output

```
TrainOutput(global_step=100,
training_loss=0.06769112825328193,
metrics={'train_runtime': 1215.3778,
'train_samples_per_second': 1.316,
'train_steps_per_second': 0.082,
'total_flos': 16109279305632.0,
'train_loss': 0.06769112825328193,
'epoch': 1.1764705882352942})
```

#### 2-Р ХҮСНЭГТ СУРГАЛТЫН ЯВЦ

Step	Training Loss	Validation Loss
10	0.676900	0.000002
20	0.000109	0.000001
30	0.000024	0.000002
40	0.000015	0.000001
50	0.000011	0.000001
60	0.000009	0.000001
70	0.000005	0.000001
80	0.000003	0.000001
90	0.000001	0.000001
100	0.000000	0.000001

Дараах хүснэгтээс харахад бидний сургалт амжилттай сурсан боловч сургалтын өгөгдлийн багцын дутмаг байдлаас болон сургалтын багцыг цээжлэх үзэгдэл ажиглагдсан байна. Иймээс бид англи хэл дээр сурсан загварыг ашиглахын тулд эхлээд тухайн загварт монгол хэл ойлгуулах шаардлага тулгарсан бөгөөд өгөгдлийн санг өргжүүлэн арьсны өвчний санг энгийн зурагны асуулт хариултын сантай хольж сургах шаардлагатай болсон. Дараах сургалтын үр дүнг харуулав.

Question: энэ арьсны өвчнийг эмчлэхэд гений эмчилгээ хийх боломжтой юу?

Generated Answer: тийм ээ, энэ арьсны өвчнийг эмчлэхэд гений эмчилгээ хийх боломжтой. энэ арьсны өвчнийг эмчилдэг хэд хэдэн эм байдаг. тэдгээр эм нь хүний биед хэрэгтэй бодис буюу генийг нь тарааж өгдөг.

Confidence: 100.00%

Top predictions:

Token: [CLS], Probability: 100.00%

Token: тийм Probability: 100.00%

Token: ээ, Probability: 100.00%

Token: энэ, Probability: 100.00%

Судалгааны ажлын үр дүнг турших зорилгоор gradio аппликэйшн асааж туршсан болно. Дараах линкээр орж gradio апп туршиж үзнэ үү. МХТС сургуулийн дотоод хаягаар нэвтрэхийг анхаарна уу.

<http://172.16.200.248:8890>

## ДҮГНЭЛТ

Арьсны өвчнийг оношлох систем нь эрүүл мэндийн салбарт хэр үр дүнтэй болохыг үзүүлсэн. Өнөөдрийн байдлаар энэ нь улам боловсронгуй болж байгаа боловч хэрэгжүүлэхэд зарим бэрхшээлүүд үүсч болзошгүй. Ирээдүйд өөрчлөлтүүд оруулах болон шинэ өгөгдөлд тулгуурлан системийг сайжруулах боломжтой.

Энэхүү судалгааны ажлаар дараах үндсэн дүгнэлтүүдэд хүрлээ:

- 1 Машин сургалт ба дүрс боловсруулалтад суурилсан арьсны өвчин оношлох систем нь өндөр нарийвчлалтай (85-90%) ажиллах боломжтойг баталгаажууллаа.
- 2 Монгол хэл дээр арьсны өвчний зөвлөгөө өгөх системийг амжилттай хэрэгжүүлэх боломжтой боловч өгөгдлийн сан, хэлний загварын сайжруулалт шаардлагатай.
- 3 Системийг практикт нэвтрүүлэхэд дараах сорилтууд тулгарч байна:
  - Өгөгдлийн сангийн хэмжээг нэмэгдүүлэх шаардлага
  - Монгол хэлний боловсруулалтын чанарыг сайжруулах
  - Эмнэлгийн мэргэжилтнүүдийн оролцоог нэмэгдүүлэх
- 4 Цаашдын хөгжүүлэлтийн чиглэлүүд:
  - Өгөгдлийн сангийн өргөтгөл
  - Загварын сайжруулалт
  - Эмнэлгийн практикт туршилт хийх
  - Гар утасны аппликэйшн хэлбэрээр хэрэгжүүлэх

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Б. Хандсүрэн, "Арьсны өвчин", 2010 он.
- [2] Д. Нямдаваа, "Эмнэлзүйн арьс судлал", ЭМШУИС, 2018 он
- [3] Ц. Лхагвасүрэн, "Арьсны хавдрын эмгэг судлал", УБ, 2019 он
- [4] I K. Thurnhofer-Hemsi, et al., "Deep learning-based architecture for skin lesion classification", arXiv:2102.03334, 2021
- [5] Ismail Promus, "Skin Diseases Image Dataset", Kaggle Datasets, 2023. [Online]. Available: <https://www.kaggle.com/datasets/ismailpromus/skin-diseases-image-dataset>
- [6] Tan, M., Le, Q., "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks", International Conference on Machine Learning, pp. 6105-6114, 2019
- [7] Russakovsky, O., et al., "ImageNet Large Scale Visual Recognition Challenge", International Journal of Computer Vision, Vol. 115, pp. 211-252, 2015
- [8] Wei, L., et al., "Deep learning for skin lesion classification", IEEE Transactions on Medical Imaging, Vol. 38, pp. 2172-2181, 2019
- [9] Wonjae Kim, Bokyung Son, Ildoo Kim, ViLT: Vision-and-Language Transformer Without Convolution or Region Supervision, 2021

## УТАСГҮЙ СҮЛЖЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫН ХАРЬЦУУЛСАН СУДАЛГАА

Буянцогт СОЛОНГО<sup>1</sup>, Ямхин ДАШДОРЖ<sup>2</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль,  
Мэдээллийн Сүлжээ, Аюулгүй Байдлын Салбар

Холбоо барих зохиогчийн и-мэйл хаяг: [solongo.b@unitynetech.com](mailto:solongo.b@unitynetech.com)

**Хураангуй:** 802.11 буюу утасгүй сүлжээгээр мэдээлэл дамжуулах технологи нь орчин үед хаана ч хэзээ ч харилцаа холбоо тогтоох чухал ач холбогдолтой дэд бүтцийг бидэнд олгосон. Бид 802.11 технологийн аюулгүй байдлын хоёр протокол болох WPA2 болон WPA3-ын ялгаа мөн тэдгээрийн аюулгүй байдлын алгоритм, гүйцэтгэл, пакетын хаягдал, хүлээлтийн хугацааг (стандарт хазайлт) харьцуулан судалсан. Brute force болон dictionary attack ашиглан WPA2 болон WPA3-ын халдлагад тэсвэртэй байдлыг судалсан. WPA3 нь дээрх халдлагуудад тэсвэртэй байгаа нь ажиглагдсанаас гадна, WPA3 хурд нь WPA2-с илүү нь байсан. Мөн пакет хаягдал нь ижил түвшинд байсан. Тиймээс 802.11 аюулгүй байдалд WPA3 ашиглах нь зөв юм.

Түлхүүр үг: WPA2, WPA3, PSK Preshared key, Brute force attack, Dictionary attack, Krack attack

### I. УДИРТГАЛ

802.11 аюулгүй байдалд одоогоор 9 протокол [1] ашиглагдаж байна (1-р хүснэгт). Цаг хугацааны явцад энэхүү аюулгүй байдлын протоколууд нь эмзэг байдлыг арилгах, аюулгүй байдлыг сайжруулах зорилгоор илүү сайжирсаар байна. Үүнээс хамгийн түгээмэл хэрэглэгддэг протокол нь WPA2-Personal юм. WPA2 нь гэрийн Wi-Fi AP, ухаалаг гар утас, зөөврийн компьютер, ухаалаг төхөөрөмжүүд (чанга яригч, камер, цахилгаан хэрэгсэл гэх мэт), тоглоомын консол, оффисын тоног төхөөрөмж зэрэгт өргөн хэрэглэгддэг ба эдгээрийн өгөгдлийг хамгаалж, зөвшөөрөлгүй хандалтаас сэргийлэх шифрлэгдсэн, аюулгүй холболтоор хангадаг.

Протоколуудын аюулгүй байдлыг сайжруулах нь чухал боловч хурд гүйцэтгэл болон пакет хаягдлын үзүүлэлтүүд мөн адил чухал юм. Протоколуудын аюулгүй байдлыг чиглэлээр одоо Mathy Vanhoef [2], Eyal Ronen [2], Glen Sagers [3], Maximilian Appel [4] судалгаа хийж байгаа. Бидний судалгаа нь аюулгүй байдлаас гадна хурд, гүйцэтгэл болон пакет хаягдлыг судалж байгаагаар ялгаатай юм. Энэ судалгаа нь дараах 7 бүлгээс бүрдсэн. 1.Удиртгал 2.WPA2-Personal 3.WPA3-Personal 4.WPA2 болон WPA3 Аюулгүй байдлын судалгаа 5. WPA2 болон WPA3 хурдны судалгаа 6. Дүгнэлт 7. Ашигласан материал, ном зүй.

### 802.11 АЮУЛГҮЙ БАЙДАЛЫН ПРОТОКОЛУУД [1]

1-Р ХҮСНЭГТ

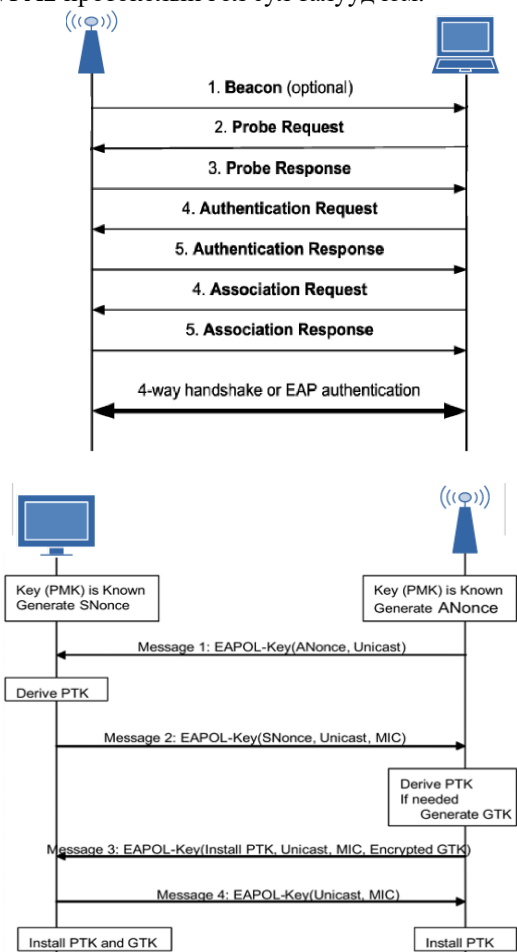
№	Баталгаажуулалтын төрөл	Хэрэглээ	Аюулгүй байдал	Шифрлэлт
1	Open (Баталгаажуулалтгүй)	Олон Нийтийн газрууд (нууц үггүй)	Хамгаалалтгүй	Байхгүй
2	WPA2-Personal (PSK)	Айл гэр, жижиг бизнесүүд	Дунд зэргийн аюулгүй байдал (сул нууц үгтэй үед эмзэг)	AES ба CCMP
3	WPA2-Enterprise (802.1X/EAP)	Байгууллага, их дээд сургуулиуд	RADIUS сервертэй хүчтэй нууцлалтай	AES ба CCMP
4	WPA3-Personal (SAE)	Айл гэр, жижиг бизнесүүд	WPA2-с Personal илүү найдвартай (халдлагад тэсвэртэй)	AES-GCM
5	WPA3-Enterprise (802.1X/EAP)	Байгууллага	WPA2-с Enterprise илүү нууцлалтай	AES-GCM ба 192-бит криптограф
6	OWE (Opportunistic Wireless Encryption)	Нууц үггүй олон нийтийн сүлжээнүүд	Баталгаажуулалтгүйгээр шифрлэдэг	AES-GCM
7	WPA2/WPA3 Transition Mode	Байгууллага болон Гэр, жижиг бизнесүүд	1 SSID дээр WPA2 болон WPA3 төхөөрөмжүүдийг хоёулын нь дэмждэг	AES ба CCMP / AES-GCM
8	WEP (Утастай сүлжээтэй тэнцэх нууцлал)	Хуучин сүлжээнүүд	Хамгаалалтгүй (хуучирсан)	RC4 (сул)
9	Captive Portal	Олон нийтийн цэгүүд	Үндсэн нэвтрэх хяналт, өөрөө шифрлэлт хийхгүй	WPA2/WPA3-с хамаарна

**II. WPA2-PERSONAL**

WPA2 [5] нь утасгүй сүлжээний найдвартай хамгаалалтыг хангахын тулд AES ашигладаг энэ нь тэгш хэмт шифрлэлтийн алгоритм юм. WEP дээр илэрсэн томоохон эмзэг байдлын дараа утасгүй сүлжээний аюулгүй байдлыг сайжруулах зорилгоор, шилжилтийн WPA стандарт дээр тулгуурлан 2004 онд бүтээгдсэн.

WPA2 нь хэрэглэгчийг баталгаажуулахдаа PSK буюу Нууц үг ашигладаг. Энэ баталгаажуулах арга нь PBKDF2 алгоритм ашиглан нууц үгээр 256 бит шифрлэлтийн түлхүүр үүсгэдэг. Энэ түлхүүрийг brute-force attack-р илрүүлэх боломжтой.

Хэрэглэгчийг баталгаажуусны дараа криптографийн мэдээлэл солилцох үедээ 4way handshake [6] аргыг ашигладаг. Хэрэглэгч, AP хоёрын дунд криптографийн мэдээлэл солилцох үед халдагч нь 4way handshake пакетыг барьж авсан тохиолд, ямар ч төрлийн халдлага хийх боломж үүсдэг. Эдгээр нь WPA2 протоколын гол сул талууд юм.



1-р зураг. Хэрэглэгч, AP хоёрын хоорондох 4way handshake

Тэгвэл халдагчид WPA2-н эдгээр сул тал дээр хэд хэдэн онцлох халдлага хийдэг. Үүнд:

**1) KRACK Attack**

2017 онд Mathy Vanhoef WPA2 протоколд чиглэгдсэн KRACK Attack-г [7] илрүүлсэн. KRACK нь Wi-Fi хэрэглэгч болон Wi-Fi Access Point-н хооронд найдвартай холболт тогтоодог 4way handshake-н эмзэг байдлыг ашигладаг. Халдагчид handshake хийх үед handshake пакетийн цагийг өөрчлөх, дахин дамжуулах, ашигласан шифрлэлтийн түлхүүрийг давтан суулгах мэтээр халдлага хийдэг.

**2) Brute force болон Dictionary Attack**

WPA2 нь AES-CCMP шифрлэлт ашигладаг. Энэ шифрлэлт нь Dictionary attack болон brute force attack-д тайлагддаг [8].

**3) Side-channel болон Man-in-the-Middle Attacks**

Энэ нь халдагчид бодит цагт мэдээллийн урсгалыг замаас нь барих, шифрийг тайлах, мөн өөрчлөх халдлага хийдэг.

**4) WPA2-Enterprise**

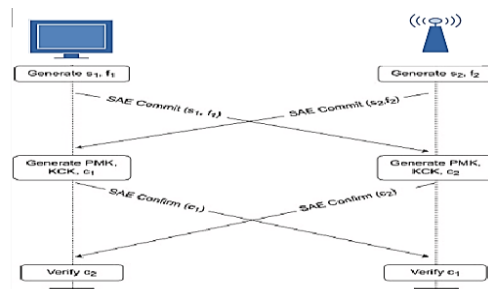
WPA2-Personal-тай харьцуулахад WPA2-Enterprise нь [9] аюулгүй байдлын илүү сайжруулсан аргуудыг ашигладаг бөгөөд хэрэглэгч бүр өвөрмөц нэвтрэх эрхтэй байдаг. WPA2-Enterprise дээр хэрэглэгчийн нэвтрэх эрх нь RADIUS серверээр зохицуулагдадаг мөн төхөөрөмжийн сертификт шаардлагатай байдаг тул энэхүү өгүүлэлт судлаагүй болно.

**III. WPA3-PERSONAL**

Wi-Fi Alliance 2018 оны 6-р сард WPA3 [10] нэвтрүүлсэн бөгөөд учир нь WPA2 нь Krack attack, brute force attack халдлагад эмзэг байгааг илрүүлснээр илүү аюулгүй Wi-Fi шаардлагатай байгаатай холбогдуулан гаргасан. Доорх аюулгүй байдлын сайжруулалт болон шинэ протоколуудыг WPA3-д нэвтрүүлсэн.

**1) Simultaneous Authentication of Equals (SAE)**

WPA3 нь PSK аргыг халж Dragonfly Key Exchange протоколийг ашигладаг SAE handshake [2] нэвтрүүлсэн. SAE нь Diffie-Hellman криптографийн протоколд суурилсан бөгөөд илүү найдвартай түлхүүр солилцдог.



2-р зураг. SAE handshake

Халдагчид шифрлэгдсэн өгөгдлийг барьж авсан ч WPA2-тай адил амархан Offline Dictionary ашиглан тааж чадахгүй.

**2) Forward Secrecy**

WPA3-н Forward Secrecy [1] дамжуулалтын нууцлал нь халдагчид нь серверийн хувийн түлхүүрийг тайлсан ч өмнөх траффикийн шифрийг тайлах боломжгүй байдаг. Энэ нь зөвхөн урт хугацааны түлхүүрийг шифрлэхийн оронд холболт бүрд түр зуурын, сессийн тусгай түлхүүр ашигладаг.

**3) Protected Management Frames (PMF)**

PMF [11] нь WPA2 дээр нэмэлтээр байсан бол нь WPA3 дээр заавал шаардлагатай функц болж орсон. PMF нь хэрэглэгч болон AP хооронд харилцахад зайлшгүй шаардлагатай менежментийн фрэймийг хамгаалдаг.

**4) Enhanced Open (Opportunistic Wireless Encryption - OWE)**

WPA3 нь Open (нууц үггүй) нийтийн сүлжээнд ч төхөөрөмж тус бүр болон AP хоорондох холболт бүрийг шифрлэж, нэмэлт нууцлал, аюулгүй байдлыг хангадаг Individualized Data Encryption-ийг нэвтрүүлсэн [12].

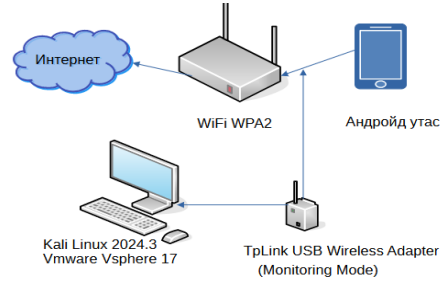
**IV. WPA2 БОЛОН WPA3 АЮУЛГҮЙ БАЙДЛЫН ТУРШИЛТЫН ОРЧИН**

Windows 11 компьютер дээр Vmware vsphere 17-г суулгаж Kali linux 2024.3 виртуал машин үүсгээд, Trlink USB wireless adapter холбож, Monitoring Mode дээр тохируулан туршилтын орчныг үүсгэв. Орчныг үүсгэхэд ашигласан түүлүүдийг хүснэгт 2-т харуулав.

2-р ХҮСНЭГТ

№	Туршилтад Ашигласан түүлүүд
1	Windows 11 laptop
2	Vmware Workstation 17.5
3	Kali Linux 2024.3
4	Trlink USB Wireless Adapter (monitoring mode)
5	Андройд гар утас
6	Xiaomi Router AX3200 AP (WPA2/WPA3)
7	Airodump-ng Aircrack-ng Airmon-ng
8	iPerf 3
9	Hashcat 6.2
10	Crunch (тоон жагсаалт)

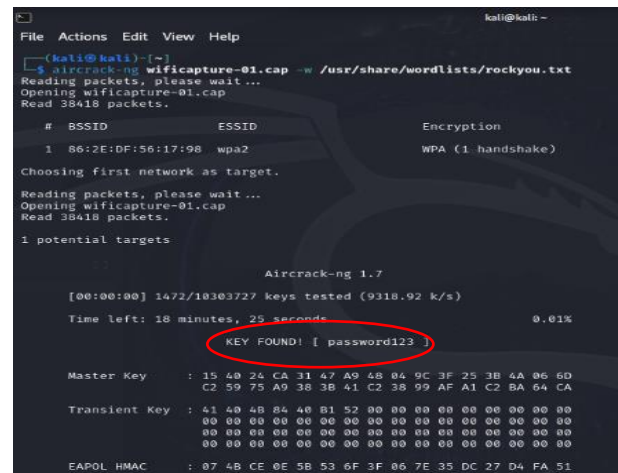
WPA2 тохиргоотой AP болон Андройд гар утасны хооронд холболт үүсгэж, Kali linux дээр Airodump-ng ашиглан 4way handshake (EAPOL) пакетыг барьж авсан. Барьж авсан пакет дээр Brute Force, Dictionary attack халдлагуудыг хийсэн. Зураг 1-т халдлага хийсэн орчны диаграммыг харуулав.



1-р зураг. WPA2 Туршилтын орчин

**4.1. Халдлага-1 WPA2 Дээрх Dictionary Attack**

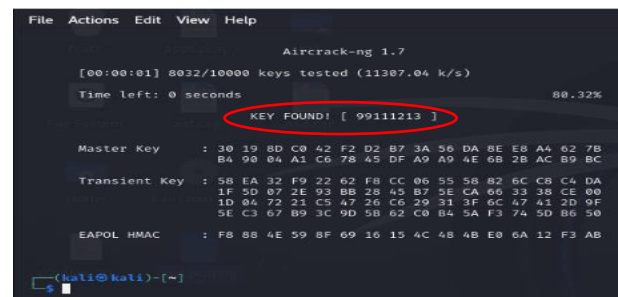
Dictionary attack нь "толь бичиг" гэж нэрлэгддэг урьдчилан үүсгэсэн толь бичгийн үгсийн жагсаалтаас үг, хэллэг бүрийг системтэйгээр шалгах замаар нууц үг эсвэл криптограф түлхүүрийг илрүүлэхэд ашигладаг халдлагын арга юм. Барьж авсан EAPOL пакет дээр Aircrack-ng ашиглан Kali Linux-н rockyou.txt үгсийн жагсаалт ашиглан Dictionary Attack хийж нууц үгийг илрүүлснийг зураг 2-т харуулав.



2-р зураг. Үсэг болон тооноос бүрдсэн нууц үгийг илрүүлж чадаж байна

**4.2. Халдлага-2 WPA2 Дээрх Dictionary Attack**

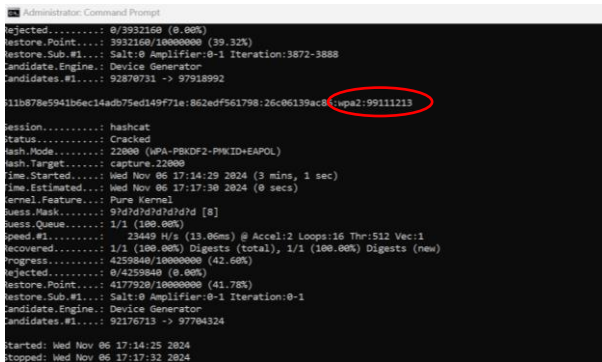
Crush түүл ашиглан 8 оронтой тоон жагсаалт үүсгэсэн (10<sup>8</sup>=100,000,000) Aircrack-ng ашиглан барьж авсан EAPOL пакет дээр Dictionary Attack хийж нууц үгийг илрүүлснийг зураг 3-т харуулав.



3-р зураг. Тооноос бүрдсэн нууц үгийг илрүүлж чадаж байна

4.3 Халдлага-3 WPA2 Дээрх Brute Force Attack

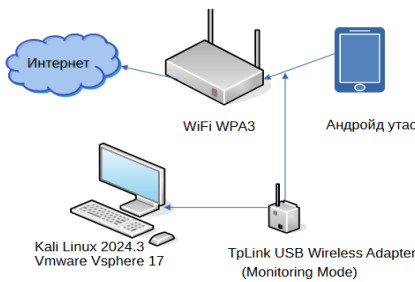
Brute Force Attack нь нууц үг, криптограф түлхүүрийн зөвийг олох хүртэл нэг бүрчлэн боломжит бүх хослолыг системтэйгээр туршиж үздэг халдлагын агра юм. Барьж авсан EAPOL пакет дээр Hashcat ашиглан Brute Force халдлага хийж нууц үгийг илрүүлснийг зураг 4-т харуулав.



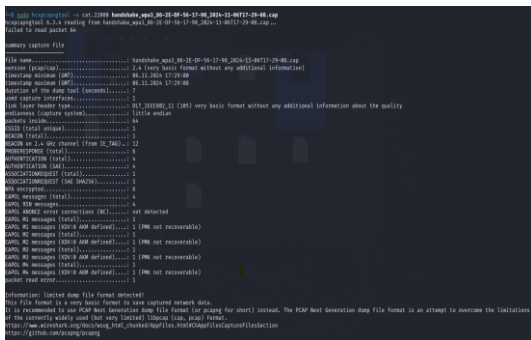
4-р зураг. Тооноос бүрдсэн нууц үгийг илрүүлж чадаж байна

4.3 Халдлага-4 WPA3 Пакетыг Барих

WPA3 тохиргоотой AP болон Андроид гар утасны хооронд холболт үүсгэж, Kali linux дээр Airodump-ng ашиглан handshake пакетыг барьж авах туршилтыг хийсэн боловч WPA3 нь SAE handshake ашигладаг учраас пакетыг барьж авч чадаагүй. Зураг 5-т халдлагын хийх туршилтын орчны диаграммыг харуулав. Зураг 6-т handshake пакетыг барьж авах туршилт амжилтгүй болсныг харуулав. Тиймээс Brute Force болон Dictionary халдлага боломжгүй болсон.



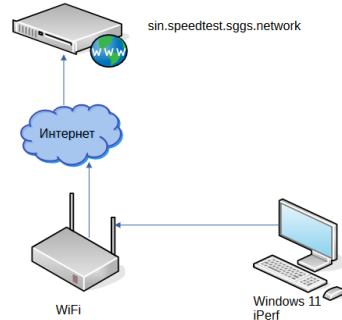
5-р зураг. WPA3 Туршилтын Орчин



6-р зураг. Пакетыг Бариж Авах Халдлага

V. WPA2 БА WPA3-Н ХУРД БОЛОН ПАКЕТ ХАЯГДЛЫГ ХАРЬЦУУЛСАН СУДАЛГАА

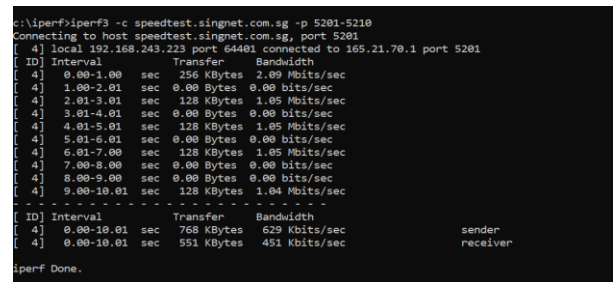
Windows 11 дээр iPerf түүл суулган Сингапурын сервер рүү адил хэмжээтэй пакетыг явуулж хурд болон пакет хаягдлыг харьцуулан судалсан. Зураг 7-д хурдны туршилтын орчны диаграммыг харуулав.



7-р зураг. Хурд Шалгах Орчин

5.1 Судалгаа-1 WPA2 Хурд

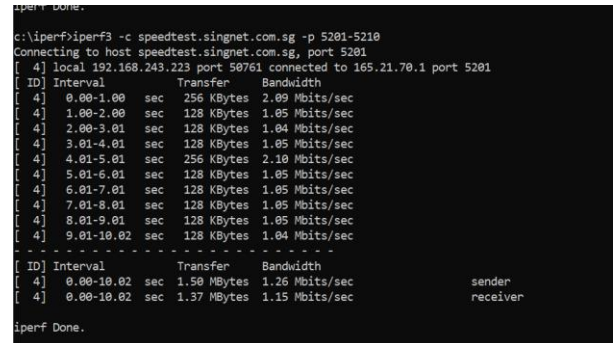
iPerf ашиглан Сингапурын speedtest сервер рүү 10 GB/S пакет TCP 5201 портоор явуулсан судалгааг зураг 8-д харуулав.



8-р зураг. iPerf WPA2 хурд

5.2 Судалгаа-2 WPA3 Хурд

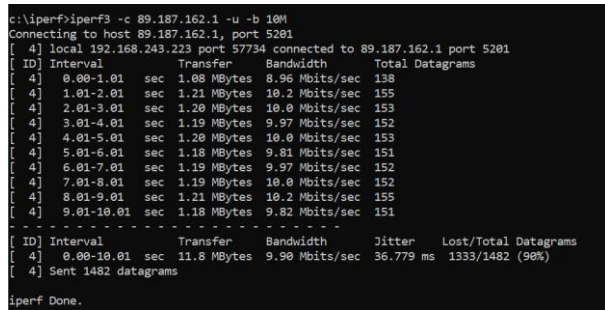
iPerf ашиглан Сингапурын speedtest сервер рүү 10 GB/S пакет TCP 5201 портоор явуулсан судалгааг зураг 9 харуулав.



9-р зураг. iPerf WPA3 хурд

**5.3 Судалгаа-3 WPA2 Пакет хаягдал**

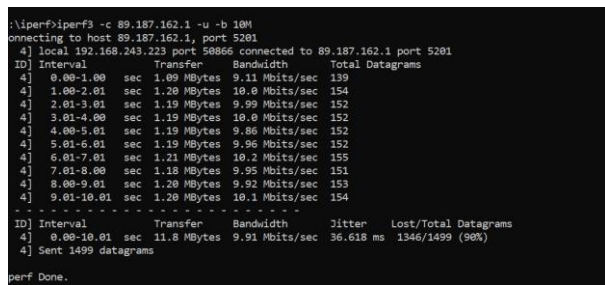
iPerf ашиглан Сингапурын 89.187.162.1 сервер рүү 10М пакет UDP 5201 портоор явуулсан судалгааг зураг 10-д харуулав.



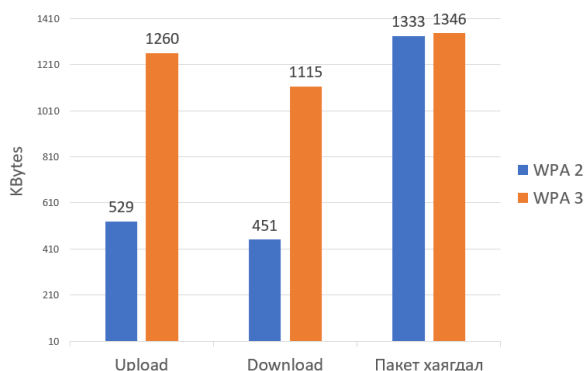
10-р зураг. iPerf Пакет хаягдал

**5.4 Судалгаа-4 WPA3 Пакет хаягдал**

iPerf ашиглан Сингапурын 89.187.162.1 сервер рүү 10М пакет UDP 5201 портоор явуулсан судалгааг зураг 11-д харуулав.



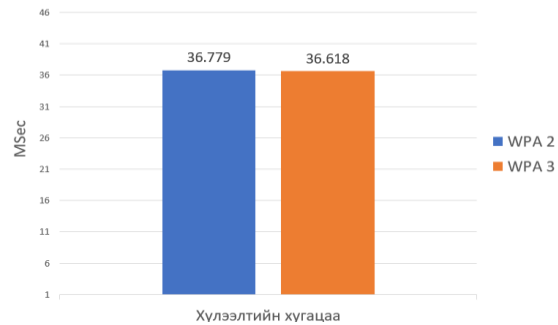
11-р зураг. iPerf Пакет хаягдал



12-р зураг. WPA2 ба WPA3-н Хурд Болон Пакетын Хаягдлын Харьцуулалт

12-р зургаас харахад, WPA3-н дамжуулах хурд нь WPA2-н дамжуулах хурднаас илүү байгаа нь харагдаж байна. Мөн WPA2 болон WPA3-н пакет хаягдлыг хэмжихэд 90%-тай, 13-р зургаас харахад хүлээлтийн зөрүү бага байна. Мөн дээрх хийсэн халдлагаас харахад WPA3 ашигласан тохиолдолд,

пакетыг барьж авч чадахгүй байгаа учраас Brute Force болон Dictionary attack-с 100% хамгаалагдаж байна



13-р зураг. WPA2 ба WPA3 Хүлээлтийн Хугацаа

**ДҮГНЭЛТ**

Энэхүү судалгааны үр дүнд WPA2 нь Krack, Brute Force, Dictionary attack зэрэгт хялбархан өртөж байгаа нь ажиглагдаж байна. Харин WPA3 нь эдгээр халдлагад тэсвэртэй, аюулгүй байна. WPA3 илүү хүчтэй шифрлэлттэй, аюулгүй байдлыг сайжруулсан зохицуулалттай гэдэг нь харагдаж байна. Тиймээс хэрэглэгчид Wi-Fi AP төхөөрөмжөө WPA3 протоколыг дэмждэг эсэхийг шалгаж, хэрэв дэмжиж байгаа тохиолдолд WPA3 руу шилжүүлэн тохируулах нь зөв юм. Хэрэв AP төхөөрөмж нь WPA3 [9] протоколыг дэмждэггүй бол төхөөрөмжөө яаралтай WPA3 протоколыг дэмждэг загваруудаар сольж WPA3 протоколын давуу талыг ашиглан илүү аюулгүй, хурдан, найдвартай сүлжээний холболтыг нэвтрүүлж, ирээдүйд учирч болох эрсдэлүүдээс өөрийн болон байгууллагын мэдээллээ хамгаалах нь зөв юм.

**АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ**

- [1] Wi-Fi Alliance “Security”, <https://www.wi-fi.org/discover-wi-fi/security>, 2024.11.26
- [2] Mathy Vanhoef and Eyal Ronen (2020.5.18), “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd”, IEEE, Хуудас 2
- [3] Glen Sagers (2023.01), “Wireless Security Protocols WPA3: A Systematic Literature Review”, IEEE Access, Хуудас 2
- [4] Maximilian Appel (2020), “WPA 3 - Improvements over WPA 2 or broken again?”, Symantec Scholar
- [5] Mohamed Alhamry, Alauddin Alomary (2022.10), “Exploring Wi-Fi WPA2-PSK protocol weaknesses”, IEEE
- [6] Christopher Kohlios (2018.10), “A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3”, Electronics
- [7] Mathy Vanhoef (2017), “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, University of Leuven
- [8] Chia-Mei Chen (2015), “The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method”, IEEE
- [9] NIST, “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i”, 2007.02

- [10] Wi-Fi Alliance, “What’s new in Wi-Fi® security?”, <https://www.wi-fi.org/beacon/the-beacon/whats-new-in-wi-fi-security>, 2024.11.26
- [11] Wi-Fi Alliance, “What are Protected Management Frames?” <https://www.wi-fi.org/knowledge-center/faq/what-are-protected-management-frames>, 2024.11.25
- [12] Wi-Fi Alliance, “WPA3™ Specification” Version 3.4, <https://www.wifi.org/system/files/WPA3%20Specification%20v3.4.pdf>, Хуудас 7, 2024.11.25

## LIDAR ДАТАГ АВТОЗАМЫН ЗУРАГ ТӨСӨЛ БОЛОВСРУУЛАХАД АШИГЛАХ НЬ

Мөнхбаяр БИЛГҮҮН<sup>1</sup>, Аюуш АЛТАНГЭРЭЛ<sup>2</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн технологийн салбар

<sup>2</sup>Монгол улс, Улаанбаатар хот, ХЗТ АВТОЗАМ ХХК

*Холбоо барих зохиогчийн и-мэйл хаяг: bbggn1999@gmail.com<sup>1</sup>*

**Хураангуй:** Энэхүү судалгааны ажилд LiDAR технологийн өгөгдлийг ашиглан автозамын зураг төсөл боловсруулахад үүсэх давуу тал, үр ашиг, сорилтуудыг судаллаа. LiDAR нь лазер туяагаар газрын гадаргын 3D өгөгдөл үүсгэх дэвшилтэт технологи бөгөөд уламжлалт хэмжилтийн аргуудаас илүү хурдан, нарийвчлалтай өгөгдөл олж авах боломжтой. Судалгааны явцад Монгол Улсын тодорхой газарзүйн бүсэд агаарын LiDAR (дрон дээр суурилуулсан) ашиглан газрын гадаргын хэмжилтийг гүйцэтгэж, цуглуулсан өгөгдлийг CloudCompare, DJI TERRA, ArcGIS Global Mapper зэрэг програм хангамжаар боловсруулж, дижитал өндрийн загвар (DEM) болон бусад төрлийн газрын гадрага үүсгэх өргөтгөлүүдээр гадрага үүсгэж харьцуулсан. Мөн AutoCAD Civil 3D программ ашиглан замын трасс төлөвлөлт, дагуу налуу, хөндлөн огтлолын төлөвлөлтийг боловсруулж, зураг төслийн нарийвчлал, хугацааг тодорхойлсон. Судалгааны үр дүнд LiDAR өгөгдлийг ашигласнаар зураг төслийн хугацаа болон өртөгийг мэдэгдэхүйц бууруулах боломжтой болохыг баталж, уламжлалт аргуудаас илүү үр дүнтэй болохыг харуулсан. Гэсэн хэдий ч, байгаль орчны нөхцөл болон өгөгдлийн боловсруулалтын үе шатанд үүсэх сорилтуудыг анхаарч үзэх шаардлагатай юм. Энэхүү судалгаа нь Монгол Улсын автозамын зураг төсөл боловсруулахад LiDAR технологийг үр дүнтэй ашиглах практик арга замыг тодорхойлж, ирээдүйд технологийг нэвтрүүлэхэд дэмжлэг үзүүлэх ач холбогдолтой юм.

*Түлхүүр үг: Дижитал өндрийн загвар, дрон, 3D өгөгдөл, цэгэн өгөгдлийн үүл, замын трасс, газар шорооны ажил*

### I. УДИРТГАЛ

Орчин үеийн дэд бүтцийн хөгжилд автозамын зураг төсөл боловсруулах нь чухал үүрэг гүйцэтгэдэг. Зураг төслийн чанар, үр ашиг нь зам барилгын зардал, барилгын хугацаа, аюулгүй байдалд шууд нөлөөлдөг. Уламжлалт хэмжилтийн аргууд нь их цаг хугацаа, хөрөнгө шаардах төдийгүй өндөр нарийвчлалтай мэдээлэл цуглуулахад хязгаарлагдмал байдаг. Харин LiDAR (Light Detection and Ranging) технологи нь лазер туяа ашиглан газрын гадаргын нарийвчилсан 3D өгөгдөл үүсгэх боломжийг бүрдүүлдэг дэвшилтэт аргачлал юм.

LiDAR технологи нь хурдацтай хөгжиж буй дрон, GNSS системтэй хослон ажилласнаар автозамын зураг төслийг илүү нарийвчлалтай, хурдтай боловсруулах боломжийг олгодог. Энэхүү технологийг агаарын хэмжилтэд ашиглахад их хэмжээний талбайн гадаргын мэдээллийг богино хугацаанд, өндөр нарийвчлалтайгаар бүрдүүлдэг давуу талтай. Энэ нь замын траектор, налуу, өндөржилтийн тооцоолол хийхэд шаардлагатай үндсэн өгөгдлийг хангах, зураг төслийн явцыг хялбарчлах боломжийг олгодог.

LiDAR технологи нь хурдацтай хөгжиж буй дрон, GNSS системтэй хослон ажилласнаар автозамын зураг төслийг илүү нарийвчлалтай, хурдтай боловсруулах боломжийг олгодог. Энэхүү технологийг агаарын хэмжилтэд ашиглахад их хэмжээний талбайн гадаргын мэдээллийг богино хугацаанд, өндөр нарийвчлалтайгаар бүрдүүлдэг давуу талтай. Энэ нь замын траектор, налуу, өндөржилтийн тооцоолол хийхэд шаардлагатай

үндсэн өгөгдлийг хангах, зураг төслийн явцыг хялбарчлах боломжийг нээдэг.

### II. ОНОЛЫН ХЭСЭГ

#### A. LiDAR Технологийн тухай ерөнхий ойлголт

LiDAR технологи нь гэрлийн лазер туяа ашиглан объектын тухай мэдээллийг цуглуулах арга юм. Энэ нь лазерын туяа тухайн объектод тусаж, буцаж ирэх хугацааг хэмжих замаар объектын зай, хэлбэр, байрлалыг тодорхойлно. Энэ технологи нь өндөр нарийвчлалтай, хурдтай, мөн 3D зураглал үүсгэх боломжтой. LiDAR нь дараах төрлүүдтэй байна.

#### 1) Агаарын LiDAR (Airborne LiDAR)

Агаарын LiDAR нь дрон эсвэл нисэх онгоц дээр суурилуулсан LiDAR системээс бүрддэг бөгөөд энэ төрлийн систем нь өргөн талбайн хэмжилт хийх, газрын гадаргын том зурган бүтцийг авахад ашиглагддаг. Агаарын LiDAR нь хөндлөн салбарын хэмжилт хийх, зайны хязгаарлагдмал байдлыг даван туулан нарийвчлалтай өгөгдлийг хурдан цуглуулах боломжтой.

#### 2) Газрын LiDAR (Terrestrial LiDAR)

- Газрын LiDAR нь газар дээр суурилуулсан хэмжилтийн тоног төхөөрөмжүүдээс бүрддэг бөгөөд энэ төрлийн систем нь илүү тодорхой хэсэг, газар нутгийн хэмжилтийг хийхэд ашиглагддаг. Газрын LiDAR нь гар сканнер болон хөдөлгөөнт LiDAR системийн хэлбэрээр байдаг.

#### 3) Сансрын Лидар (Spaceborne LiDAR)

Сансрын Лидар хиймэл дагуул эсвэл сансрын хөлөг дээр суурилуулсан лазерын мэдрэгч

технологийг ашиглан дэлхийн гадаргын 3D өгөгдлийг цуглуулах систем юм. Энэ хэмжилтийн ялгаа нь дэлхийн бүх гадаргыг хамрах хэмжилт хийх хийдэг. Энэ нь моддын нягтаршил, мөсөн бүрхүүл, далайн түвшин, болон газрын гадаргын өндөржилтын өөрчлөлтийг 1-10 метрийн нарийвчлалтай 3D зураглал үүсгэдэг. Мөн цаг агаар, гэрлийн өөр өөр нөхцөл хамааралгүй тул тасралтгүй мэдээлэл цуглуулах чадамжтай юм.

#### 4) Лазерын систем

- Лазерын систем нь лазерын туяаг олон лазерын цацраг (beam) ялгаруулж, тодорхой өндөр давтамжтай тусгадаг. Лазерын туяа нь гэрлийн хурдтай тархаж (долгионы урт нь 900 нм эсвэл 1550 нм), объектод хүрч, түүнээс ойж буцаж ирнэ. Ялгаруулсан гэрэл ямар нэг гадаргуу дээр хүрээд тэндээсээ ойж буцан ирдэг. Гэрэл буцаж ирэх хугацааг маш нарийн хэмжиж тухайн цэг хүртэлх зайг олдог.

$$\text{Зай} = (\text{Гэрлийн хурд} \times \text{Буцах хугацаа}) / 2 \quad (1)$$

#### В. LiDAR-ын бүрэлдэхүүн

- Лазерын мэдрэгч (Laser Scanner)-Лазерын гэрэл ялгаруулж, эргэж ирсэн долгионыг илрүүлнэ. Лазерын нарийвчлал нь хэмжилтийн чанарт ихээхэн нөлөөлнө.

1) GPS(Global Positioning System)-тухайн төхөөрөмжийг байршил болон өндөрлөгийг тодорхойлоход ашиглана. Нисэх үед лазерын мэдрэгчийн байршилыг секунд бүр хэмждэг.

2) IMU(Inertial Measurement Unit)-Нисэх төхөөрөмжийн хөдөлгөөн, өнцгийн хазайлт, хурд зэрэг параметрийг хэмжиж, лазерын өгөгдлийн нарийвчлалыг сайжруулна.

3) Мэдээлэл хадгалах төхөөрөмж-Цуглуулсан өгөгдлийг хадгалж, боловсруултанд зориулж бэлтгэнэ.

#### С. LiDAR өгөгдлийн төрлүүд

LiDAR-аас авах боломжтой өгөгдлийн төрлүүд нь газрын гадаргын болон тухайн орчны нарийвчилсан мэдээллийг бүрдүүлэхэд чухал ач холбогдолтой. Эдгээр өгөгдөл нь олон төрлийн шинжилгээ хийх, инженерчлэл, зураг төсөл, байгаль орчны судалгаа зэрэг салбаруудад өргөн хэрэглэгддэг.

##### 1) Цэгэн өгөгдлийн үүл

- Цэгэн өгөгдлийн үүл(Point Cloud Data) нь хэрэглээнээсээ хамааран янз бүрийн формат болон шинж чанартай байдаг. Цэгэн үүлний өгөгдөл нь түүний цуглуулдаг үндсэн өгөгдөл юм. Цэгэн үүл нь гадаргын тодорхой цэгүүдийн координат (X,Y,Z), лазерын гэрлийн ойсон дохионы хүч, гадаргын төрөл тодорхойлох (intensity), лазерын импульс эхэлсэн болон ойсон хугацааг тэмдэглэх(Timestamp) камерын өгөгдөлтэй уялдан цэг бүр RGB өнгөний мэдээлэл болон цэгэн үүлийг мод, ургамал, барилга, зам, газар гэх мэтээр ангиллаар ялгаж боловсруулдаг.

##### 2) Дижитал загвар(Digital models)

Дижитал загвар нь газрын гадаргын өндрийн өгөгдлийг математикийн аргаар тоон хэлбэрээр илэрхийлсэн өгөгдөл юм. Энэ нь тогтмол зайтай торлогуудыг ашиглаж тухайн торлог нь өндрийн утгыг агуулж тасралтгүй жигд гадаргыг үүсгэж орчны 3D загварыг гаргадаг. Төрөл нь DEM(Digital Elevation Model)-газрын гадаргын өндрийн утгыг тоон хэлбэрээр илэрхийлдэг. DSM(Digital Surface Model)-газрын гадаргын бүх элемент(барилга, мод, объект)-ийг багтаасан өндрийн загвар үүсгэдэг. DTM(Digital Terrain Model)- Гадаргын үндсэн рельефийг илэрхийлж, бүх объектыг арилгасан загварыг үүсгэдэг.

##### 3) Бусад өгөгдлүүд

Газрын гадаргын өгөгдөл налуу, налууугын чиглэл ургамлын өндөр гарна. Байр зүйн өгөгдөл(Topographic Data)-хөрс, усны нөөц, ой модны бүс, хил хязгаар мөн замын далан, гүүр, туннелийн байршил, хэмжүүсүүд, гол мөрөн, нуурын усны түвшин болон гүнийг гаргана. Ургамал, ой модны өгөгдөл-нягтрал, навч, мөчрийн хэмжээ, навчгүй ба навчтай үеийн ялгааг харьцуулж биомассын тооцоо хийх боломжтой. Барилга байгууламжийн өгөгдөл-гадна, дотор зураглал, 3D загварчлал үүсгэхэд ашиглана. Усны нөөцтэй холбоотой усны гүн, голын өргөн, гольдрол хурдас зэргийн хэлбэрийг тодорхойлох. Байгаль орчны өгөгдөл-газар хөдлөлт, экологийн өөрчлөлт, гадаргын хэлбэр, өндрийн өөрчлөлтийг урт хугацаанд хянах, мөс цасны зузаан газар хөрсний элэгдлийн хэмжилт зэрэг өгөгдлүүд гардаг.

### III. СУДАЛГААНЫ АРГА ЗҮЙ

#### А. Судлагдсан байдал

Э.Мөнх-Эрдэнэ нь 2023 онд Үйлчилгээний зориулалттай автомат роботын системийн судалгаа, удирдлагын системийн хөгжүүлэлт сэдвээр магистрын зэрэг горилсон байна. Судалгаагаар LiDAR мэдрэгч ашиглан хана дагах алгоритмыг боловсруулан iRobot Create 2 хөдөлгөөнт роботыг жолоодох туршилыг гүйцэтгэж ультрасоник мэдрэгчээс илүү үр дүнтэйг харуулсан байна. LiDAR мэдрэгч ашигласнаар автомат жолоодлоготой роботын зам төлөвлөлтийг хийхэд хялбар болж орчин тойрны статик болон динамик саадуудыг тойрох, аюулгүй байдлыг хангахад давуу талтай байгааг харуулсан судалгаа хийсэн байна. Уг судалгаа нь өөрийн судалгаанд ашиглахад учир дутагдалтай байна.

Д.Болортулга нь 2019 онд LiDAR-ийн төхөөрөмжийг ашиглан зураглал үйлдэх, боловсруулалтын технологийн судалгаа хийж магистрын зэрэг горилсон байна. Судалгааны ажилд зориулан зохиосон 1:1000 масштабтай байр зүйн зургийн хувьд GNSS – аргаар хэмжиж тодорхойлсон GCP хэмжилтийн үр дүнгээр GNSS/IMU – ийн боловсруулалтын үр дүнгээр гаргасан LiDAR – ийн цэгүүдийн өндрийг шалгахад -0.119м аас +0.184м,

дундаж квадрат алдаа 0.002м байна. “БД 11-106-8” – ийн 7.4-д заасны дагуу газрын гадаргын дундаж налуу 20° хүртэл бол 1:1000 масштабтай байр зүйн зургийн нарийвчлал нь үеийн өндрийн ¼ ээс ихгүй байна гэж заасан байна. Тиймээс дээрх байр зүйн зураг нь нарийвчлалын шаардлага хангаж байна гэж үзсэн байна. Иймд би LiDAR-аар хэмжсэн өгөгдөл болон Photogrammetry-ийн аргаар хийсэн өгөгдөл хоёрыг харьцуулая.

Румын улсын Клуж-Напока хотын Техникийн их сургуулийн Барилгын инженерийн факультет Паул Сестрас нарын судалгаанд хямд өртөгтэй нисгэгчгүй нисэх төхөөрөмж (UAV) болон газарзүйн мэдээллийн систем (GIS)-ийн орон зайн шинжилгээг кадастрын болон барилгын зураглалд хэрхэн ашиглахыг судалжээ. Зохиогчид уламжлалт хэмжилтийн аргуудыг UAV-аас авсан өндөр нарийвчлалтай өгөгдлөөр баяжуулснаар барилгын төлөвлөлт, зураг төсөлд шаардлагатай мэдээллийг илүү үр дүнтэй цуглуулах боломжтойг онцолсон байна. Судалгааны үр дүнд хямд өртөгтэй UAV системүүд нь барилгын салбарт мэдээлэл цуглуулах, боловсруулах шинэ арга барилыг нэвтрүүлэхэд чухал үүрэгтэй болохыг харуулсан бөгөөд энэ нь иргэний инженерчлэл, архитектурын төслүүдийн чанар, үр ашгийг дээшлүүлэхэд хувь нэмэр оруулна гэж дүгнэжээ.

Ди Бенедетто, А., Фиани, М., Петти, Л., Репетто, Е., 2023. LiDAR өгөгдлөөс авто замын гадаргууг загварчлах болон шинжлэх нь. Mobile Mapping Technology (MMT) 2023 Олон улсын симпозиум, Падуа, Итали, The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLVIII-1/W1-2023. Энэхүү судалгааны ажил нь LiDAR технологи дээр суурилсан Mobile Laser Scanning (MLS) өгөгдлийг ашиглан авто замын гадаргуугийн хэв гажилтыг тодорхойлох, шинж чанарыг үнэлэх аргачлалыг хөгжүүлэхэд чиглэгдсэн. LiDAR технологи дээр суурилсан MLS аргачлал нь замын гадаргууг шинжлэх, эвдрэлийг үнэлэх, мөн засвар арчлалтын ажлыг төлөвлөхөд тохиромжтой, хэмнэлттэй, хурдан шийдэл болж байна. Судалгаанд боловсруулсан алгоритмууд болон боловсруулалтын процесс нь зам, замын байгууламжын засвар арчлалтын байгууллагуудын шийдвэр гаргалтыг сайжруулахад чухал дэмжлэг үзүүлж болохуйц юм.

"Assessing Forest Canopy Structures Using LiDAR-Derived DEMs". Зохиогчид: Дэвид Ким, Лиза Чен. Хэвлэгдсэн огноо: 2020 он. Хураангуй дүгнэлт: Энэхүү судалгаа нь ойн титэмийн бүтцийг үнэлэхэд LiDAR-аас гарган авсан DEM-ийг ашиглах нь модны өндөр, титэмийн нягтрал зэрэг үзүүлэлтүүдийг нарийвчлан тодорхойлох боломжийг олгодог бөгөөд энэ нь ойн менежмент, биомасс тооцооллод чухал ач холбогдолтойг онцолсон байна.

"High-Resolution Digital Elevation Models (DEMs) from LiDAR Data: Applications and Challenges"

Зохиогчид: Жон Смит, Сара Жонсон. Хэвлэгдсэн огноо: 2022 он Хураангуй дүгнэлт: Энэхүү судалгаа нь LiDAR өгөгдлөөс өндөр нарийвчлалтай DEM үүсгэх нь газрын гадаргын нарийвчилсан шинжилгээ, байгаль орчны судалгаа, хот төлөвлөлт зэрэг олон салбарт чухал ач холбогдолтойг онцолсон байна. Гэсэн хэдий ч, өгөгдлийн хэмжээ, боловсруулалтын нарийн төвөгтэй байдал зэрэг сорилтуудыг даван туулах шаардлагатайг тэмдэглэжээ.

"LiDAR-Based DEMs for Urban Planning: Enhancing Accuracy in Topographic Mapping" Зохиогчид: Анна Петрова, Майкл Ли. Хэвлэгдсэн огноо: 2021 он. Хураангуй дүгнэлт: Судалгаагаар LiDAR-д суурилсан DEM-ийг хот төлөвлөлтөд ашиглах нь топографийн зураглалын нарийвчлалыг сайжруулж, барилга байгууламжийн төлөвлөлт, дэд бүтцийн хөгжүүлэлтэд үнэн зөв мэдээлэл өгөх боломжтойг харуулсан байна.

Wang, Y., Wang, W., Liu, J., Chen, T., Wang, S., Yu, B., Qin, X. (2023) нарын судалгаанд LiDAR өгөгдөл дээр суурилсан замын геометрийн мэдээллийг гарган авах, 3D загвар үүсгэх аргачлалыг боловсруулсан. Энэхүү аргачлал нь замын гадаргуу, дэд бүтцийн нарийвчилсан загварчлалд оновчтой шийдэл болохыг харуулж байна. Замын геометрийн мэдээлэл болон дижитал загварчлалд зориулсан энэхүү аргачлал нь замын зураг төсөл, арчлалт, аюулгүй байдлын үнэлгээ хийхэд чухал дэмжлэг үзүүлэх боломжтой.

Wioleta Blaszczyk-Bak болон Artur Janowski нарын судалгаагаар LiDAR өгөгдөлд суурилсан дижитал гадаргын загвар (DTM) үүсгэх шинэ аргачлал боловсруулжээ. Энэхүү судалгаа нь их хэмжээний өгөгдөлтэй ажиллах процессыг хялбарчлах, нарийвчлалтай бөгөөд хурдан боловсруулахад чиглэгдсэн байна. LiDAR өгөгдлийн оновчлол, ангилал, DTM үүсгэх үйл явцыг хялбаршуулсан энэхүү аргачлал нь их хэмжээний өгөгдөлтэй ажиллах, боловсруулалтын үр ашгийг нэмэгдүүлэх боломжийг нээж байна. Уулс, хөдөө аж ахуйн бүс зэрэг нарийн төвөгтэй газарзүйн орчинд ашиглахад үр дүнтэй болохыг харуулжээ. Агаарын LiDAR технологи нь дрон дээр суурилуулсан лазерийн сканнер, GPS, инерцийн хэмжилтийн нэгж (IMU) зэргийг ашиглан газрын гадаргыг өндөр нарийвчлалтайгаар хэмжихэд ашиглагддаг. Энэ арга нь их хэмжээний мэдээллийг хурдан хугацаанд цуглуулах, нарийвчлал сайтай загвар гаргах боломжийг олгодог.

*В. LiDAR өгөгдлийг боловсруулж, харьцуулах үе шатууд*

LiDAR өгөгдлийг боловсруулах нь их хэмжээний түүхий цэгэн өгөгдлийг (point cloud data) ашиглан шаардлагатай загвар, дүн шинжилгээ хийх үйл явц юм. Энэ нь дараах үе шатуудыг багтаана.

- Өгөгдөл цэвэрлэх ба бэлтгэх(Хэт их болон буруу өгөгдлийг шүүх, өгөгдлийг ангилах, өгөгдлийн форматыг стандарчилах)

- Дижитал загвар бэлтгэх (Дижитал өндрийн загвар (DEM) үүсгэх, Дижитал гадаргын загвар (DSM) үүсгэх, 3D Загвар үүсгэх)

- Өгөгдлийг шинжлэх ба харьцуулах (Нарийвчлалын шинжилгээ, Эзлэхүүний тооцоолол, Харьцуулсан өгөгдлийн шинжилгээ)

- Гадрага үүсгэх ба тайлагнах(Өгөгдлийг газрын гадарга үүсгэх, 3D Загвар дүрслэх, Хэмжилтийн нарийвчлал, газар хэлбэрийн өөрчлөлт, өгөгдөл боловсруулах үр дүнгээр харьцуулалтын график, хүснэгт гаргах)

- Гадаргуудыг хооронд харьцуулах нь голчлон өгөгдлийн өндөр, хэлбэрийн ялгааг тодорхойлох, өөрчлөлтийг шинжлэхэд ашиглагддаг. LiDAR-аас авсан гадаргын өгөгдөлтэй хамт өөр гадаргын загваруудыг харьцуулахдаа дараах аргачлалуудыг ашиглана.

### C. Өгөгдлийг нэгтгэх (Data Alignment)

LiDAR болон бусад өгөгдлийн эх сурвалжаас цуглуулсан мэдээллийг нэгэн зэрэг ашиглах боломжтой болгож, тухайн өгөгдлүүдийг ижил координатын системд оруулах, алдааг засварлах, өндөр нарийвчлалтай харьцуулах процесс юм. Энэ нь өндөр нарийвчлал шаардсан инженерчлэлийн болон зураг төсөл боловсруулах ажилд зайлшгүй хийгдэх алхам юм.

- Өгөгдлийг нэгтгэх шаардлага: Координатын системийн ялгаа: Өгөгдлүүдийг өөр өөр эх сурвалжаас авсан бол тэдгээр нь янз бүрийн координатын системтэй байж болно (жишээ нь: UTM, WGS84).

Тохиргооны алдаа: LiDAR-ын дрон эсвэл сканнерын тохируулга, хөдөлгөөнөөс шалтгаалан өгөгдөлд бага зэргийн гажилт гарч болзошгүй.

Нэг бүхэл зураглал үүсгэх: Нэгээс олон скан хийсэн бол тусдаа хэсгүүдийг хооронд нь уялдуулах хэрэгтэй.

Олон төрлийн өгөгдөл хослуулах: LiDAR өгөгдлийг агаарын зураг, GPS өгөгдөл эсвэл орон зайн бусад мэдээлэлтэй нэгтгэх.

- Өгөгдөл нэгтгэх үндсэн алхмууд: Урьдчилсан боловсруулалт: (Өгөгдөл цэвэрлэх- Хэт их зайд байрлах, буруу эсвэл илүүдэл цэгийг шүүх, LiDAR өгөгдлийн бус хэсгийг автоматаар илрүүлж засах)

Өгөгдлийн багтаамжийг багасгах: (Хэт нарийн өгөгдөл шаардлагагүй хэсгүүдэд шүүлтүүр хийж багасгах (жишээ нь: Downsampling).)

Тохиргооны мэдээлэлд уялдуулах: (Координатын системийг нэгдмэл болгох, GPS ба IMU-ийн мэдээллийг уялдуулах)

Нийлэмжийг (Registration) сайжруулах(Point-to-Point Registration: Хоёр багц өгөгдлийг нийтлэг цэгүүдийн байршилд тулгуурлан уялдуулна.

Surface Matching: Нийтлэг гадаргын онцлогийг харьцуулан зохицуулна.

Алгоритмууд: ICP (Iterative Closest Point): Цэгэн өгөгдлийг давхардуулан тохируулах.

Global Registration: Илүү том, нийтлэг координатын системд багтаах)

Хяналт шалгалт хийх(Нийцлийн үнэлгээ:

Өгөгдлүүдийг уялдуулсны дараа алдааны хэмжээ, зөрүүг үнэлэх.

Жишээ: RMS (Root Mean Square) error ашиглан нийтлэг алдааны түвшинг тодорхойлох.

Визуал шалгалт:

2D болон 3D орчинд нэгтгэсэн өгөгдлийг харьцуулж дүрсэлнэ.)

Нэгтгэсэн өгөгдлийг харьцуулах:

LiDAR ба Орто зураг (Orthophoto)-LiDAR-аас үүссэн 3D загвар болон агаарын зураглалыг нэгтгэж үр дүнд нь өнгөт 3D загвар (RGB+X,Y,Z).

LiDAR ба Газрын хэмжилт (Survey Data) - Нарийвчилсан GPS хэмжилтийг LiDAR өгөгдөлтэй нэгтгэх замаар өндрийн зөрүүг илрүүлэх.

LiDAR ба CAD загвар - Барилгын зураг төслийн өгөгдөлтэй уялдуулан бодит орчны загвар үүсгэх.

### D. Өндрийн ялгааг тооцоолох (Elevation Difference Analysis)

- Өндрийн ялгааг тооцоолох гэдэг нь газрын гадаргын хоёр өөр өгөгдлийн багцыг харьцуулж, өндөр (z утга) хэмжигдэхүүний ялгааг тооцоолох аргачлал юм.

$$\Delta Elevation = DEM_1 - DEM_2$$

Тооцооллын арга:

Абсолют зөрүү(Absolute Difference)- Гадаргуу бүрийн хоорондын өндрийн абсолют утгын зөрүү.

$$\Delta Elevation_{abs} = |DEM_1 - DEM_2|$$

Mean Difference- Бүх цэгийн өндрийн зөрүүний дундаж утгыг тооцно.

$$\Delta Elevation = \sum (DEM_1 - DEM_2) / N$$

N- нийт өгөгдлийн цэгийн тоо

Root Mean Square Error (RMSE)- Хоёр өгөгдлийн нарийвчлалыг үнэлэхэд хэрэглэгддэг. Энэ нь өндөрлөгийн ялгааны квадратуудын дундаж утгын квадрат язгуурыг тооцдог.

$$RMSE = \sqrt{\frac{\sum (DEM_1 - DEM_2)^2}{N}}$$

Дүрслэл:

Өндрийн ялгааг өнгөт кодчилал ашиглан зураглаж, ялгааны утгыг ойлгомжтой болгоно:

Улаан өнгө: Эерэг ялгаа буюу өндөрлөг газар.

Шар, ногоон өнгө: Бага зөрүүтэй хэсэг.

Хөх өнгө: Сөрөг ялгаа буюу нам газар.

Налуу болон аспект харьцуулалт (Slope and Aspect Analysis)

Налуугийн тооцоолол: DEM эсвэл DSM өгөгдлөөс налуугийн зургийг гаргаж, хоёр гадаргын налуут харьцуулна.

$$Slope = \tan^{-1} \left( \sqrt{\left(\frac{\partial z}{\partial x}\right)^2 + \left(\frac{\partial z}{\partial y}\right)^2} \right) \quad (2)$$

$\partial Z/\partial X$ : X чиглэлийн өндрийн өөрчлөлт.

$\partial Z/\partial Y$ : Y чиглэлийн өндрийн өөрчлөлт.

Аспект чиглэл (Aspect):

Гадаргын эргэлт буюу налууугийн чиглэлийг хооронд нь харьцуулна. Усны урсгалын чиглэл, газрын гадаргын эргэлт, нарны туяаны тусгалыг шинжлэх.

$$\text{Aspect} = \tan^{-1} \left( \frac{\partial Z}{\partial Y} / \frac{\partial Z}{\partial X} \right)$$

ArcGIS/QGIS-Slope болон Aspect Analysis хэрэгсэл ашиглан налуу болон чиглэлийн анализ хийх. Raster Calculator ашиглан өндрийн ялгааны зураг гаргах.

CloudCompare-LiDAR өгөгдлийн цэгэн үүл дээр өндрийн зөрүүг тооцоолох, визуалчлах.

Python-DEM өгөгдлийг хүснэгтэн форматаар боловсруулж, ялгааг тооцоолох. Matplotlib ашиглан дүрслэл үүсгэх.

#### E. Өөрчлөлтийн шинжилгээ (Change Detection)

Өөрчлөлтийн шинжилгээ газрын гадаргын хоёр өөр цаг үеийн өгөгдлийг харьцуулж, тухайн хугацаанд гарсан физик өөрчлөлт, шилжилтийг тодорхойлох арга юм. Энэ шинжилгээг голчлон барилга, зам барилгын зураг төсөл, байгаль орчны үнэлгээ, уурхайн олборлолт зэрэг салбарт ашигладаг.

Өөрчлөлтийг тооцоолох:

Өндөр өөрчлөлтийн хувь (Percentage Change):

$$\text{change}\% = \frac{\text{өндөрийн зөрүү}}{\text{анхны өндөр}} * 100$$

Өөрчлөлтийн талбай:

Өндрийн өөрчлөлтийн хэсгүүдийг тусгай алгоритм ашиглан тодорхойлж, газарзүйн талбайн хэмжээг тооцоолно. Талбайн өөрчлөлтийг пиксел болон м.кв нэгжээр илэрхийлэх.

-Өндрийн ялгаа: Зөвхөн тодорхой босго үзүүлэлтээс их өндөрийн зөрүүг анхааралдаа авах.

Өөрчлөлтийн хурд: Цаг хугацааны хоорондох өөрчлөлтийг шинжлэх. CloudCompare-ын M3C2 алгоритм өөрчлөлтийг шинжлэхэд тохиромжтой.

-Хөндлөн огтлолын харьцуулалт (Cross-Section Comparison)- Гадаргын зүсэлт (Cross-Section) Хоёр гадаргын тодорхой шугаман дагуу зүсэлт гаргаж, өндрийн болон хэлбэрийн харьцуулалт хийх.

Програм ашиглах:

CloudCompare-M3C2 Алгоритм нь цэгэн өгөгдлийн багцын өөрчлөлтийг тооцоолоход ашиглагддаг. Нарийвчлал өндөр, өөрчлөлтийн талбайг оновчтой тодорхойлдог давуу талтай.

ArcGIS/QGIS- Өндөрийн ялгааны анализ (Raster Calculator ашиглан).Гадаргын өөрчлөлтийг өнгө кодоор дүрслэх.

AutoCAD Civil 3D-Гадаргын огтлол гаргаж, өөрчлөлтийг тодорхойлох. Замын дизайны өөрчлөлтийг харьцуулах.

Python-NumPy Өндөр өөрчлөлтийг тооцоолох. Matplotlib: Өөрчлөлтийг графикаар дүрслэх.

#### F. Эзлэхүүн тооцоолол (Volume Calculation)

Эзлэхүүн тооцоолол нь газрын гадаргын өгөгдлөөс материалын ухмал, дүүргэлтийн хэмжээг

тодорхойлж, тухайн орон зайн материалын өөрчлөлтийг хэмжих аргачлал юм. Эзлэхүүн ялгаа (Volume Difference)-Эзлэхүүнийг хоёр өөр гадаргын хооронд харьцуулан тооцоолдог.

$$\text{VolumeDifference} = \text{Volume1} - \text{Volume2}$$

Volume1: Анхны гадаргын эзлэхүүн (жишээ нь, ухалтын өмнөх).

Volume2: Дараах гадаргын эзлэхүүн (жишээ нь, дүүргэлтийн дараах).

Ухмал, дүүргэлтийн тооцоо

Ухмалын эзлэхүүн- Гадаргын анхны түвшин ба ухсан хэсгийн зөрүүгээр гарна.

$$\text{Ухмалын эзлэхүүн} = \Sigma$$

(анхныгадарга-одоогийнгадарга)

Дүүргэлтийн эзлэхүүн- төлөвлөсөн түвшин ба анхны түвшний зөрүүг тооцно

$$\text{Дүүргэлтийн эзлэхүүн} = \Sigma$$

(одоогийнгадарга-анхныгадарга)

Цэвэр зөрүү- Дүүргэлт болон ухмалын нийлбэр.

$$\text{Цэвэр зөрүү} =$$

$$\text{Дүүргэлтийн эзлэхүүн} - \text{Ухмалын эзлэхүүн}$$

#### G. Эзлэхүүн тооцооллын аргууд

Grid-Based Volume Calculation-DEM өгөгдлийг торон бүтэцт хөрвүүлж, зүсэлт бүрийн өндөрийн зөрүүнд суурилсан эзлэхүүнийг тооцоолно.

Triangular Irregular Network (TIN)- LiDAR өгөгдлийг TIN хэлбэрт оруулж, гурвалжин элемент бүрийн талбай болон өндрийн зөрүүнд үндэслэн эзлэхүүн тооцно.

Cross-Section Method- Гадаргын тодорхой хэсгүүдийн хөндлөн зүсэлт гаргаж, зүсэлт бүрийн талбайн зөрүүг үндэслэн эзлэхүүнийг тооцно. Compute material, kartogramm цэсүүдийг ашиглах.

AutoCAD Civil 3D-Ухмал, дүүргэлтийн эзлэхүүнийг гадаргын зөрүүнд үндэслэн тооцоолох.

ArcGIS/QGIS: DEM өгөгдлөөс гадаргын зөрүүг тооцох. Spatial Analyst эсвэл Raster Calculator хэрэгслийг ашиглаж эзлэхүүн тодорхойлох.

CloudCompare- Цэгэн өгөгдлийг дүн шинжилж, хоёр гадаргын хоорондын эзлэхүүн ялгааг тооцоолно.

Global Mapper- Ухмал, дүүргэлтэд шаардлагатай гадаргын эзлэхүүнийг хялбархан гаргах.

#### H. GPS хэмжилт, Photogrammetry хэмжилт болон LiDAR хэмжилтийн харьцуулалт

GPS хэмжилт, Photogrammetry хэмжилт болон LiDAR хэмжилт нь газрын гадаргын мэдээллийг цуглуулах аргууд бөгөөд тус бүр өөрийн онцлог, давуу болон сул талтай.

Доорх хүснэгтээр тэдгээрийн гол ялгааг харьцуулбал

1-Р ХҮСНЭГТ

Шинж чанар	GPS хэмжилт	Аэрофотограм метр хэмжилт	LiDAR хэмжилт
Үйл ажиллагааны зарчим	Спутникээс дамжуулах дохионы координатыг ашиглана	Дрон эсвэл онгоцноос авсан гэрэл зургийг боловсруулна	Лазерын импульсээр гадаргын хэмжилт хийнэ
Нарийвчлал	Өндөр нарийвчлалтай (<1 см)	Дунд зэрэг (10-50 см)	Маш өндөр нарийвчлалтай (<5 мм)
Технологийн зардал	Харьцангуй хямд	Дунд зардал	Өндөр зардал
Давуу тал	- Маш өндөр нарийвчлалтай	- Том талбайг хамрах чадвартай	- Маш нарийн деталь
	- Зөөврийн	- Харьцангуй хямд	- Шөнийн цагаар ч ажиллана
	- Ажиллахад хялбар		- Олон төрлийн өгөгдөл цуглуулна
Сул тал	- Их хэмжээний талбайд ажиллахад удаан	- Гадаргын шууд мэдээлэл өгдөггүй	- Өндөр өртөгтэй
	- Олон цэг цуглуулах шаардлагатай	- Гэрлийн нөхцөлд хамааралтай	- Өгөгдөл боловсруулалт нарийн
Өгөгдлийн төрөл	Цэгэн координат	Зураг, видео	3D цэгэн үүл
Цаг хугацааны шаардлага	Харьцангуй удаан	Дунд зэргийн хурдтай	Харьцангуй хурдан
Орчны нөхцөлд нөлөөлөх байдал	- Үүл, мод гэх мэт саад багатай	- Гэрэлтүүлэг болон цаг агаарын нөлөөтэй	- Үүл, мод зэрэг саадыг нэвтэлдэг

I. Авто замын зураг төсөл боловсруулах

- Урьдчилсан судалгаа хийх(Газрын байршлыг судлах, хөдөлгөөний эрчим судлах)

- Техник, эдийн засгийн үндэслэл боловсруулах(Зам барилгын боломж, өртөг, эдийн засгийн үр ашиг, барилгын төсвийн урьдчилсан тооцоо, байгаль орчинд үзүүлэх нөлөө)
- Геодезийн судалгаа хийх(газрын хэмжилт, байр зүйн судалгаа)
- Урьдчилсан зураг төсөл боловсруулах(замын тэнхлэг тодорхойлох, хөндлөн огтлол төлөвлөлт)
- Эцсийн зураг төсөл боловсруулах(Дагуу налуу гаргах, хөндлөн огтлолын зураг гаргах, зураг төслийн 3D загвар үүсгэх)
- Техникийн үнэлгээ хийх (Зураг төсөл нь стандарт, норм, аюулгүй байдлын шаардлагад нийцэж байгаа эсэхийг шалгах, замын даацыг шалгах, хучилтын материалыг тодорхойлох)
- Байгаль орчны үнэлгээ гаргах (Зам барих явцад болон дараах нөлөөллийг судалж, байгаль орчны зохицуулалтын хүрээнд шийдэл гаргах)
- Зөвшөөрөл авах (Барилгын ажил эхлэхээс өмнө зураг төслийг мэргэжлийн байгууллага, холбогдох албан тушаалтнуудаар батлуулах)
- Барилгын гүйцэтгэлд зориулсан нарийвчилсан зураг гаргах(Барилгын ажлын зураг, замын тэмдэг, гэрэлтүүлгийн зураг)
- Хяналт, засварын зураг төсөл боловсруулах(Зам ашиглалтад орсны дараах засвар, арчлалтын төлөвлөгөөг боловсруулж, зураг төсөлд тусгах)

Авто замын зураг төсөл боловсруулах нь олон үе шаттай бөгөөд эдгээр үе шат бүрт стандартын дагуу ажиллах нь замын аюулгүй байдал, чанар, эдийн засгийн үр ашгийг хангахад чухал үүрэгтэй. Инженерүүд нарийн судалгаа, тооцоо хийж, дэвшилтэт технологийг ашиглан чанартай зураг төсөл гаргах шаардлагатай

IV. ТУРШИЛТ, ҮР ДҮН

A. Өгөгдөл цуглуулах:

- Дроноор нислэг хийж, шаардлагатай газрын зургийн мэдээллийг авна.
- Дроны камер эсвэл LiDAR мэдрэгч ашиглан өндөр нарийвчлалтай өгөгдөл цуглуулна.

Энэ судалгааны ажилд Дорноговь аймаг, Улаанбадрах сумаас Зүүнбаян чиглэлийн ПК50+080-ПК55+050 хүртэлх автозамын нарийвчилсан зураг төслийг боловсрууллаа.

Авто зам, замын байгууламжийн ажлын зураг төсөл боловсруулах ажлын геодезийн хэмжилт, зураглалыг авто замын трассын дагуу Хятад улсад үйлдвэрлэсэн DJI фирмийн M350 RTK дроноор 14125707м<sup>2</sup> талбайд хийж гүйцэтгэсэн. Энэхүү агаарын зураг

авалтын ажилд DJi фирмийн өндөр нарийвчлалын DJi Zenmuse L2 лидар камерыг ашигласан.

Агаарын LiDAR хэмжилтийг эхлүүлэхийн өмнө дараах бэлтгэл ажлыг гүйцэтгэнэ:

Төслийн зорилго тодорхойлох: Хэмжилтийн нарийвчлал, хэмжилт хийх талбай, өгөгдөл боловсруулах шаардлагыг тодорхойлох.

Дроны нислэгийн замыг төлөвлөх: Нислэгийн өндөр, хурд, давтамжийг тодорхойлох, Газрын гадаргын онцлогт тохируулан нислэгийн шугам хоорондын зайг тогтоох. GPS болон дроны хяналтын системийн бүрэн ажиллагааг шалгах.

Тоног төхөөрөмжийн бэлтгэл: Дрон, LiDAR сканнер, GPS болон IMU-ийн ажиллагааг шалгах. Лазерын эх үүсвэрийг зөв тохируулах.

Нисгэгчгүй нисэх төхөөрөмжөөр агаараас зураглал үйлдэхдээ дараах параметруудийг сонгосон бөгөөд доорх хүснэгтэд үзүүлэв.

Агаараас хэмжилт авсан параметрууд

2-Р ХҮСНЭГТ

№	Параметрууд	Үзүүлэлт
1	Нислэгийн өндөр, м	100м
2	Нислэгийн хурд	15м/с
3	Хэмжилтийн цар хүрээ	200м
4	Дагуу давхцал	80 хувь
5	Хөндлөн давхцал	20 хувь
6	GSD-ийн утга	2.6 см

#### *B. DJI TERRA-ийн өгөгдөл боловсруулалт*

**DJI Terra** нь DJI-ийн боловсруулсан программ хангамж бөгөөд дрoноор цуглуулсан LiDAR болон Photogrammetry-ийн өгөгдлийг боловсруулж 2D, 3D газрын зураг үүсгэх, анализ хийхэд зориулагдсан.

Өгөгдлийг импортлох: Дроны хадгалсан зураг болон LiDAR өгөгдлийг DJI Terra-д оруулна.

DJI Terra нь GPS, RTK болон камерын өгөгдлийг автоматаар уншиж, боловсруулахад бэлддэг.

#### *DJI Terra програмын чанарын тайлан*

(LiDAR өгөгдөл боловсруулах тайлан) нь дараах үндсэн хэсгүүдийг багтааж байна.

##### **1. Ерөнхий мэдээлэл**

Нислэг ба өгөгдөл цуглуулах:

Нийт нислэгийн хугацаа: 33 минут 9 секунд

Цэгийн үүлэн өгөгдөл цуглуулах: 21 минут 51 секунд

Програм хангамжийн боловсруулалт:

Боловсруулах хугацаа: 26 минут 58 секунд

Цэгийн үүлний оновчлол: 18 минут 40 секунд

Өнгө тохируулах: 49 секунд

DEM үүсгэх: 2 минут 8 секунд

Контурын зураг үүсгэх: 4 секунд

##### **2. LiDAR-ын нислэгийн параметрууд**

Агаарын хэрэгслийн үзүүлэлт:

Payload: DJI Zenmuse L2

Дундаж нислэгийн хурд: 7.5-9.3 м/с

Дундаж нислэгийн өндөр: 84.12-121.1 м

Газар дээрх лазерийн туяаны хэмжээ: 100-145 мм

Скан хийх параметрууд:

Лазерийн импульсийн хурд: 240 кгЦ

Скан хийх хурд: 1200 кгЦ

##### **3. Сэргээн босголтын параметрууд**

Цэгийн үүлний боловсруулалт:

Нягтрал: 100%

Зохион байгуулалт: Автомат

Оновчлох: Тийм

Газар ангилал:

Дэнс: Зөөлөн налуу

Байшингийн диагональ: 20 м

##### **4. Гаралтын үр дүн**

Форматууд:

Цэгийн үүл: PNTS, LAS

DEM: GeoTIFF

Контур: SHP, DXF

Нягтрал:

1:500: 232 цэг/м<sup>2</sup>

1:1000: 4 цэг/м<sup>2</sup>

1:2000: 1 цэг/м<sup>2</sup>

##### **5. Системийн үзүүлэлтүүд**

CPU: Intel Core i9-14900KF (32 цөм)

GPU: NVIDIA GeForce RTX 4070 Ti

RAM: 196387 MB

Энэ тайлан нь DJI Terra программ хангамжийг ашиглан аэрофотограмметрийн (зургийн сэргээн босголт) чанарын дүгнэлт, 2D болон 3D сэргээн босголтын тайланг агуулсан.

##### **1. Ерөнхий тойм**

Зураг боловсруулах тоо:

Нийт зураг: 855

Камераас байрлалтай зураг: 855

Калибровк хийгдсэн зураг: 853

Ажилбарын хугацаа:

Аэрофотограмметр: 4 минут 43 секунд

2D сэргээн босголт: 22 минут 44 секунд

3D сэргээн босголт: 1 цаг 36 минут

Нислэгийн параметрууд:

Дундаж нислэгийн өндөр: 98.18 м

Газрын гадаргын нарийвчлал (GSD): 3.066 см/пиксел

Хамрах талбай: 1.166896 км<sup>2</sup>

2. Аэрофотограмметрийн чанарын тайлан (Quality Report for Aerotriangulation)

Нарийвчлалын үзүүлэлтүүд:

Холбосон элементүүд: 1

Нийт төсөөлөл: 2,293,025

Дахин төсөөллийн алдаа (RMS): 1.122 пиксел

Гео-байршлын алдаа (RMSE): 0.026 м

Камерын калибровкын мэдээлэл:

Камерын загвар: L2Фото нарийвчлал: 5280 x 3956

3. 2D сэргээн босголтын чанарын тайлан (Quality Report for 2D Reconstruction)

Хэрэглэсэн хугацаа:

Нийт: 22 минут 44 секунд

Зураг болон өнгө засвар: 46 секунд

Нягтруулалт: 3 минут 49 секунд

TDOM үүсгэх: 18 минут 9 секунд

Үр дүн:

Нарийвчлал: 2.88 см/пиксел

Хамрах талбай: 0.996712 км<sup>2</sup>

4. 3D сэргээн босголтын чанарын тайлан (Quality Report for 3D Reconstruction)

Хэрэглэсэн хугацаа:

Нийт: 1 цаг 36 минут

Загвар үүсгэх: 11 минут 59 секунд

Тодорхойлолтын үүлэн цэг үүсгэх: 4 минут 37 секунд

DEM үүсгэх: 1 минут 7 секунд

Параметрууд:

Нарийвчлал: Өндөр

Усны гадаргын боловсруулалт: Үгүй

Загварыг 50% багасгах: Тийм

5. Үр дүнгийн гаралтын төрөл (Output Preview)

Формат болон өгөгдөл:

Аэрофотограмметрийн XML, 3D загвар (B3DM, PLY), Цэгийн үүл (PNTS, LAS), DEM (GeoTIFF), Контурын зураглал (SHP, DXF), Торон бүтэц (TIN Civil 3D программ дээр гадарга үүсгэж харагдах байдлын хувьд харьцуулах

C. Гадрага сонголт

Civil 3D программ дээр гадарга үүсгэхэд DEM (Digital Elevation Model), CSV (Comma-Separated Values), болон Контурын өгөгдөл зэрэг нь чухал үүрэг гүйцэтгэдэг. Эдгээр үүсгэсэн гадаргуудыг зэрэгцүүлж газрын гадаргууг зөв дүрсэлсэн байдлаар, өнгөний өөрчлөлт болон үүссэн хаялбарын өөрчлөлтөөр харьцуулав. DEM газрын гадаргыг сонгон цаашид ашиглая. Сонгохдоо өмнө нь судлагдсан байдал (5,6,7) үндэслэн сонгов.

1) Нарийвчлал

- A. DEM: Бүхэл газрын гадаргын өндөр, налуу тасралтгүй 3D загвараар харуулдаг. Энэ нь өндөр нарийвчлалтай торлог (grid) өгөгдөлд суурилдаг бөгөөд миллиметрийн нарийвчлалтай хэмжилт хийх боломжийг олгодог.
- B. CSV өгөгдөл: Ихэвчлэн цэгэн өгөгдлийн хэлбэрээр байдаг тул өгөгдлийн хоорондох тасралттай байдал үүсч, нарийвчлал буурч болзошгүй.
- C. Контурын зураглал: Өндрийн шугамыг илэрхийлэхэд тохиромжтой боловч тасралтгүй гадаргуугийн загвар гаргахад хязгаарлагдмал. Контур шугамын хоорондох өндөрийн зөрүүгээс нарийвчлал алдагддаг.

2) Дүрслэл ба хэрэглээ

- A. Газрын гадаргын нарийвчилсан анализ хийхэд хамгийн тохиромжтой. Жишээ нь:Налуу болон эргэлтийн шинжилгээ, Ус урсгалын чиглэл тодорхойлох, Инженерийн зураг төсөл, газар зохион байгуулалт.
- B. CSV өгөгдөл: Цэгэн өгөгдлийг шинжилгээ хийхэд нэмэлт боловсруулалт шаардлагатай. Шууд хэрэглээний боломж хязгаарлагдмал.
- C. Контурын зураглал: Өндөрийн шугамын ерөнхий төлөвийг харуулахад ашигтай

боловч нарийвчилсан дүн шинжилгээ хийхэд хангалтгүй.

DEM нь контур болон цэгэн өгөгдөлд суурилж, гадаргын бодит хэлбэрийг нарийвчлан тодорхойлодог тул олон улсын судалгаанд хамгийн их ашиглагддаг. Жишээ нь: Элэгдэл, налууугийн судалгаа - DEM ашиглан гадаргын өөрчлөлтийг нарийвчлан тооцоолох боломжтой. Инженерийн шийдэл - Зам барилга, усны менежмент зэрэгт DEM нь хамгийн оновчтой сонголт болдог. DEM нь нарийвчлал, хэрэглээний цар хүрээ, боловсруулалтын үр ашиг зэрэг үзүүлэлтүүдээр CSV өгөгдөл, контурын зураглалаас илүү. Энэ нь газрын гадаргын үнэн зөв загвар гаргаж, шинжилгээ хийхэд хамгийн тохиромжтой сонголт юм.

D. Civil 3d программ дээр зураг төсөл боловсруулах, тоо хэмжээ болон үнийн дүнгийн хувьд харьцуулах

LIDAR болон Аэрофотограмметр аргуудаар хийсэн 2 өөр DEM гадрага дээр ижил трасс татаж газар шорооны ажлын тоо хэмжээг бодож Civil 3D программ дээр зураг төсөл боловсруулаж харьцуулая.

1) Civil 3D программ зураг төсөл боловсруулах:

Civil 3D дээр "Alignment" функц ашиглан замын голч шугамыг татна. Трассыг аль аль DEM гадаргуу дээр ижил хэмжээсээр (өндөр, өргөн, налууугийн стандарт) байршуулна.

2) Тоо хэмжээ харьцуулалт

LiDAR ашиглан хийсэн хэмжилтэн дээр тулгуурлан Civil 3D программ дээр газар шорооны ажлын тоо хэмжээ бодуулахад ухмал байгуулах ажил нь 92709.31м3 , далан байгуулах ажил нь 54663.34м3 гарж байна. Аэрофотограмметр ашиглан хийсэн хэмжилтэн дээр тулгуурлан Civil 3D программ дээр газар шорооны ажлын тоо хэмжээ бодуулахад ухмал байгуулах ажил нь 99617.37м3 , далан байгуулах ажил нь 52030.68м3 гарж байна.

3) Үнийн дүнгийн харьцуулалт

Тухайн хоёр ажил дээр тусад нь “Estimator pro” программ дээр бодож үнийн дүнгийн хувьд харьцуулав.

Үнийн дүнгийн хувьд LiDAR болон Аэрофотограмметр өгөгдөл дээр боловсруулсан зураг төсвийн үнийн харьцуулалт

Хэмжилтийн хэлбэр	Үнийн дүн, төгрөг
LiDAR	4,129,458,018
Аэрофотограмметр	3,936,409,485
Зөрүү	193,048,533

Нийт үнийн дүнгээр сонгож авсан 4.5км замын хувьд “Estimator pro” программ дээр зөрүү үнийн дүн

193,048,533 төгрөгөөр Lidar-аар хийсэн хэмжилт үнийн дүнгийн хувьд бага гарж байна. GPS болон LiDAR ашиглан хэмжсэн хэмжилтийн харьцуулалт

GPS болон LiDAR ашиглан хийгдсэн хэмжилтүүдийг хугацаа, хүн хүч, болон зардлын хувьд харьцуулж үзэхэд дараах үр дүн гарсан байна. Эдгээр үр дүн нь хэмжилтийн технологийн онцлог, үр ашигт байдлыг тодорхойлж, цаашид аливаа төсөлд сонголт хийхэд чухал мэдээлэл болно.

#### 4) Хугацааны харьцуулалт

- GPS хэмжилт: 21 хоног зарцуулсан. Үүнд хэмжилт, боловсруулалтын бүх үе шат багтсан.
- LiDAR хэмжилт: 12 хоног зарцуулсан. Хугацааны хувьд 1.75 дахин бага хугацаа шаардсан.

LiDAR технологи нь илүү өргөн талбайг богино хугацаанд өндөр нарийвчлалтай хэмжих чадвартай. GPS-ийн хувьд олон цэгт тус бүр хэмжилт хийх шаардлагатай бол LiDAR нь цэгэн өгөгдлийг өндөр хурдтай цуглуулдаг.

#### 5) Хүн хүчний харьцуулалт

- GPS хэмжилт: Нийт 8 хүний баг ажилласан.
- LiDAR хэмжилт: Нийт 3 хүний баг ажилласан.

LiDAR хэмжилт нь хүн хүчний хувьд 2.6 дахин бага нөөц шаардсан.

LiDAR систем нь автоматжуулсан процессуудыг ашигладаг тул цэг суулгах, хэмжилт хийх зэрэг ажлуудад багийн оролцоо бага шаардлагатай. Харин GPS-ийн хэмжилтэд олон хүн оролцож, хэмжилт хийх процесс нь цаг хугацаа их зарцуулдаг.

#### 6) Санхүүгийн харьцуулалт

- GPS хэмжилт: Нийт 43.8 сая төгрөгийн зардал гарсан.
- LiDAR хэмжилт: Нийт 10.5 сая төгрөгийн зардал гарсан.

LiDAR хэмжилт нь 4.1 дахин бага зардалтай.

GPS хэмжилтэд олон тооны хүн, машин, тоног төхөөрөмж шаардлагатай бол LiDAR хэмжилт нь тоног төхөөрөмжийн өндөр хүчин чадалд тулгуурлан ажлын хугацааг багасгаж, зардлыг хэмнэж чаддаг.

GPS хэмжилтийн цэг бүрийг биеллэн хэмжих шаардлагатай байдаг бол LiDAR нь өргөн талбайг нэг дор хэмжиж, боловсруулах ажлыг автоматжуулдаг.

#### 7) Өргөн талбайн өгөгдлийн харьцуулалт

- GPS: 100 м өргөн зурвасыг хамарсан.
- LiDAR: 200 м өргөн зурвасыг хамарсан.

LiDAR нь GPS-ээс 2 дахин өргөн талбайн өгөгдлийг нэг хэмжилтээр бүртгэсэн.

LiDAR системийн өндөр хүчин чадал нь илүү өргөн зурвасыг хэмжих боломж олгодог. Энэ нь GPS-тэй харьцуулахад талбайн хэмжээ, өгөгдлийн цар хүрээний хувьд давуу талтай.

#### 8) Харьцуулалт:

GPS ашиглан хэмжсэн хэмжилт Завхан, Говь-Алтай аймгуудын нутагт явагдсан бөгөөд нийт 50км замыг 2ш машин, 6ш GPS, 8 хүний баг нийт 13 өдрийн дотор хэмжив. Мөн ирсний дараа хэмжилт боловсруулалтын ажлыг 3 компьютер ашиглан 8 хоногт хийж нийт 21 хонгийг зарцуулж хэмжилтэнд 43сая 800мянган төгрөг зарцуулав.

Эндээс хархад LiDAR ашиглан хэмжсэн хэмжилт нь GPS ашиглан хэмжсэн хэмжилтээс зурвасын хувьд 2 дахин их, хоног хугацааны 1.75 дахин бага хугацаа, хүн хүчний хувьд 2.6 дахин бага, хөрөнгө санхүүгийн хувьд 4.1 дахин бага мөнгө зарцуулав.

### ДҮГНЭЛТ

Агаарын LiDAR технологи нь дрон дээр суурилуулсан лазерийн сканнер, GPS, инерцийн хэмжилтийн нэгж (IMU) зэргийг ашиглан газрын гадаргыг өндөр нарийвчлалтайгаар хэмжихэд ашиглагддаг. Энэ арга нь их хэмжээний мэдээллийг хурдан хугацаанд цуглуулах, нарийвчлал сайтай загвар гаргах боломжийг олгодог.

Авто зам, замын байгууламжийн ажлын зураг төсөл боловсруулах ажлын геодезийн хэмжилт, зураглалыг авто замын трассын дагуу Хятад улсад үйлдвэрлэсэн DJI фирмийн M350 RTK дроноор 14125707м<sup>2</sup> талбайд хийж гүйцэтгэсэн. Энэхүү агаарын зураг авалтын ажилд DJI фирмийн өндөр нарийвчлалын DJI Zenmuse L2 лидар камерыг ашигласан.

Civil 3D программ дээр гадарга үүсгэхэд DEM, CSV, болон Контурын өгөгдөл зэрэг нь чухал үүрэг гүйцэтгэдэг. Эдгээр үүсгэсэн гадаргуудыг зэрэгцүүлж газрын гадаргууг зөв дүрсэлсэн байдлаар, өнгөний өөрчлөлт болон үүссэн хаялбарын өөрчлөлтөөр харьцуулав.

DEM нь нарийвчлал, хэрэглээний цар хүрээ, боловсруулалтын үр ашиг зэрэг үзүүлэлтүүдээр CSV өгөгдөл, контурын зураглалаас илүү. Энэ нь газрын гадаргын үнэн зөв загвар гаргаж, шинжилгээ хийхэд хамгийн тохиромжтой сонголт юм. DEM газрын гадаргыг сонгон ашиглахдаа өмнө нь судлагдсан байдалуудыг [5,6,7] болон бусад үзүүлэлтүүдийг үндэслэн сонгов.

LiDAR болон Аэрофотограмметр аргуудаар хийсэн 2 өөр DEM гадрага дээр ижил трасс татаж газар шорооны ажлын тоо хэмжээг бодож Civil 3D

программ дээр зураг төсөл боловсруулаж харьцуулан сонгов.

LiDAR ашиглан хийсэн хэмжилтэн дээр тулгуурлан Civil 3D программ дээр газар шорооны ажлын тоо хэмжээ бодуулахад ухмал байгуулах ажил нь  $92709.31\text{м}^3$ , далан байгуулах ажил нь  $54663.34\text{м}^3$  гарж байна. Аэрофотограмметр ашиглан хийсэн хэмжилтэн дээр тулгуурлан Civil 3D программ дээр газар шорооны ажлын тоо хэмжээ бодуулахад ухмал байгуулах ажил нь  $99617.37\text{м}^3$ , далан байгуулах ажил нь  $52030.68\text{м}^3$  гарж байна. 2 гадарга дээрх автозамын нийт ухмалын ажлын зөрүү  $6908.06\text{м}^3$  далангын ажлын тоо хэмжээ зөрүү  $-2632.66\text{м}^3$  гарав. Нийт үнийн дүнгээр сонгож авсан 4.5км замын хувьд "Estimator pro" программ дээр зөрүү үнийн дүн 193,048,533 төгрөгөөр LiDAR-аар хийсэн хэмжилт үнийн дүнгийн хувьд бага гарж байна.

LiDAR-ийн өгөгдлийг боловсруулан автозамын зураг төсөл боловсруулах схем байгуулав.

LiDAR ашиглан хэмжсэн хэмжилт нь GPS ашиглан хэмжсэн хэмжилтээс зурвасын хувьд 2 дахин их, хоног хугацааны 1.75 дахин бага хугацаа, хүн хүчний хувьд 2.6 дахин бага, хөрөнгө санхүүгийн хувьд 4.1 дахин бага мөнгө зарцуулав.

#### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] ЗЗБНБД 22-004-2016 "Авто зам төсөллөх"
- [2] Шинжлэх Ухаан, Технологийн Номын Сангийн вэб сайт
- [3] DJI Terra Overview-Хэрэглэгчийн гарын авлага, DJI Terra-ийн функцуудыг видео хичээл хэлбэрээр суралцахыг хүсвэл DJI-ийн YouTube сувар
- [4] Civil 3D Documentation-Хэрэглэгчийн гарын авлага, Civil 3D Tutorials -Youtube сувар
- [5] Э.Мөнх-Эрдэнэ нь 2023 онд "Үйлчилгээний зориулалттай автомат роботын системийн судалгаа, удирдлагын системийн хөгжүүлэлт" магистрын бүтээл
- [6] Д.Болортулга нь 2019 онд "LiDAR-ийн төхөөрөмжийг ашиглан зураглал үйлдэх" магистрын бүтээл
- [7] "Low-Cost UAV and GIS-Based Spatial Analysis for Cadastral and Construction Mapping." Зохиогч: Паул Сестрас. Хэвлэгдсэн огноо: 2020 он.
- [8] "Modeling and Analyzing Road Surfaces Using LiDAR Data." Зохиогчид: Ди Бенедетто А., Фиани М., Петти Л., Репетто Е. Хэвлэгдсэн огноо: 2023 он.
- [9] "Assessing Forest Canopy Structures Using LiDAR-Derived DEMs." Зохиогчид: Дэвид Ким, Лиза Чен. Хэвлэгдсэн огноо: 2020 он.
- [10] "High-Resolution Digital Elevation Models (DEMs) from LiDAR Data: Applications and Challenges." Зохиогчид: Жон Смит, Сара Жонсон. Хэвлэгдсэн огноо: 2022 он.
- [11] "LiDAR-Based DEMs for Urban Planning: Enhancing Accuracy in Topographic Mapping." Зохиогчид: Анна Петрова, Майкл Ли. Хэвлэгдсэн огноо: 2021 он.
- [12] "A Novel Approach for Creating Digital Terrain Models (DTMs) from LiDAR Data." Зохиогчид: Wioleta Błaszczyk-Bak, Artur Janowski. Хэвлэгдсэн огноо: 2022 он.
- [13] "Remote Sensing Platforms and Sensors: A Survey." Зохиогчид: С. Toth, G. Józkow. Хэвлэгдсэн огноо: 2016 он.
- [14] "Topographic Laser Ranging and Scanning: Principles and Processing." Зохиогчид: J. Shan, С. Toth. Хэвлэгдсэн огноо: 2018 он.
- [15] "Airborne Laser Scanning: Basic Relations and Formulas." Зохиогч: E. Baltsavias. Хэвлэгдсэн огноо: 1999 он.
- [16] "Photogrammetry: Geometry from Images and Laser Scans." Зохиогч: К. Kraus. Хэвлэгдсэн огноо: 2007 он.
- [17] "A Comparison of DEM Derived from LiDAR Data and Photogrammetry." Зохиогчид: К. Zhang нар. Хэвлэгдсэн огноо: 2003 он.
- [18] "Open Source 3D Point Cloud and Mesh Processing Software." Зохиогч: CloudCompare баг. Хэвлэгдсэн огноо: 2023 он.
- [19] "ArcGIS Pro: Surface Analysis Tools." Зохиогчид: ESRI баг. Хэвлэгдсэн огноо: 2023 он.
- [20] "Effects of LiDAR Post-Spacing and DEM Resolution to Mean Slope Estimation." Зохиогчид: Т. Е. Chow, М. Е. Hodgson. Хэвлэгдсэн огноо: 2009 он.
- [21] "DEM Generation from Laser Scanner Data Using Adaptive TIN Models." Зохиогч: Р. Axelsson. Хэвлэгдсэн огноо: 2000 он.
- [22] GPS-ийн технологи ашигласан байр зүйн судалгааны тайлан (2024). Завхан, Говь-Алтай аймгуудад хийгдсэн.
- [23] LiDAR хэмжилтийн тайлан (2024). Дорноговь аймгийн нутагт хийгдсэн.
- [24] "Photogrammetry Software for Aerial Surveying." Зохиогчид: DJI Terra баг. Хэвлэгдсэн огноо: 2023 он.
- [25] "Infrastructure Design Software." Зохиогчид: AutoCAD Civil 3D баг. Хэвлэгдсэн огноо: 2023 он.
- [26] "Accuracy Assessment of LiDAR and Photogrammetry in DEM Generation." Зохиогчид: F. Khosrowshahi, Н. Mazaheri. Хэвлэгдсэн огноо: 2020 он.
- [27] "LiDAR Remote Sensing of Forest Canopy Structure and Ground Elevation." Зохиогчид: F. Morsdorf нар. Хэвлэгдсэн огноо: 2004 он.
- [28] CatalogChatGPT, OpenAI (2024), Youtube, Wikipedia, Google

## ЛАБОРАТОРИЙН ТУРШИЛТЫН ЗУРГАН ӨГӨГДЛИЙН БОЛОВСРУУЛАЛТ

Батзоригийн ТҮВШИНТӨГС<sup>1</sup>, Доржсүрэнгийн ТЭМҮҮЛЭН<sup>2</sup>, Ишдоржийн ЦЭРЭН-ОНОЛТ<sup>1</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын Ухааны Салбар

<sup>2</sup>Монгол улс, АШУҮИС, Био анагаах ухааны сургууль, Биологийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: tseren-onolt@must.edu.mn<sup>1\*</sup>

**Хураангуй:** Энэхүү судалгааны ажлын зорилго нь эмнэлгийн судалгааны лабораторид зориулагдсан, зургийг тэмдэглэн, гүн сургалтын Faster R-CNN загварыг ашиглан судалгааны тусгай сэдвүүдэд тохируулан загвар боловсруулах платформ бүтээх явдал юм. Сүүлийн үед гүн сургалт нь олон салбарт өргөн ашиглагдаж байгаа бөгөөд үүнийг дагаад мэргэжлийн биш хүмүүс ч зурган өгөгдлийг ашиглан загвар боловсруулж, судалгаандаа хэрэглэх боломжийг олгох орчныг бүрдүүлэхэд анхаарч байна. Эхний үе шатанд бид УНТЭ-ийн ерөнхий мэс заслын тасагт бэтэг өвчний улмаас мэс заслын эмчилгээнд хамрагдсан үйлчлүүлэгчийн Cystic Echinococcosis[3] буюу бэтгийн туузан хорхойн 100 орчим протосколексийн зургийг data augmentation хийн олшруулан баталгаажуулалтыг хийж байна. Энэхүү платформ нь судлаачдад өөрсдөө зургийг тэмдэглэн, тусгай сэдэвт зориулсан загваруудыг үр дүнтэй, уян хатан байдлаар хөгжүүлэх боломжийг олгох бөгөөд эмнэлгийн дүрс оношлогооны салбарт шинэ боломжуудыг нээх зорилготой юм.

Түлхүүр үг: *Faster R-CNN, Data preprocessing, Object detection platform*

### I. УДИРТГАЛ

Сүүлийн жилүүдэд дижитал технологи болон машин сургалтын хөгжил нь эрүүл мэндийн салбарын судалгаа, шинжилгээнд томоохон үр дүнгүүдийг авчрахад түлхэц үзүүлж байна. Машин сургалт, гүн сургалтын загварууд нь олон төрлийн эмнэл зүйн үзүүлэлтийг илүү нарийвчлан тодорхойлох, шинжилгээний үр дүнг үнэн зөвөөр дүгнэх, эмчилгээний аргуудыг сайжруулахад ашиглагдаж байгаа нь эмнэл зүйн чадамжийг сайжруулж байна. Энэхүү судалгаагаар бид эрүүл мэндийн судалгаанд зориулсан өвчтөний болон лабораторийн туршилтын зураг дээрх таних объектыг шошгожуулан тэмдэглэх, хиймэл оюуны загвараар сургах платформ бүтээх юм.

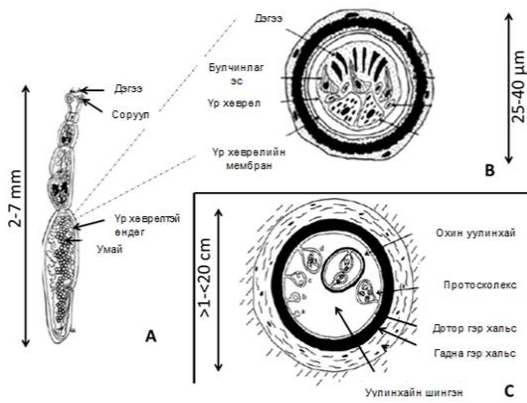
Энэхүү системийн гол онцлог нь эмч, судлаачид өөрсдөө лабораторийн зурган өгөгдлийг ашиглан гүн сургалтын загваруудыг хялбархан хөгжүүлэх боломжийг бий болгох зорилготой. Үүний үр дүнд нарийн мэргэжлийн эмч мэргэжилтэн хэрэгтэй оношилгоог шуурхай хийн ажлын үр дүнг сайжруулах, шимэгч хорхойн эсрэг эмийн судалгаа зэрэгт тухайн сэдэвт тохирсон гүн сургалтын загваруудыг бүтээж, туршин судалгааг илүү бодитой, үр дүнтэй хялбараар хийх зэрэг нэмэлт боломжуудыг бий болгож чадна.

### II. БЭТЭГ ӨВЧНИЙ ТАЛААР

Хөгжүүлэлтэд ашиглаж байгаа бэтэг (*Echinococcus*)-ийн туузан хорхой нь нохой, чоно, үнэг зэрэг махчин амьтдын нарийн гэдсэнд бие гүйцсэн байдлаар шимэгчилж, ялгадсаар нь өндгөө гадаад орчинд байнга гадагшлуулдаг. Иймд мэрэгч, хивэгч амьтад болон хүн *Echinococcus*-ын өндгийг залгисан тохиолдолд

авгалдаг тээн, “Уйланхайтах бэтэг” буюу *Cystic Echinococcosis* хэмээх өвчтэй болдог. Монгол улс *Cystic Echinococcosis* тархалт өндөртэй эндемик орон бөгөөд энэхүү өвчин нийгэм, эдийн засагт асар их хор хөнөөл учруулдаг.[1]

Манай улсын хүн ам болон мал, амьтдын дунд *Echinococcus granulosus*, *Echinococcus canadensis Echinococcus multilocularis* гэсэн 3 зүйл байгалийн бүсээс хамааралгүй тархжээ. Эхинококкийн бие гүйцсэн хэлбэр нь 3-4 үеэс тогтсон, 2-7мм урттай, толгой дээрээ соруулаас гадна 2 эгнээ гох дэгээтэй. Толгойн араас хүзүү, дараа нь хос бэлэгтэй үе залгах бөгөөд үений бэлгийн сүвүүд тэдгээрийн баруун, зүүн талд байрладаг. Хорхойн их биений төгсгөлийн үеийг бие гүйцсэн үе гэх бөгөөд онкосфер хөгжсөн 5000 орчим өндөг агуулсан байдаг (1-р зураг А). Эхинококкийн өндөг нь 30-40 мкм диаметртэй, дугариг хэлбэртэй, 3-4 давхар бүрхүүлтэй, дотор нь хос дэгээ бүхий үр хөврөл хөгжиж эхэлдэг (1-р зураг В) ба тенийдийн овгийн бусад туузан хорхойнуудаас өндгөөр ялгаварлан оношлох боломжгүй. Эхинококкийн өндөг гадаад орчинд буюу халуун, хүйтэн температурт маш тэсвэртэй бөгөөд -18°C-д 240 хоног, -27°C-д 54 хоног хүртэл амьд байдаг. Мөн +4°C-ийн усанд 16 сар хүртэл амьдрах чадвартай. Эхинококкийн өндгийг 0°C-д 116 хоногийн турш үхэлгүй хадгалагдаж байжээ. А.Ф.Носикийн судалгаагаар (1950,1951) сүүдэртэй газрын хөрсөн дээр 10-26°C-д 1 сарын турш, өвсөн дотор 2-20°C-д 6 сар хүртэл халдварлах чадвартай хэвээрээ байсан ба 50°C-ийн усанд 1 цаг, 60°C-д 10 минут, 100°C-д нэг секундийн дараа тус тус үхэж байжээ. Тасалгааны чийглэг 60-80%, температур 5-20°C байхад 10-12 сар, 18-50°C-ийн хуурай халуунд 1-2 хоног, тундрт үхээд цасанд булагдсан үнэгний сэгэнд хэдэн сарын турш халдварлах чадалтай хэвээрээ байсан байна. [1]



1-р зураг. А. Бие гүйцсэн Эхинококкийн диаграмм, В. Эхинококкийн өндөгний диаграмм, С. Эхинококкийн авгалдай болох уйланхайн диаграмм

Хүн амын нэлээд хувь нь мал аж ахуй эрхэлдэг манай оронд бэтэг өвчин түгээмэл байгаа ба шимэгчээр үүсдэг өвчнүүдийн дотроос бэтэг өвчин нь удаан явцтай эмнэлзүй шинж тэмдэг тод илрэхгүй улмаас оношлох эмчлэхэд бэрхшээлтэй өвчин юм.

### III. ӨГӨГДӨЛ, ӨГӨГДӨЛ БЭЛТГЭХ

#### A. Өгөгдөл цуглуулах

Гүн сургалт ашиглаж бодит таамаглал гаргах загвар сургахад өгөгдлийн тоо ширхэг болон үнэн зөв байдал хамгийн чухал байдаг.

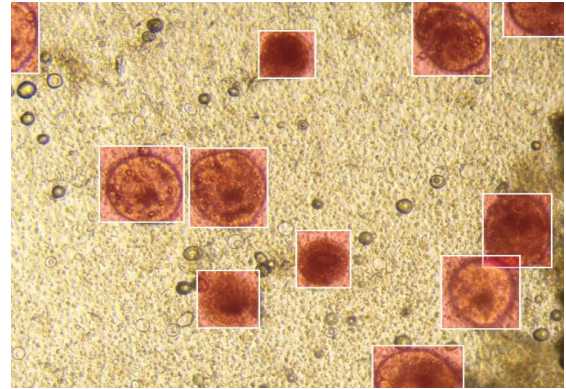
Хөгжүүлэлтэд зургууд нь Эхинококкийн авгалдайг (1-р зураг С) лабораторийн нөхцөлд өсгөвөрлөн эмийн туршилт хийх явцад цуглуулсан зургууд болно.

#### B. Өгөгдөл бэлтгэх

Бидний цуглуулсан өгөгдлүүд нь бүгд png болон bmp өргөтгөлтэй лабораторийн microscope-оор авсан өндөр нягшилтай зургууд бөгөөд эхинококкийн авгалдайг лабораторийн нөхцөлд өсгөвөрлөн эмийн туршилт хийх явцад цуглуулсан. Өөрөөр хэлбэл зургуудад бусад бичил биетэн байхгүй учраас өөрсдөө тэмдэглэгээг хийсэн /data labeling/. (2-р зураг)

#### C. Өгөгдөл тэмдэглэгээ

Энэхүү ажлын хүрээнд хийгдэж байгаа платформыг ашиглан өгөгдлийн тэмдэглэгээг гүйцэтгэсэн. Цуглуулсан өгөгдөл нь нэг л төрлийн тэмдэглэгээ хийх зорилготой учраас эхинококкийн авгалдайг бүх зурган дээр тэмдэглэн платформын өгөгдлийн санд хадгалсан.



2-р зураг. Эхинококкийн авгалдайн тэмдэглэгээ

### IV. ПЛАТФОРМЫН ТАЙЛБАР

#### A. Ерөнхий загвар

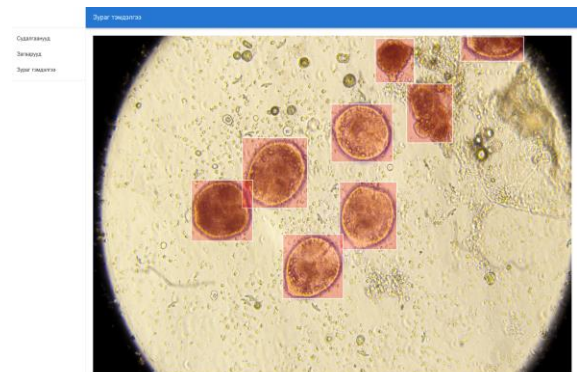
Frontend, Backend, Model, Database гэсэн хэсгүүдээс бүрдэх ба бүртгэлтэй хэрэглэгчид нь системд нэвтрэн дараах үйлдлүүдийг хийх боломжтой байна (3-р зураг).

- Зургийн тэмдэглэгээ хийх болон засах
- Тэмдэглэгээ хийсэн өгөгдлийг augmentation хийх
- Тэмдэглэгээ хийсэн өгөгдлийг ашиглан загвар сургах
- Сургасан загварыг хэрэглэн зураг дээрээс тухайн загварын таниж чадах бичил биетийг илрүүлэх болон үр дүнг засварлах
- Туршилтад зориулан тухайн туршилтад ашиглах template-г бэлтгэх

#### C. Tech stack

Цаашдын хөгжлүүлэлт болон тасралтгүй, аюулгүй үйл ажиллагааг хангах зорилгоор сүүлийн үеийн технологиудыг ашигласан.

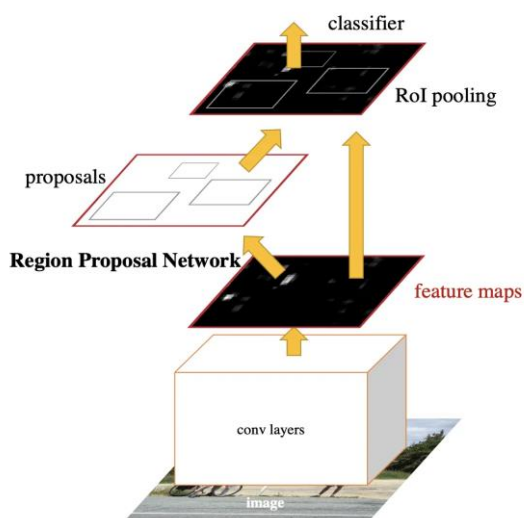
- asdf/npm/poetry
- Typescript/React
- Python/Fastapi
- PostgreSQL/Alembic
- Pytorch
- Faster R-CNN



3-р зураг. Frontend-ийн харагдах байдал

#### D. Faster R-CNN

Faster Region-based Convolutional Neural Network (Faster R-CNN) нь зурган өгөгдлөөс магадлалт хэсгүүд буюу Region Proposal Network (RPN)-г сонгон тухайн хэсгүүдэд Convolutional Neural Network (CNN)-г ашиглан гүнзгийрүүлэн боловсруулж онцлог шинж чанаруудыг гарган авдаг. Тухайн онцлог шинж чанаруудыг ашиглан объект танилтыг гүйцэтгэдэг ба R-CNN болон Fast R-CNN-н сайжруулсан загвар юм (5-р зураг).



5-р зураг. Faster R-CNN-н бүтэц [2]

#### ДҮГНЭЛТ

Уг платформыг ашигласнаар нарийн мэргэжлийн судлаачид өөрсдөө, өөрсдийн бэлдсэн өгөгдөл дээр хурдан шуурхай цаг алдалгүйгээр загвар сургах боломжтой болсноор судалгааны явцад гүн сургалтын загварыг хэрэглэх боломжтой болоод зогсохгүй бусдын сургасан загвар дээр суурилсан дараа дараагийн судалгаа туршилтыг хийх боломжтой болно. Цаашилбал эмч судлаачдын ажлын бүтээмж өндөрснөөр эрүүл мэндийн салбарт тулгамдаад байгаа боловсон хүчний асуудалд мөн хувь нэмэр оруулж чадах болно.

#### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Мал эмнэлгийн ерөнхий газрын даргын 2018 оны А/64 дугаар тушаалын нэгдүгээр хавсралт МАЛ, АМЬТНЫ БЭТЭГ ӨВЧНӨӨС УРЬДЧИЛАН СЭРГИЙЛЭХ, ТЭМЦЭХ ЗААВАР
- [2] Shaoqing Ren, Kaiming He, Ross Girshik, Jian Sun, Faster R-CNN: Toward Real-Time Object Detection with Region Proposal Networks, <https://arxiv.org/abs/1506.01497v3>
- [3] Velasco-Tirado, V., Alonso-Sardón, M., Lopez-Bernus, A. et al. Medical treatment of cystic echinococcosis: systematic review and meta-analysis. *BMC Infect Dis* **18**, 306 (2018). <https://doi.org/10.1186/s12879-018-3201-y>

## НР/ЛР НЕЙРОНТ ЗАГВАРААР ЕВКЛИДИЙН ЗАЙГ ОЙРОЛЦООГООР ТООЦООЛОХ

Зандраабазарын ЦЭНД<sup>1</sup>, Ишдоржийн ЦЭРЭН-ОНОЛТ<sup>2</sup> Ганбаатарын ГАНБАТ<sup>3</sup> Агвааны ОТГОНБАЯР<sup>4</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын Ухааны Салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: tseren-onolt@must.edu.mn<sup>1\*</sup>*

**Хураангуй:** Энэхүү судалгаа нь Евклидийн зай болон комплекс тооны L2-нормыг хурдан ойролцоогоор тооцоолох аргыг судалсан. Энэхүү тооцоолол нь дүрс боловсруулах, дижитал дохионы боловсруулалт болон криптографид өргөн хэрэглэгддэг. Үндсэн зорилго нь хамгийн бага хүчин чармайлтаар хамгийн өндөр тоон нарийвчлалтай анхны хэмжилтэд хүрэх явдал юм. Бид квадрат язгуур гаргах тооцооллыг арилгаж, зөвхөн цөөн хэдэн шилжилт, нэмэх үйлдэл ашиглан ойролцооллын нарийвчлалыг 41 %-иас 4 % болгон сайжруулж буйг батлан харуулсан. Энэ нь нарийвчлалыг 1 битээс бараг 5 бит хүртэл сайжруулсантай тэнцэнэ. Дараалсан Ньютоны давталтууд нь битийн тоог хоёр дахин нэмэгдүүлдэг тул эхний хоёр давталт шаардлагагүй болдог. Жишээлбэл, 16-битийн нарийвчлал бүхий үр дүнг ердөө хоёр давталтаар, дөрвөн давталт шаардалгүйгээр гаргаж болно. Бид энэхүү тооцооллыг НР/ЛР нейронуудыг ашиглан мембран тооцоолол зэрэг био-үүдэлтэй тооцооллын хүрээнд хэрэгжүүлсэн.

**Түлхүүр үг:** НР/ЛР нейронууд, Евклидийн зай, Спайк нейрон Пи систем, MUST-Adder, MUST- Euclidean

### I. УДИРТГАЛ

Энэхүү судалгааны зорилго нь  $\sqrt{x^2 + y^2}$  -ыг ойролцоолох буюу Евклидийн зай эсвэл L2-нормыг тооцоолоход оршино. Энэ тооцоолол нь Картезийн координатыг туйлын координат руу хөрвүүлэхэд шаардлагатай бөгөөд олон төрлийн хэрэглээтэй [3].

Гэвч квадрат язгуурыг тооцоолох нь их өртөгтэй. Мембран тооцоололд НР/ЛР-нейрон (НР нь High-Pass буюу өндөр давтамж дамжуулагч, ЛР нь Low-Pass буюу нам давтамж дамжуулагч) ашиглан квадрат язгуур тооцоолох төхөөрөмж одоогоор бидэнд байхгүй юм [20]. Харин бидэнд өмнөх [18] судалгаанд танилцуулагдсан MUST-Adder байгаа бөгөөд үүнийг энэ тооцоололд ашиглах боломжтой. Сүүлийн хэдэн арван жилд цахиур түүхий эдийн электрон төхөөрөмжүүд нь Мурын хуулийн дагуу амжилттай загвар байсаар ирсэн. Гэвч Мурын хуулийн хэрэгжилтийн хугацаа дуусах дөхөж байгаа тул бид тооцооллын шинэ парадигмыг эрэлхийлж байна. Энэ үүднээс мембран тооцоолол дээр суурилсан био/нейрон үүдэлтэй тооцооллыг [1,15–17,21] шинэ парадигм [19] болгон авч үзэж байна. Мембран тооцооллын нэг төрөл болох Спайк нейрон Пи системүүд [7] нь нейрон эсүүдээс үүдэлтэй бөгөөд эдгээрийг электрон төхөөрөмж, мөн микро шингэний төхөөрөмжүүд зэрэг бусад системүүдэд хэрэгжүүлж болно.

Манай судалгаа нь Хи болон түүний хамтрагчдын [25] бодит судалгаанд тулгуурласан ба энэ нь НР болон ЛР гэсэн хоёр үндсэн нейрон төрлийг ашиглан дурын Спайк Нейрон Пи системийг хэрэгжүүлэх аргыг санал болгодог. Мөн энэ судалгаа нь эдгээр нейронуудыг CMOS логикт хэрэгжүүлэх аргыг танилцуулсан. Гэхдээ энэ хандлага нь ерөнхий тохиолдлынх тул олон төрлийн өөр өөр түүхий эд дээр хэрэгжүүлэх ч боломжтой юм. Гиймээс био-нано технологи [13] болон микро-шингэн био-чип технологи [11]-д суурилсан. Пи системүүдийн

хэрэгжүүлэлтийн талаар цөөн хэдэн судалгааны ажил одоогоор танилцуулагдаад байна.

#### A. Спайк Нейрон (СН) Пи систем

Спайк нейрон Пи систем нь мембран системийн нэг төрөл бөгөөд [19, 20] нейроны нейрофизиологийн үйл ажиллагаанд үндэслэсэн байдаг [7]. Спайк нейрон Пи системд боловсруулалтын элементүүд нь нейронууд бөгөөд эдгээр нь синапсын граф гэж нэрлэгдэх чиглэлтэй графаар холбогддог. Спайк нейрон Пи систем нь зөвхөн цочрол (spike)-той ажилладаг бөгөөд бүх цочрол нь ижил байдаг ч тооцооллын хүндрэлийг шийдвэрлэх, мөн комбинаторик оновчлолын асуудлуудыг [9, 14] үр дүнтэйгээр шийдэх боломжтой тооцооллын систем юм [26]. Энэ хэсэгт Спайк нейроны үндсэн дүрмийг математикийн аргаар тайлбарлах болно. Спайк нейрон Пи системд нейрон эсүүд (нейронууд гэж нэрлэдэг) чиглэлтэй графын зангилаануудад байрладаг. Нейрон бүрийн агуулга нь цөөн тооны цочрол хэмээх ижил төрлийн объектууд болон тодорхой цочрол үүсгэх ба мартах дүрмүүдээс бүрдэнэ. Цочрол үүсгэх дүрэм нь нейронд бусад нейрон руу дохио (цахилгаан импульс) илгээж мэдээлэл дамжуулах боломжийг олгодог бөгөөд энэ нь очих эсүүд дээр хуримтлагдана. Дүрмийн хэрэглэгдэх эсэх нь нейрон дахь агуулгыг дүрэмтэй холбоотой өгөгдсөн утгатай харьцуулж шалгагдсанаар тодорхойлогдоно. Хэрэв тодорхой нэг цаг хугацааны нэгжид нейрон хэд хэдэн дүрэм ашиглах боломжтой бол эдгээр дүрмийн нэгийг сонгох шаардлагатай бөгөөд тухайн дүрэм нь тодорхой бус байдлаар санамсаргүйгээр сонгогдоно. Дүрмүүдийг нейрон тус бүр дотор дараалалтайгаар ашигладаг ч олон нейронууд зэрэгцээ ажиллагаатай ажилладаг. Хэрэв цочрол үүсгэх дүрэм нейронд хэрэгжих боломжгүй бол урьдчилан тогтоосон тооны цочролыг устгах мартах дүрмийг ашиглах боломжтой. Ерөнхийдөө, Спайк нейрон Пи системд оролт авч, гаралт өгч чаддаг тооцооллын хувилбараар

тодорхойлсон  $m$ -ээс багагүй зэрэгтэй Спайк нейрон Пи системийг [6] дараах байдлаар илэрхийлнэ:

$$P = (O, \sigma_1, \sigma_2, \dots, \sigma, syn, in, out) \quad (1)$$

гэж өгөгдсөн бөгөөд

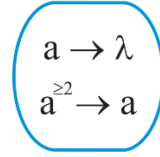
1.  $O = \{a\}$  нь үсэг бөгөөд ( $a$  нь цочрол гэж нэрлэгддэг);
2.  $\sigma_1, \sigma_2, \dots, \sigma$  нь нейронууд,
3.  $syn \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, m\}$ , нь  $1 \leq i \leq m$  үед  $(i, i) \notin syn$  байх нөхцөлтэйгээр нейронуудын хоорондын синапсуудын чиглэгдсэн графыг илэрхийлнэ;
4.  $in, out \in \{1, 2, \dots, m\}$  нь Пи -ийн оролт болон гаралт нейронуудыг тус тус илэрхийлнэ.

*Цочирлын дүрэм:*  $\frac{E}{a^c} \rightarrow a; d \in R_i$  нь  $\sigma_i$  нейронд дараах нөхцөл хангагдсан үед хэрэглэгдэх боломжтой:  $k \geq c$  цочрол агуулсан ба  $a^k \in L(E)$ . Энэ дүрмийг хэрэгжүүлэхэд  $\sigma_i$ -ээс  $c$  цочролыг авдаг (ингэснээр  $k-c$  цочрол үлдэнэ), ба  $\sigma_j$  нейрон бүр рүү цочролыг хүргэхэд бэлддэг, энд  $(i, j) \in syn$ . Хэрэв  $d = 0$  бол цочрол шууд дамжуулагдах бөгөөд эс тэгвээс системийн  $d$  тооны тооцооллын алхмын дараа дамжуулагдана. Дээр дурдсанаар, эдгээр  $d$  тооцооллын алхмуудын үед нейрон хаалттай байж, шинэ цочрол хүлээн авах боломжгүй (нейрон хаалттай нейрон руу синапсаар цочрол дамжуулахыг оролдвол тухайн цочрол алдагдана), мөн цочрол илгээж (эсвэл сонгож) чадахгүй.

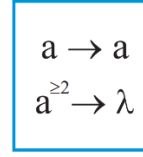
*Мартах дүрэм*  $a^s \rightarrow \lambda$ , нь  $\sigma_i$  нейронд яг цочрол агуулсан үед хэрэгжиж болох бөгөөд энэ дүрмийн хэрэгжилт нь зүгээр л  $\sigma_i$ -ээс бүх  $s$  цочролыг арилгах үйлдэл юм.

*Нейроны үндсэн төрлүүд:* Спайк нейрон Пи системд илэрхийлэл  $E$ -д хязгаарлалт байхгүй тул нейрон дахь дүрмүүдийг хослуулах боломж хязгааргүй байдаг бөгөөд энэ нь нейрон хэлхээг боловсруулахад төвөгтэй болгож болзошгүй юм. Ерөнхий Спайк нейрон Пи системд нейрон нь хэд хэдэн дүрэм агуулж болно [2]. Энэ судалгаанд өндөр дамжуулалтын (HP) нейрон болон бага дамжуулалтын (LP) нейрон гэсэн Спайк нейрон Пи нейроны хоёр үндсэн төрлийг [18] ашиглаж байна. Эдгээр нь харгалзах цочрол үүсгэх дүрмүүдээр тодорхойлогдоно. Энэ төрлийн нейронууд нь хязгааргүй тооны оролтыг хүлээн авч, зөвхөн нэг гаралт үүсгэдэг. Цочрол үүсгэх дүрмийн босго утга нь 2-оор тогтоогдсон: HP нейрон нь хоёр буюу түүнээс дээш оролтын цочрол хүлээн авахад цочрол үүсгэдэг бол LP нейрон нь зөвхөн нэг оролтын цочрол хүлээн авахад цочрол үүсгэнэ. Эдгээр тусгай төрлийн нейронуудыг ашиглаж байгаа тул бид ердийн илэрхийллийн оронд илүү тодорхой (босго

хэлбэрийн) бичиглэл ашиглана [2]. Энгийн болгох үүднээс HP болон LP нейронуудыг 1-р зурагт үзүүлсэн хэлбэрээр нь дүрсэлнэ.



(a) HP нейрон



(b) LP нейрон

*1-р зураг. HP нейрон болон LP нейрон нь үндсэн нейронууд юм. HP нейрон нь хоёр буюу түүнээс дээш цочрол хүлээн авбал цочрол үүсгэнэ, харин бусад тохиолдолд оролтын цочрол мартагдана. LP нейрон нь үүний эсрэгээр ажилладаг*

Спайк нейрон Пи системийг хэрэгжүүлэхэд эдгээр нейронуудын үүрэг нь Boolean логикийн NAND хаалтуудтай төстэй юм: Тэдгээр нь хамгийн хэмнэлттэй дизайныг санал болгодоггүй боловч илүү ерөнхий хэрэгжүүлэлтийн үндэс болж байна. Үнэндээ, HP болон LP нейронуудыг илүү нарийн төвөгтэй нейронуудыг дараах аргаар бүтээхэд ашиглаж болно. Нэг нейрон нь хэд хэдэн дүрэмтэй байх тохиолдолд, түүнийг хоёр дараалсан үе шатанд ажиллаж байгаа гэж үзэж болно: оролтын дохионуудыг тоолох, дараа нь ямар дүрмийг хэрэглэхээ шийдэх (бид эдгээр хоёр үе шатыг тоолох ба шийдвэрлэх үе шат гэж нэрлэсэн). HP болон LP нейронуудыг ашиглан илүү нарийн төвөгтэй нейроныг хэрэгжүүлэхийн тулд эдгээр хоёр үе шатыг тусад нь авч үзсэн.

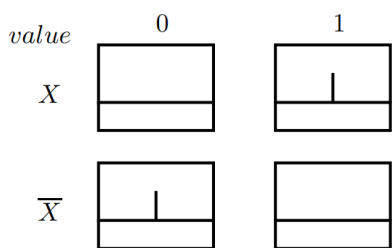
**В. LP болон HP Нейронуудын Электрон Субстратын Хэрэгжилт**

Стандарт CMOS логик болон нейрон системийн гол ялгаа нь CMOS логик нь 0 болон 1 гэсэн тогтвортой сигналын утгуудыг боловсруулдаг бол нейрон сүлжээнүүд нь түр зуурын цочролуудыг ашигладаг явдал юм. Эдгээр цочролууд заримдаа хоцрогдож эсвэл алдагдаж болох юм. Хи болон түүний хамтрагчдын хийсэн [25] хэрэгжилт нь дижитал системд домино логиктой холбоотой [12, 24]. Домино логик нь ихэвчлэн хос-замт логик (dual-rail logic) ашиглан хэрэгжүүлэгддэг [22].

**II. СУДАЛГААНЫ АРГАЗҮЙ**

Бид HP болон LP элементүүдийг ашиглан хоёртын бүтэн нэмэгч хэрэгжүүлсэн [25]. 2 оролттой HP нь AND үйлдлийг гүйцэтгэдэг бол 2 оролттой LP нь XOR үйлдлийг гүйцэтгэдэг. 1 оролттой LP нь хүлээлт (delay) болж ажилладаг. ( $\{0, 1\}$ , XOR, AND) нь хязгаарлагдмал талбай (finite field) юм. Домино логикийн хос-замт логикоос санаа авч, бид дохиог хос-замт логиктой үнэлэх арга барилаар ажиллахаар шийдсэн. Ийнхүү, дараа нь бид Хи болон түүний хамтрагчдын судалгаагаар тодорхойлсон [25] гол

алдаа загварыг спайк алдагдлыг амархан илрүүлж чадна гэдгийг харуулах болно. Өмнөх судалгаанд хэрэглэсэн нэгжийн тооны илэрхийлэл нь хоёр үндсэн сул талтай байсан. Нэгдүгээрт,  $X$  болон хамтран ажиллагчдын нэмэгчийн тусгай хэрэгжилтийн шинж чанараас шалтгаалан зөвхөн нэг тоо нь нэг байх тохиолдолд л тоонуудыг нэмэх боломжтой. Хоёрдугаарт, бид криптологи дахь хэрэглээ рүү чиглэж байгаа бөгөөд 2048-битийн RSA түлхүүрийг нэгжийн илэрхийллээр боловсруулах нь оновчтой бус юм. Тиймээс бид хоёртын тоон илэрхийллийг сонгосон.



2-р зураг. Дохионы дүрслэл

2-р зурагт Спайк нейрон Пи системүүдэд логик утгуудыг хэрхэн дүрсэлж буйг харуулсан. Бидэнд  $X$  гэсэн логик утга байгаа бөгөөд үүнийг  $X$  болон  $\bar{X}$  гэсэн хоёр дохиогоор дүрсэлдэг. Хэрэв  $X$  дохионы логик утга 1 байвал  $X$ -д цочрол байх ба  $\bar{X}$ -д дохио байхгүй байна. Харин эсрэгээрээ,  $X$  дохионы логик утга 0 байвал  $\bar{X}$ -д дохио байх ба  $X$ -д дохио байхгүй байна.

**III. ЕВКЛИДИЙН ЗАЙГ ХЭРЭГЖҮҮЛЭХ НЬ**

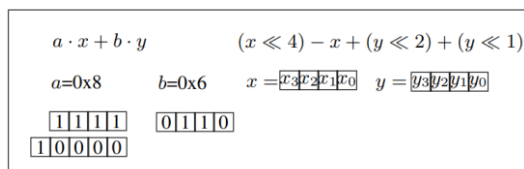
**A. Хэрэгжүүлэлтийн үндсэн зарчим**

Бид ойролцооллыг 4 битээр гүйцэтгэнэ. [23] -ийн дагуу, 1 хүснэгтэд параметрууд болох  $a$  болон  $b$  -г 4 битээр илэрхийлэх шаардлагатай.

**4 БИТ ХЭРЭГЖҮҮЛЭЛТ**

1-Р ХҮСНЭГТ

Параметр	Аравтын ойролцоолол	4 бит арван зургаатын тоолол	Хоёртын тоолол
$a$	0.96	0xf	1111
$b$	0.4	0x6	0110



3-р зураг. Дохионы дүрслэл

$x$  болон  $y$ -ийн бүх боломжит оролтын утгуудыг симуляц хийхэд, хамгийн их харьцангуй алдаа  $\epsilon = 7.19\%$  байгааг тогтоосон бөгөөд энэ нь үр дүнгийн нарийвчлалыг 3.80 бит хүргэж байна. Хамгийн их

алдааг үүсгэсэн оролтын утгууд нь  $x=0x1$  and  $y=0x1$ . Бидний зорилго бол  $a \cdot x + b \cdot y$ -г тооцоолох явдал юм.  $x$  болон  $y$  нь дурын утга байж болох бөгөөд  $x \geq y \geq 0$  нөхцлийг хангана.  $a$ -г хоёртын тоололд 1111,  $b$ -г хоёртын тоололд 0110 гэж өгсөн бөгөөд аль аль нь тогтмол утгууд юм. Туршилтын тохиолдол  $x = 0x1$  and  $y = 0x1$ : Векторын уртыг тооцоолно.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \sqrt{2} \approx 1.4142 \dots \quad (2)$$

Ойролцооллыг тооцоолбол доорх үр дүн гарсан

$$a \cdot x + b \cdot y = 0xf \cdot 0x1 + 0x6 \cdot 0x1 = 0x15 = 1.3125$$

Үүссэн утга 0x15 нь дөрөвдүгээр битэд хоёртын цэгтэй тогтмол цэгийн утга юм. Тиймээс, бодит утга нь  $0x1.5$  буюу  $\frac{0x15}{2^4}$  байна. Энэ нь аравтын тоогоор:  $1 + \frac{5}{16} = 1.3125$ .

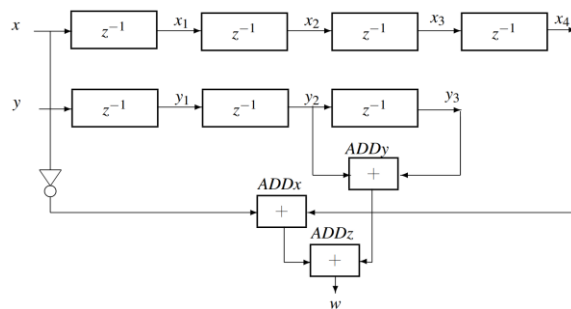
Үүнээс бид алдааг, өөрөөр хэлбэл харьцангуй алдаа  $\epsilon$ -г тооцоолж болно. Энэ нь:

$$\epsilon = \left| \frac{1.3125 - 1.4142}{1.4142} \right| = 7.1922 \%$$

Манай бүх боломжит оролтын утгуудыг хамарсан иж бүрэн симуляц нь энэ нь хамгийн муу тохиолдолд гарах алдаа болохыг харуулсан.

**B. Блок схем**

4-р зурагт шинэ MUST-Euclidean буюу musteuclid4 дизайныг харуулсан ба 4-битийн нарийвчлалтай. Бид хос-замт логикийг харж болно, учир нь логик утга бүр  $X$  нь өөрийн хэрэгжилтэндээ  $X$  болон  $\bar{X}$  гэсэн дохиотой байна. Жишээлбэл, оролтын  $A$  болон  $B$  битүүдийн урвуу  $\bar{A}$  болон  $\bar{B}$  нь байдлаар тус тусдаа байна.



4-р зураг. MUST-Euclidean сүлжээний жагсаалт

$x_4$ -ын доор байгаа сумыг нөгөө чиглэлд заах ёстой. Голд байрлах MUST-Adder (хамгийн зүүн талынх) хасагч байх шаардлагатай.

**C. Хэрэгжүүлэх стратеги**

$a$ -ын үржвэр. Бид  $x$  оролтыг тогтмол параметр  $a$ -аар үржүүлэх шаардлагатай. Үржүүлэгчийн өртөг өндөртэй байдаг тул [4], оронд нь шилжүүлэлт ба нэмэх үйлдлүүдийн хослолыг ашигладаг.  $x$ -ийг 4 битээр зүүн тийш шилжүүлнэ. Энэ нь 16-аар

үржүүлж буйтай адил. Дараа нь  $x$ -ийг хасна. Үр дүн нь 15-аар үржүүлсэнтэй тэнцүү болно

$$15 \cdot x = (16 - 1) \cdot x = 16 \cdot x - x = (x \ll 4) - x \quad (3)$$

MUST-Adder ашиглан хэрхэн хасах үйлдэл хийх вэ? Бид дараах тэгшитгэлийг ашиглана:  $-x = \bar{x} + 1$ .  $x$ -ийг сөрөг тоо болгохын тулд бүх битийг нь урвуу болгоод, нэгийг нэмнэ. Битүүдийг урвуулах нь амархан, учир нь бид хоёр замт логик ашиглаж байгаа. Бүх битийн шугамыг урвуу битийн шугамтай нь зүгээр л сольж өгнө. Нэгийг нэмэх нь бага зэрэг төвөгтэй. Бид эхний дамжуулах битийг нэг болгон тохируулж энэ үйлдлийг гүйцэтгэдэг. Гэхдээ MUST-Adder-ийн загварын улмаас дамжуулах флаг нь шууд хянах боломжгүй дотоод дохио юм. MUST-Adder-ийн талаар [18] дурьдсанчлан, бодит нэмэх үйлдлээс өмнө хоёр тэг оруулдаг тул нэмэх үйлдлийн эхэнд дамжуулах флаг тэг байх нь тодорхой болно. Харин хасах үйлдэлд, дамжуулах флаг нэг байх ёстой тул эхэнд хоёр нэг оруулна. Гэвч MUST-Subtractor ADDx-ийн хоёр оролтыг бие даан хянах боломжгүй. Хасагдаж буй тооны хоёр дахь, урвуу оролт нь ижил оролтын тоо  $x$ -ийн өөрөө бөгөөд дөрвөн циклээр хойшлогдож, урвуу болсон хувилбар юм. Бид хүссэн үр дүнд хүрэхийн тулд битүүдийн дарааллыг сайтар төлөвлөх шаардлагатай. Харин хоёр дахь оролт  $y$ -ийг параметр  $a$ -тай үржүүлэх үйлдэл хялбар юм:  $a$  нь 0хб. Бид  $y$ -ийг хоёр битээр, дараа нь нэг битээр шилжүүлээд, эдгээр завсрын үр дүнгүүдийг нэмж өгнө, хасах үйлдэл шаардлагагүй.

$$0x6 \cdot y = (4+2) \cdot y = (y \ll 2) + (y \ll 1) \quad (4)$$

Оролтын дохионы цагийн хуваарийг дараах байдлаар үзүүлэв

- [цикл 1] оролт  $x_0, y_0$  баруун талд,
- [цикл 2] оролт  $x_1, y_1$  баруун талд,
- [цикл 3] оролт  $x_2, y_2$  баруун талд,
- [цикл 4] оролт  $x_3, y_3$  баруун талд,
- [цикл 5] оролт  $x_4, y_4$  баруун талд.

Тэгвэл,  $x_0$ -ийг  $x_0$ -д (баруун дохио),  $x_4$ -ийг  $x_4$ -д (зүүн дохио) байрлуулна. Одоо  $x_0 - x_4$ -ийг тооцоолох шаардлагатай. Энэ тооцооллыг ADDx-д гүйцэтгэнэ. Үүний зэрэгцээ,  $y_2 + y_3$  -ийг тооцоолно. Энэ тооцооллыг ADDy-д гүйцэтгэнэ.

[цикл 6] оролт  $x_5, y_5$  баруун талд

Дараа нь,  $x_0$ -д  $x_1$  (баруун дохио),  $x_4$ -д  $x_5$  (зүүн дохио) байрлана. Одоо  $x_1 - x_5$ -г тооцоолох шаардлагатай байна. Энэ тооцооллыг ADDx-д гүйцэтгэж байна. Үүний зэрэгцээ,  $y_3 + y_4$  -г тооцоолно. Энэ тооцооллыг ADDy-д гүйцэтгэж байна. Өмнөх циклээс  $x_0 - x_4$  болон  $y_2 + y_3$  байгаа. Энэ циклд эдгээр хоёрыг нэмж, үр дүнгийн эхний бит болох  $w_0 = x_0 - x_4 + y_2 + y_3$  -г гарган авна. Энэ тооцооллыг ADDz-д гүйцэтгэж байна.

ОРОЛТЫН ДОХИОНЫ ХУГАЦАА

2-Р ХҮСНЭГТ

A:	0	0	0	0	$x_3$	$x_2$	$x_1$	$x_0$	0	0	0	0	1	0	0	0	0	x	x	x	x
B:					0	0	0	0	$\bar{x}_3$	$\bar{x}_2$	$\bar{x}_1$	$\bar{x}_0$	1	1	1	1	0	1	1	1	1
C:													1	0	0	0	x	x	x	x	x
S:					$\bar{w}_7$	$\bar{w}_6$	$\bar{w}_5$	$\bar{w}_4$	$\bar{w}_3$	$\bar{w}_2$	$\bar{w}_1$	$\bar{w}_0$	0	1	1	x	x	x	x	x	x
A:	0	0	0	0	0	0	0	$y_3$	$y_2$	$y_1$	$y_0$	0	0	0	0	x	x	x	x	x	x
B:					0	0	$y_3$	$y_2$	$y_1$	$y_0$	0	0	0	0	0	x	x	x	x	x	x
C:												0	0	0	0	x	x	x	x	x	x
S:					$\bar{v}_7$	$\bar{v}_6$	$\bar{v}_5$	$\bar{v}_4$	$\bar{v}_3$	$\bar{v}_2$	$\bar{v}_1$	$\bar{v}_0$	0	x	x	x	x	x	x	x	x

D. Цагийн тохиргоо ба дохионы эхлүүлэх үйл явц

Энэхүү загварт ADDx, ADDy, ADDz гэсэн гурван MUST-Adder-ийг ашигласан болно. Ерөнхийдөө ADDx нь хасах үйлдэл гүйцэтгэнэ. Эдгээр нь дараах тооцооллуудыг хийдэг:

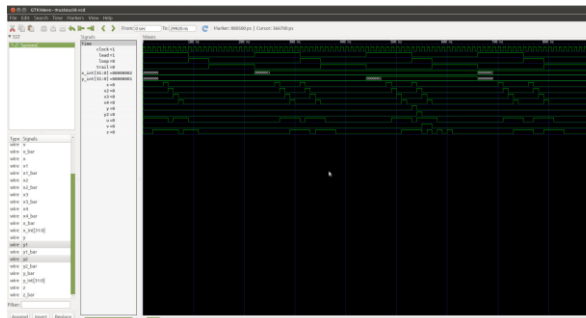
MUST-ADDER-ИЙН ХАСАХ ҮЙЛДЭЛ

3-Р ХҮСНЭГТ

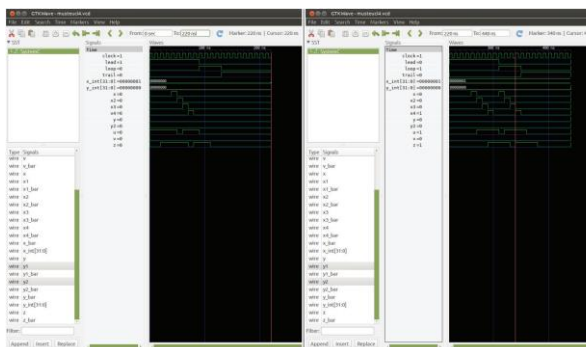
Нэр	Функци	Хэрэгжүүлэлт
ADDx	$x \cdot 15$	$(x \ll 4) - x$
ADDy	$y \cdot 6$	$(x \ll 2) + (x \ll 1)$
ADDz	$ADDx + ADDy$	-

MUST-Adder-ийг зөв ажиллуулахын тулд үндсэн тоог нэмэхээс өмнө дотоод дамжуулах дохиог дахин тохируулахын тулд '0' оруулах шаардлагатай.  $y$ -ийн оролтод энэ нь хялбар бөгөөд тооцооллын эхэнд хангалттай тооны '0'-ийг оруулахад хангалттай. Харин ADDx дээр нэмэх бус, хасах үйлдэл хийдэг тул эхэндээ дамжуулах дохиог '1' болгон тохируулах шаардлагатай учраас энэ нь нэлээд төвөгтэй. MUST-Adder нь дангаар хасах үйлдэл гүйцэтгэх үед тооцооллын өмнө '0' оруулахын оронд '1' оруулах шаардлагатай болно. Мөн хасах үйлдэл хийхийн тулд хасагдаж буй тоог логикийн хувьд урвуулах шаардлагатай байдаг. Бид хос замт логик ашигладаг тул [18] энэ нь амархан бөгөөд зүгээр л  $x$  болон  $\bar{x}$  дохионы шугамуудыг сольж урвуулах боломжтой. Гэхдээ хасах үйлдлийн эхэнд дамжуулах дохиог '1' болгоход бэрхшээлтэй байдаг, учир нь бид ADDx-ийн хоёр оролтыг бие даан хянах боломжгүй. Зөвхөн нэг оролтын дохио болох  $x$ -ийг хоёр удаа оруулдаг: нэг нь урвуу, нөгөө нь дөрвөн циклээр хоцорсон хувилбараар. Иймээс хүссэн үр дүнг гаргахын тулд урьдчилсан оролтын дарааллыг маш нарийн боловсруулж төлөвлөх шаардлагатай. Мөн ADDz-г зөв эхлүүлэхийн тулд (дотоод дамжуулах дохиог цэвэрлэх) ADDx ба ADDy хоёулаа эхлээд бодит тоонуудаа гаргахаас өмнө '0' гаралт үүсгэх шаардлагатай. Тиймээс тооцооллын эхэнд ADDx нь дотоод дамжуулах дохиог '1', мөн 'ADDz'-д '0' нийлбэр гаралтыг үүсгэх ёстой. Энэ чухал хугацааг 2-р хүснэгтэд хоёр давхар зураасаар тэмдэглэсэн. 2-р хүснэгтийн дээд хэсэгт 'ADDx'-ийн тооцооллыг харуулсан бол доод хэсэгт 'ADDy'-ийн тооцооллыг харуулсан. Доод хэсэгт  $y$ -ийн эхэнд хангалттай тооны '0' оруулахад л хангалттай, энэ нь харьцангуй хялбар хэсэг юм. 2-р хүснэгтийн дээд хэсэгт  $x$ -ийн өмнө

дөрвөн '0' оруулж, шилжсэн  $x$ -ийг хасах үйлдэлд зориулж тэгээр дүүргэх ёстой. Гэхдээ энэ нь ADDx-ийн хоёр дахь оролтод дөрвөн анхны '1' гарах шалтгаан болно, учир нь бүх зүйл цаг хугацааны хувьд шилжиж, урвуу болсон байдаг. Тоон утга 'x' эхлэхээс өмнөх цагийн циклд нийлбэрт '0', дамжуулалтад '1' үүсгэх шаардлагатай. Иймээс, тасархай зураастай шугам дээр 'x' дохиог '1' болгож тохируулна, ингэснээр 4 циклээр өмнө урвуу оролт дээр '0' гарах болно. Дараа нь дамжуулах дохио нэг циклээр өмнө '0' байх ёстойг баталгаажуулах шаардлагатай. Гэвч оролт 'B'-гийн бүх оролт '1' учраас оролт 'A'-гийн бүх оролт тэг байх шаардлагатай. Ингэснээр, өмнөх циклээс дамжуулалт дараагийн цикл рүү дамждаг. Энэ дамжуулалтыг таслах цорын ганц боломж нь 'B'-д байгаа дөрвөн '1'-ийн яг дараа, 'A'-гийн '1' нь 'B'-д '0' болох мөч юм. Энэ үед бид нэмэлтээр өөр нэг '0' оруулна. Энэ '0' нь дөрвөн циклээр дараа байх '1'-тэй хамт дотоод дамжуулах флагт шаардлагатай '0'-г үүсгэдэг. Нийтдээ бид 'x'-ийн оролтыг '000010000', у-ийн оролтыг '000000000' болгон урьдчилж тохируулах ёстой. System-C-д хэрэгжүүлсэн симуляцуудыг 5-р зурагт харуулсан ба туршилтын жишээнүүдийг  $x=0x0$ ,  $y=0x0$  утгатайгаар 6-р зургийн а хэсэгт,  $x=0x1$ ,  $y=0x0$  утгатайгаар 6-р зургийн b хэсэгт,  $x=0x1$ ,  $y=0x1$  утгатайгаар 7-р зурагт тус тус үзүүлсэн болно.



5-р зураг. MUST-Euclidean-ийн System-C дээрх загварчлал

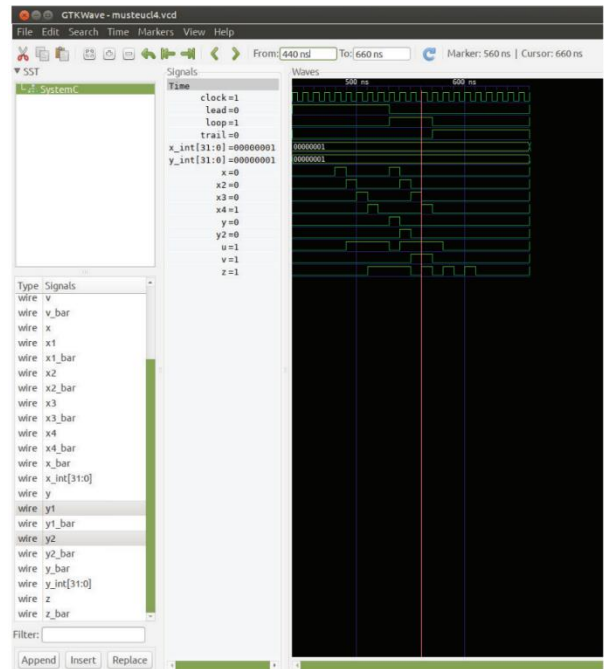


6-р зураг. MUST-Euclidean. Туршилт: a)  $x=0x0$ ,  $y=0x0$  болон b)  $x=0x1$ ,  $y=0x0$ .

**IV. ҮР ДҮН БА ХЭЛЭЛЦҮҮЛЭГ**

Бид  $\sqrt{x^2 + y^2}$  -ыг  $a \cdot x + b \cdot y$  эсвэл  $a \cdot y + b \cdot x$  оор ойролцоо тооцоолсон [23]. Үүнд  $x$ ,  $y$  хоёр тооны

ихийг нь  $a$ -аар үржүүлж, бага тоог  $b$ -ээр үржүүлсэн. Үүний өмнө аль аль тооны абсолют утгыг авсан.



7-р зураг. MUST-Euclidean. Туршилт:  $x=0x1$ ,  $y=0x1$ .

Мөн  $a$  ба  $b$  нь цөөн хэдэн бит бүхий тогтмолууд учир, үржүүлэх үйлдлийг шилжүүлэлт болон нэмэх үйлдлүүдээр сольсон. Эдгээр тооцооллыг MUST-Adder дээр суурилсан HP/LP нейронууд [18] ашиглан Спайк нейрон Пи системийн орчинд хэрэгжүүлсэн. System-C программчлалын хэл дээрх симуляцийн загварууд хүсэлтээр авах боломжтой.

**V. ДҮГНЭЛТ**

Бид квадрат язгуур тооцооллыг хасч, ойролцоо утгын нарийвчлалыг 41%-иас ердөө 4% болгож сайжруулсан алгоритмыг нэвтрүүлсэн. Дараалсан Ньютоны давталт бүр битийн тоог хоёр дахин ихэсгэдэг тул эхний хоёр давталтыг хийх шаардлагагүй болсон. Жишээлбэл, 16-битийн нарийвчлалтай үр дүнг дөрвөн давталтын оронд ердөө хоёр давталтаар олж болно. Энэ тооцооллыг Спайк нейрон Пи систем дэх HP/LP мэдрэлийн элементүүд ашиглан гүйцэтгэсэн. Цаашилбал, уг алгоритмын ойролцоо тооцооллын гүйцэтгэлийг оновчтой болгож, автомат жолоодлогын туслах систем (ADA) болон RSA крипто шинжилгээ зэрэг зарим хэрэглэнд ашиглахыг зорьж байна.

**АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ**

- [1] Leonard M Adleman. On constructing a molecular computer. DNA based computers, 27:1–21, 1995.
- [2] Haiming Chen, Mihai Ionescu, and Tseren-Onolt Ishdorj. On the Efficiency of Spiking Neural P Systems. Proceedings of 8th International Conference on Electronics, Information, and Communication (ICEIC 2006), Ulaanbaatar, Mongolia, pages 49–52, Jun 2006.
- [3] D. Cohen. Precalculus: A Problems-Oriented Approach. Cengage Learning, 2004.

- [4] Ganbat Ganbaatar, Dugar Nyamdorj, Gordon Cichon, and Tseren-Onolt Ishdorj. Implementation of rsa cryptographic algorithm using sn p systems based on hp/lp neurons. *Journal of Membrane Computing*, 3(1):22–34, 2021.
- [5] Chen Haiming, Tseren-Onolt Ishdorj, and Gheorghe P`aun. Computing along the axon. *Progress in Natural Science*, 17(4):417–423, Apr 2007.
- [6] Mihai Ionescu, Andrei P`aun, Gheorghe P`aun, and Mario J. P`erez-Jim`enez. Computing with Spiking Neural P Systems: Traces and Small Universal Systems. In: Mao C. and Yokomori T. (Eds) *DNA Computing. DNA 2006. Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, 4287(16):1–16, 2006.
- [7] Mihai Ionescu, Gheorghe P`aun, and Takashi Yokomori. Spiking Neural P Systems. *Fundamenta Informaticae*, 71(2):279–308, Aug 2006.
- [8] Tseren-Onolt Ishdorj and Alberto Leporati. Uniform solutions to SAT and 3-SAT by Spiking Neural P systems with pre-computed resources. *Natural Computing*, 7(4):519–534, Dec 2008.
- [9] Tseren-Onolt Ishdorj, Alberto Leporati, Linqiang Pan, and Jun Wang. Solving NP-Complete Problems by Spiking Neural P Systems with Budding Rules. In Gheorghe P`aun, Mario J. P`erez-Jim`enez, Agustin Riscos-N`u`nez, Grzegorz Rozenberg, and Arto Salomaa, editors, *Membrane Computing*, pages 335–353, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.
- [10] Tseren-Onolt Ishdorj, Alberto Leporati, Linqiang Pan, and Xiangxiang Zeng. Deterministic solutions to QSAT and Q3SAT by Spiking Neural P systems with pre-computed resources. *Theoretical Computer Science*, 411(25):2345–2358, May 2010.
- [11] Tseren-Onolt Ishdorj, Otgonnaran Ochirbat, and Chuluunbandi Naimannaran. A  $\mu$ -fluidic biochip design for Spiking Neural P systems. *International Journal of Unconventional Computation*, 2019.
- [12] R. H. Krambeck, C. M. Lee, and H. S. Law. High-speed compact circuits with cmos. *IEEE Journal of Solid-State Circuits*, 17(3):614–619, June 1982.
- [13] Lucas Ledesma, Daniel Manrique, and Alfonso Rodr`iguez-Pat`on. A tissue P system and a DNA microfluidic device for solving the shortest common superstring problem. *Soft Computing*, 9(9):679–685, Sep 2005.
- [14] Alberto Leporati and Miguel-Angel Guti`errez-Naranjo. Solving subset sum by spiking neural p systems with pre-computed resources. *Fundamenta Informaticae*, 87(1):61–77, Dec 2008. 11
- [15] Wolfgang Maass. Computing with spikes. *Foundations of Information Processing of TELEMATIK*, 8(1):32–36, 2002.
- [16] Wolfgang Maass and Christopher M. Bishop (Eds). *Pulsed Neural Networks*. MIT Press, The address, 1 edition, 2006. A Bradford Book.
- [17] Gerd HG Moe-Behrens. The biological microprocessor, or how to build a computer with biological parts. *Computational and Structural Biotechnology Journal*, 7(8):e201304003, 2013.
- [18] Otgonnaran Ochirbat, Tseren-Onolt Ishdorj, and Gordon Cichon. An error-tolerant serial binary full-adder via a spiking neural p system using hp/lp basic neurons. *Journal of Membrane Computing*, 2(1):42–48, 2020.
- [19] Gheorghe P`aun. *Membrane Computing: An Introduction*. Springer-Verlag, Berlin, Heidelberg, 2002.
- [20] Gheorghe P`aun, Grzegorz Rozenberg, and Arto Salomaa. *The Oxford Handbook of Membrane Computing*. Oxford University Press, 2010.
- [21] Fei Wang, Hui Lv, Qian Li, Jiang Li, Xueli Zhang, Jiye Shi, Lihua Wang, and Chunhai Fan. Implementing digital computing with dna-based switching circuits. *Nature Communications*, 11(1):121, Jan 2020.
- [22] Neil H. E. Weste and Kamran Eshraghian. *Principles of CMOS VLSI Design: A Systems Perspective*. AddisonWesley Longman Publishing Co., Inc., Boston, MA, USA, 1985.
- [23] E. E. Wright. Problem corner 69.a. *The Mathematical Gazette*, 69(447):48–50, 1985.
- [24] Zhengfan Xia, Shota Ishihara, Masanori Hariyama, and Michitaka Kameyama. Dual-rail/single-rail hybrid logic design for high-performance asynchronous circuit. In 2012 IEEE International Symposium on Circuits and Systems (ISCAS), pages 3017–3020, 2012.
- [25] Zihan Xu, Matteo Cavaliere, Pei An, Sarma Vrudhula, and Yu Cao. The stochastic loss of spikes in spiking neural p systems: Design and implementation of reliable arithmetic circuits. *Fundamenta Informaticae*, 134(1-2):183–200, 2014.
- [26] Gexiang Zhang, Haina Rong, Ferrante Neri, and Mario J. P`erez-Jim`enez. An optimization Spiking Neural P system for approximately solving combinatorial optimization problems. *International Journal of Neural Systems*, 24(5):1440006, May 2014.

## ВИРУС ТАНИХ SERS ГАДАРГУУГИЙН ЗОХИОМЖ, СИМУЛЯЦ

Лхагвасүрэн ЭНХБАЯР<sup>1</sup>, Чулуунбаатар ДААРИЙМАА<sup>2</sup>, Ишдоржийн ЦЭРЭН-ОНОЛТ<sup>3</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Компьютерын Ухааны Салбар

Холбогдох зохиогчийн и-мэйл хаяг: tseren-onolt@must.edu.mn<sup>1\*</sup>

**Хураангуй:** Вирусын халдварыг түргэн, өндөр нарийвчлалтай илрүүлэх, өртөг багатай төхөөрөмж буюу түргэн оношлуурын судалгаа сүүлийн жилүүдэд эрчимтэй явагдаж байна. Бид энэхүү судалгааны ажлын хүрээнд Ковид-19 вирус, түүний гадаргуу дээр байрлах уургуудыг тухайн уураг тус бүрийн өвөрмөц Раман спектрээр нь таних биочипийн судалгаанд тулгуурласан симуляцын загвар боловсруулахыг зорьсон болно.

**Түлхүүр үгс:** симуляц, бөөмс цуглуулах, биочипийн зохиомж, DEP, SERS, вирус

### I. УДИРТГАЛ

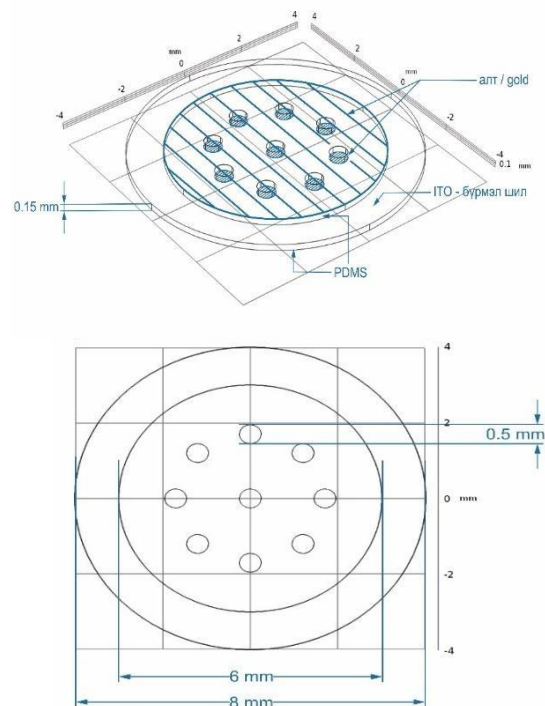
Биочипийн загвар хөгжүүлэн, үйлдвэрлэн туршихдаа лабораторын төхөөрөмжүүд дээр хэмжилтүүд хийж, олон дахин турших, хэмжих шаардлага гардаг нь цаг хугацааны болон материал, техникийн хувьд зардал ихээр шаарддаг. Тэгвэл компьютер симуляц болон симуляцын үр дүнгээр өгөгдлийн сан үүсгэж, MatLab зэрэг системд боловсруулалт хийснээр дээрх хүндрэлүүдийг багасгах боломжтой юм. Ийм зорилгоор бид өөрсдийн хөгжүүлж буй зуурамтгай шингэнээс бөөмс ялган, хуримтлуулах биочипэнд зориулсан симуляцын загвар хөгжүүлж, симуляцын үр дүнг боловсруулан хамгийн сайн параметрүүдийг харьцуулалтын аргаар тодорхойлох аргачлал боловсруулсан болно. Ингэснээр тус биочипийн загварыг хөгжүүлэх цаашдын судалгаанд дэвшил гарч, биочип үйлдвэрлэн туршихын өмнө боломжит хувилбаруудыг урьдчилан тооцож, улмаар хамгийн сайн хувилбарыг сонгон ашиглах боломжтой болж байгаа юм.

COMSOL multiphysics програм дээр биочипийн загварыг зохиомжлохдоо вирусын халдварын дээжийг цуглуулах бортого, уургуудыг цуглуулах үүрүүд рүү тус бүрийн багана барзгар бүтэц гэсэн хэсгүүдтэй байхаар тооцоолсон. Цуглуулах чипэд вирусын уургууд, эсрэг биет, наношошго зэрэг бөөмсийг хийнэ. Бортогонд жигд бус цахилгаан орон үүсгэснээр вирусын уургууд үүрүүд рүү цугласнаар багана гадаргуу дээр байрласан эсрэг биетүүд дээр холбоо үүсгэн наалдснаар нягт цугларал үүснэ. Улмаар 785нм Лазерийн гэрэл тусгаж уураг тус бүрийн болон наношошгын спектрийг бүртгэж авснаар тухайн вирусын халдвар мөн эсэхийг таних зорилготой.

### II. ЦУГЛУУЛАХ БОРТОГЫН ЗОХИОМЖ

Цуглуулагч био-чипийн гадаад диаметр 8мм, өндөр 0,15мм хэмжээтэй. Тус чипийн шингэн хадгалах дотоод цилиндрийн диаметр 7мм бөгөөд тус цилиндрийн дээд тал электрод бол ёроолд тус

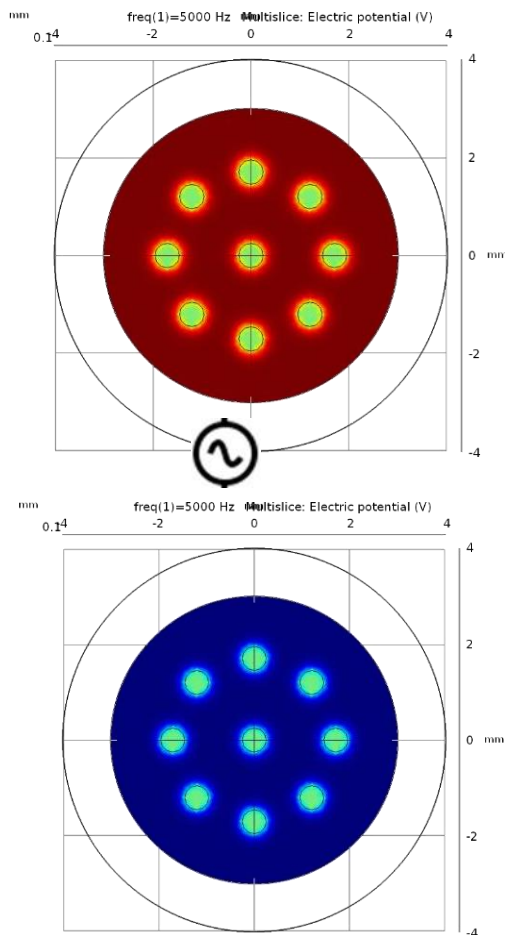
цилиндрийн хана PDMS (Polydimethylsiloxane) бүр 0,5мм диаметр бүхий 9 ширхэг электродууд байрласан. Чипийн дээд ба доод тал ITO-бүрмэл шил (Indium Tin Oxide, ITO) ба шингэн хадгалах давхарга, электродууд алтаар бүрэгдсэн байна.



Зураг 1. Бортогын зохиомж

### Цахилгаан

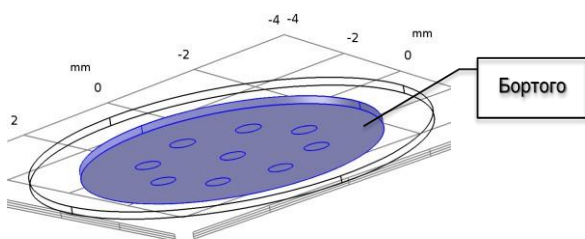
Биочипийн дээд электродыг -5V, доод талын 9 жижиг электродыг +5V ийн хувьсах хүчдэлд холбох ба ингэснээр шингэн агуулах бортогони дотор хувьсах цахилгаан орон үүснэ. Цахилгаан орны дүрслэлийг Зураг 2-оос харна уу.



Зураг 2. Бортгогнд хувьсах цахилгаан орон үүсгэх.

**Шингэний ба бөөмсийн урсгал**

Шингэн агуулах бортогыг Зураг 3-т тэмдэглэв. Зуурамтгай шингэний урсгал Greeping flow хуульд захирагдна.

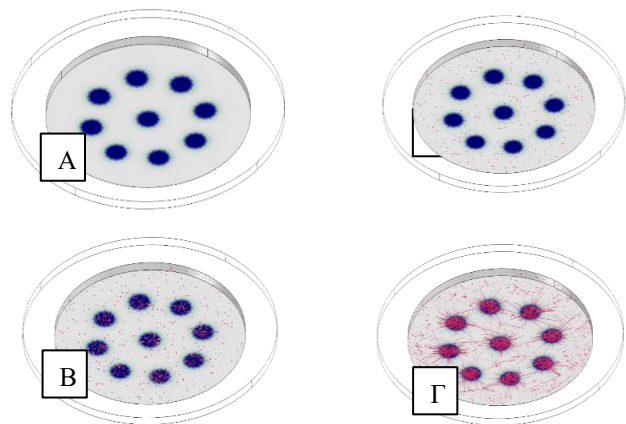


Зураг 3. Бөөмс агуулсан зуурамтгай шингэн агуулах бортого.

**Бөөмс ба түүний хөдөлгөөн**

Симуляцын загварт шингэнд агуулагдах бөөмсийг (энд авч үзэж буй жишээнд 4000 ширхэг) санамсаргүйгээр байрлуулна. Биологийн бөөмс тухайлбал цусны улаан, цагаан эс, бактери нь диэлектрик шинж чанартайгаас гадна дотроо хөндий буюу арьсны зузаантай. Бөөмсийн шинж чанарыг Хүснэгтэд 1-д үзүүлэв.

Жигд бус цахилгаан оронд хувьсах гүйдлийн улмаас диэлектрик хүч (dielectric force DEP) үүсэх бөгөөд бөөмс цилиндрт үүссэн диэлектрик хүч, электроосмотик урсгалын (electroosmotic flow EOF) нөлөөгөөр чипийн ёроолд байрлах 9 жижиг электрод бүхий нүхнүүдэд хуримтлагдах үйл явц болно. Энэ үзэгдлийн Зураг 4-т дүрслэн үзүүлэв.



Зураг 4. А. Симуляц эхлэхийн өмнөх байдал. Б. Бөөмс бүхий шингэн бортогонд байралсан байдал. В. Симуляц эхлэх агиинд бөөмс доод электродуудруу татагдаж эхлэх үе. Г. Симуляцын явцад бөөмс электродууд дээр хуримтлагдах үйл явц.

**DEP ХҮЧНИЙ ТЭГШИТГЭЛ**

$$F_{dp} = 2\pi r_p^3 \epsilon_0 \text{real}(\epsilon_r^*) \text{real}(K) \nabla |E|^2$$

$$K = \frac{\epsilon_{rp}^* - \epsilon_r^*}{\epsilon_{rp}^* + 2\epsilon_r^*}$$

$$\epsilon_r^* = \epsilon_r - \frac{i\sigma}{\omega} \text{ for time-harmonic fields}$$

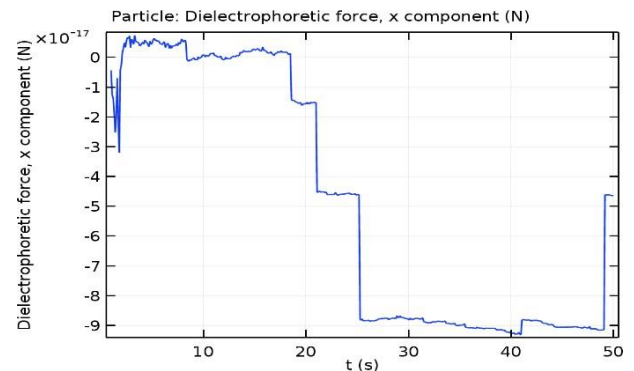
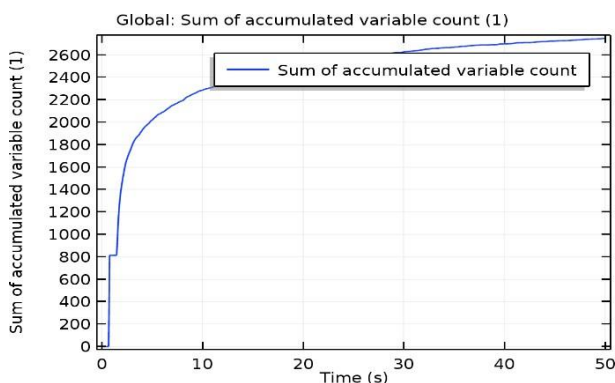
$$\epsilon_r^* = \epsilon_r \text{ for stationary fields}$$

БИОЧИПИЙН ӨГӨГДЛИЙН ШИНЖ ЧАНАРУУД

1-Р ХҮСНЭГТ

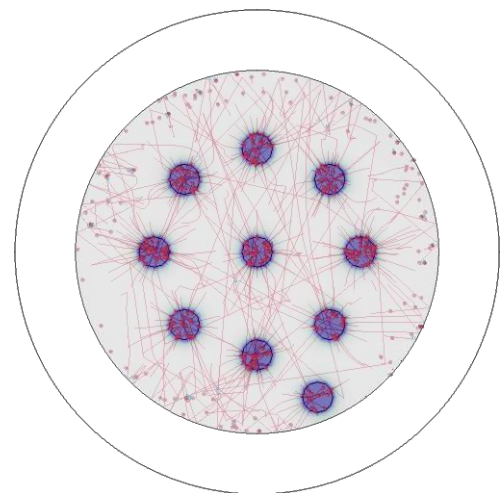
Нэр	Илэрхийлэл	Утга	Тодорхойлолт
f0	5[kHz]	5000 Hz	Цахилгаан орны давтамж
sigma_f	5.5[uS/m]	5.5E-6 S/m	Шингэний цахилгаан дамжуулах чанар
epsilon_f	70	70	Шингэний харьцангуй шингээх чадвар
rho_f	1000[kg/m <sup>3</sup> ]	1000 kg/m <sup>3</sup>	Шингэний нягт
mu_f	1e-3[Pa*s]	0.001 Pa*s	Шингэний динамик эсэргүүцэл
rho_p	1050[kg/m <sup>3</sup> ]	1050 kg/m <sup>3</sup>	Бөөмийн нягт (Цусны улаан эс ба бактери)
dp1	1.8[um]	1.8E-6 m	Бөөмийн диаметр
sigma_p1	0.25[S/m]	0.25 S/m	Бөөмийн цахилгаан дамжуулах чанар
epsilon_p1	50	50	Бөөмийн харьцангуй цахилгаан шингээх чадвар
sigma_s1	4.4[mS/cm]	0.44 S/m	Бөөмийн арьсны дамжуулах чадвар
epsilon_s1	6	6	Бөөмийн харьцангуй шингээх чадвар
th_s1	8[nm]	8E-9 m	Бөөмийн арьсны зузаан

Симуляцын үр дүн



Зураг 5. А. Биочипийн ажиллагааны үр дүнд шингэнд агуулагдаж байгаа (4000 ширхэг) бөөмсийн (E. Coli) 65% нь бортогоны ёроолд байрлах электродууд дээр ялгарч хуримтлагдсан байдал. Б. Бөөмсд үйлчилж буй диэлектрик хүчний өөрчлөлт.

Вирусын уургууд эсвэл бактерийг дээжээс ялган цуглуулж нягт орчин үүсгэх туршилтад 4000 ширхэг бөөм ашиглахад 50 секундын симуляцад 65 хувь амжилттай цугларсан ба бортогоны хүрээгээр байрлах бөөмс татагдаагүй үлдсэн байна (Зураг 6).



Зураг 6. Симуляцын дараах байдал

Био-бөөмс хуримтлуулах микрошингэн биочипийн загвар боловсруулах аргын ялгаа нь өөрсдийн шинээр хөгжүүлж буй зуурамтгай микрошингэнээс бөөмсийг дотоод шинж чанараар нь физикийн аргаар ялган, хуримтлуулах (цуглуулах) төхөөрөмж үйлдвэрлэхийн өмнө компьютерт загварчилах, симуляц хийн турших, туршилтын өгөгдлүүдээр сан үүсгэх, их өгөгдөл боловсруулах, зохимжтой параметруудийг тодорхойлоход оршино.

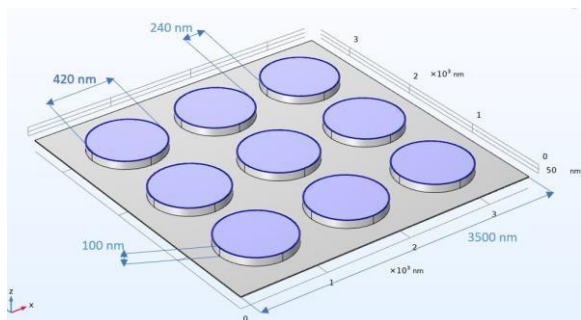
Био-бөөмс хуримтлуулах микрошингэн биочипийн симуляцын загварын ялгаа нь төхөөрөмжийг хийх материалын физик, химийн шинж чанар, ашиглагдах бөөмсийн биохимийн шинж чанар, төхөөрөмжийг ажиллуулах шингэний механикийн параметруудийг тохируулах, хувьсах цахилгааны хүчдэл, давтамжыг тохируулах юм.

Био-бөөмс хуримтлуулах микрошингэн биочипийн симуляц үр дүнгээр сан үүсгэх ялгаа нь өөр өөр өгөдөл, параметрт тохирсон туршилт бүрийн үр дүнгээр өгөгдлийн сан үүсгэж, уян байдлаар шүүлт хийх, эрэмбэлэх, ялгах, нэгтгэх зэрэг боловсруулалт хийхэд оршино.

Био-бөөмс хуримтлуулах микрошингэн биочипийн туршилтын параметруудийг сонгох ялгаа нь параметрийн үнэлгээ хийх физик, математикийн арга ашиглаж тооцоолол хийхэд оршино.

### III. БӨӨМС БУЮУ АНТИЖЕН ТАТАХ ЭСРЭГ БИЕТ БҮХИЙГ ГАДАРГУУ

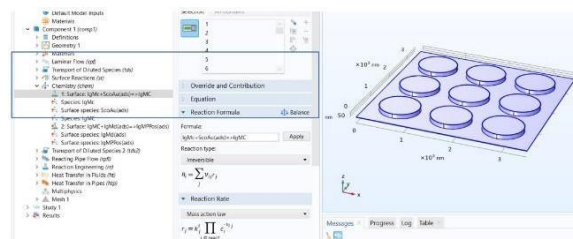
Бөөмс цуглуулах бортогоны үүр бүрд 420нм диаметртэй, 100нм өндөртэй, хоорондоо 240нм зайтай баганууд бүхий барзгар орчныг бүрдүүлж, мөнгөөр бүрнэ (Зураг 7).



Зураг 7. Бөөмс буюу вирустатаж цуглуулах, бэхлэх хавтан.

Вирус татах хавтангийн мөнгөөр бүрэгдсэн баганууд дээр эсрэг биет байрлуулснаар вирус уураг болон лазерийн спектр идэвхжүүлэх наношошгын нэгдэл үүснэ. Энэхүү химийн урвал, нэгдлийг хэрэгжүүлэхдээ COMSOL -ийн Chemistry модулын тусламжтай гүйцэтгэнэ.

Цаашид дээжийн найрлага, концентрацыг нарийвчлан тогтоож симуляцын өгөгдөл болгон өгсөнөөр туршилт хийхэд бэлэн болно. Раман спектрийг хэмжихдээ Комсолын Optics wave модулын тусламжтайгаар гүйцэтгэх боломжтой.



Зураг 8. Химийн нэгдлүүд үүсгэх

### ДҮГНЭЛТ

Биологийн бөөмс цуглуулах биочипийн зохиомжийг гарган улмаар вирусын уургуудыг цуглуулан Раман спектрээр таних функцаар өргөтгөх боломжийг Комсол программ дээр судалж, симуляц хийх оролдлогыг хийлээ. Бодит био-өгөгдлийн шинж чанаруудыг оруулах, тооцоолол гүйцэтгэх модулиудыг нарийвчлан судалж ашиглах, улмаар симуляцын үр дүнд боловсруулалт хийн загварын зохиомжид сайжруулалт хийх нь энэхүү ажлын ойрын зорилт болно.

### НОМ ЗҮЙ

- [1] COMSOL: Multiphysics Software for Optimizing Designs --- comsol.com. <https://www.comsol.com/>, [Accessed 26-11-2024]Kiran Kaladharan, Kuan-Hung Chen, Pin-Han Chen, Venkanagouda S. Goudar, Tseren-Onolt Ishdorj, Tuhin Subhra Santra, Fan-Gang Tseng, Dual-clamped one-pot SERS-based biosensors for rapid and sensitive detection of SARS-CoV-2 using portable Raman spectrometer, Sensors and Actuators B: Chemical, Volume 393, 2023.
- [2] Kuan-Hung Chen, Shih-Han Lee, Li-Ching Kok, Tseren-Onolt Ishdorj, Hwan-You Chang, Fan-Gang Tseng, A 3D-ACEK/SERS system for highly efficient and selectable electrokinetic bacteria concentration/detection/ antibiotic-susceptibility-test on whole blood, Biosensors and Bioelectronics, Volume 197, 2022,

# ӨМНӨГОВЬ АЙМАГ ДАХЬ “ТУРВАН САЙХАН” НИСЭХ БУУДЛЫГ ОЛОН УЛСЫН АНГИЛАЛД ШИЛЖҮҮЛЭХ БОЛОМЖИЙН СУДАЛГАА

Тодбаярын Үлэмж, Эрхэмбаатарын Нарантуяа

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбоо технологийн сургууль, Холбооны салбар

Монгол улс, Улаанбаатар хот

Холбоо барих зохиогчийн и-мэйл хаяг: [narantuya@must.edu.mn](mailto:narantuya@must.edu.mn)<sup>1\*</sup>

*Хураангуй:* Монгол Улсын Засгийн газрын 2020-2024 оны үйл ажиллагааны хөтөлбөрт агаарын тээврийн либералчлалыг үргэлжлүүлж өрсөлдөөн бий болгох, нислэгийн тоо, чиглэлийг нэмэгдүүлэх, орон нутгийн нисэх буудлуудын ашиглалтыг сайжруулахаар тусгасан. Өмнөговь аймгийн хүн амын шилжилт хөдөлгөөн, уул уурхайн компанийн ажилчдын урсгал, дотоод, гадаадын жуулчдын эрэлт, хэрэгцээ нь Даланзадгад суманд олон улсын нисэх онгоцны буудал байгуулах зайлшгүй шаардлагыг үүсгэж байна. Монгол Улсын Засгийн газрын тогтоолоор орон нутгийн 4 нисэх буудлын хүчин чадлыг нэмэгдүүлж, ашиглалтыг сайжруулах төсөлд Өмнөговь аймаг дахь “Турван сайхан” нисэх буудал багтсан. Нисэх буудлыг олон улсын статустай болгох боломжийн судалгаагаар Өмнөговь аймаг дахь “Турван сайхан” нисэх буудлын хүчин чадлыг нэмэгдүүлж, олон улсын стандартад нийцүүлж, 4D ангиллын болгох боломжийг гаргахыг зорилоо.

*Түлхүүр үг:* нисэх буудлын ангилал, нисэх буудлын стандарт, 4C, 4D ангиллын нисэх буудал

## I. УДИРТГАЛ

Монгол Улсын Засгийн газрын 2020-2024 оны үйл ажиллагааны хөтөлбөрт агаарын тээврийн либералчлалыг үргэлжлүүлж өрсөлдөөн бий болгох, нислэгийн тоо, чиглэлийг нэмэгдүүлэх, орон нутгийн нисэх буудлуудын ашиглалтыг сайжруулахаар тусгасан [1]. Мөн "Алсын хараа 2050" урт хугацааны хөгжлийн бодлогод "Зарим аймгийн нисэх буудлыг 4C зэрэглэлийн агаарын хөлөг хүлээн авах хүчин чадалтай аэродром, зорчигч үйлчилгээний цогцолбор олон улсын нисэх буудалтай болгож, аялал жуулчлал, гадаад худалдааг дэмжинэ" хэмээн заасан юм [2]. Монгол Улсын Засгийн газрын 2023 оны 7 дугаар сарын 5-ны өдрийн 253 дугаар тогтоолоор Дорнод аймаг дахь “Чойбалсан”, Ховд аймаг дахь “Ховд”, Хөвсгөл аймаг дахь “Мөрөн”, Өмнөговь аймаг дахь “Турван сайхан” нисэх буудлуудын хүчин чадлыг нэмэгдүүлж, олон улсын стандартад нийцүүлж, Олон улсын иргэний нисэхийн байгууллага (ИКАО)-ын шаардлагыг хангасан 4C, 4D хяналтын кодтой болгох төслийг концессын зураг төсөл боловсруулах, шинэчлэн сайжруулах, ашиглах, шилжүүлэх төрлөөр хэрэгжүүлэхээр тогтсон.

## II. СУДАЛГААНЫ АЖЛЫН ТАНИЛЦУУЛГА БА ҮНДЭСЛЭЛ

### Нисэх буудлыг олон улсын статустай болгох үндэслэл

ИНЕГ-аас танилцуулснаар эхний ээлжинд концессын сонгон шалгаруулалт зарласан дөрвөн нисэх буудал нь худалдаа, тээвэр ложистик, аялал жуулчлалын чиглэлээр бүс нутгийн олон улсын зангилаа нисэх буудлууд болгон хөгжүүлэх бүрэн

боломжтой [3]. Ховд аймгийн “Ховд” нисэх буудлыг өргөжүүлснээр төв болон дундад ази руу баруун бүсийн мах экспортлох, Хөвсгөл аймгийн “Мөрөн” нисэх буудлыг дэлхийн хамгийн цэнгэг хоёр нуур болох Хөвсгөл, Байгаль нуурыг холбон аялал жуулчлалын чиглэлээр хөгжүүлэх, Дорнод аймгийн “Чойбалсан” нисэх буудлыг зүүн өмнөд азийн ачаа тээврийн зангилаа бүс болгон хөгжүүлэх, алслагдсан бүс нутагт агаарын тээврийн үйлчилгээг тогтворжуулах, олон улсын агаарын харилцааг өргөжүүлнэ [4].

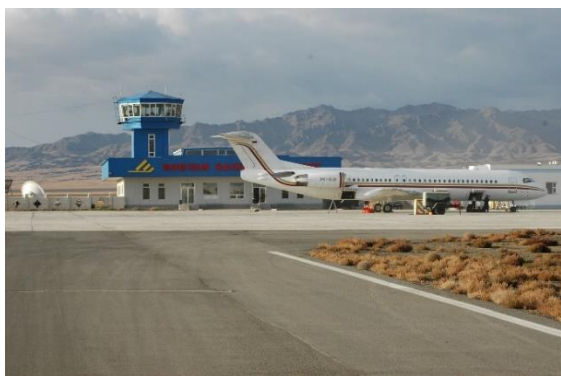
Нисэх буудлыг өргөтгөх ажлын зургийн даалгаварт аэродромын хөөрч буух зурвасыг 4C ангиллын агаарын хөлөг буюу Boeing 737-800, Airbus 320neo, Embraer 190, 3C ангиллын Embraer 145, 2B ангиллын Cessna 208, Beechcraft 1900, Embraer 110 зэрэг агаарын хөлгүүдэд тохируулан уртасгах, өргөсгөх, хучилтын даацыг тооцож гаргахаар заасан байна [4].

## III. ӨМНӨГОВЬ АЙМАГ ДАХЬ “ТУРВАН САЙХАН” НИСЭХ БУУДЛЫН ӨНӨӨГИЙН БАЙДАЛ

1957 оны 12-р сарын 04-нд Улаанбаатар хотоос Бадарч даргатай экипажийн жолоодсон АН-2 онгоц Өмнөговь аймгийн Даланзадгад хотын хойд талбай дээр бууснаар “Турван сайхан” нисэх буудлын түүх эхэлсэн юм. Анхны нисэх буудал 3 орон тоотой, 30Вт чадалтай РСР-50 маркын радио аппарат, 3 морины хүчин чадалтай Л-3 цахилгаан мотортойгоор, 7 хоногт 2 удаа Улаанбаатар хотоос зорчигч, шуудан тээврийн агаарын хөлгийг хүлээн авч үйлчилдэг байжээ. 1956 онд Дашдорж даргатай Ил-12 онгоц, 1964 онд Нэмэх даргатай АН-24 онгоцнууд тус тус аэродром дээр анх бууснаар Өмнөговийг зорьсон зорчигч олон түмэнд тохилог агаарын хөлгүүдээр

үйлчлэх болсон түүхтэй. 1961 онд зорчигчдын танхимтай болж, 7 хоногт 3 удаа УБ-ДЗ-УБ чиглэлээр, 1 удаа УБ-Мандалговь-ДЗ-Мандалговь-УБ чиглэлийн дундын нислэгүүдийг тус тус хүлээн авч үйлчилдэг болсон. 1966 оны 11-р сарын 01-нд дотоодын шуудангийн нислэг үйлдэх өөрийн АН-24 онгоцтой болж, эхний удаад аймгийн төвөөс алслагдсан 3 сумдад, удалгүй Хүрмэн, Баяндалайгаас бусад бух сумдад тогтмол зорчигч, шуудан тээврийн нислэгтэй болсноор барахгүй ДЗ-ХУЖИРТ-ДЗ, ДЗ-ДГ-ДЗ, ДЗ-Сайншанд-ДЗ, ДЗ-УБ-ДЗ чиглэлд захиалгат нислэг үйлдэх болсон түүхтэй.

1985 оноос шөнийн гэрэл суултын “Луч-2” систем тавигдсанаар өдөр шөнийн 24 цаг нислэг хүлээн авах хүчин чадалтай болж, зуны улиралд жуулчны нислэгүүдэд үйлчлэн, нисэх буудлын үйл ажиллагааны цар хүрээ өргөжин тэлсэн. Иргэний нисэхийг хөгжүүлэх Монгол Улсын Засгийн газар, ИНЕГ-ын бодлогын хүрээнд 2007 онд нисэх буудал хөөрч буух хучилттай зурвас, цагт 50-60 зорчигчид үйлчлэх хүчин чадалтай шинэ нисэх буудлын цогцолборыг хүлээн авч, одоог хүртэл орон нутгийн нисэх буудлууд дотроо хамгийн их ачаалалтай, “Буянт-Ухаа”, “Чингис хаан” ОУНБ-уудын нөөцөөр нислэгийн аюулгүй байдал, аюулгүй ажиллагааг найдвартай ханган ажиллаж байна. Өнөөдрийн байдлаар нисэх буудал 6 хэсэг, 37 орон тоотойгоор үйл ажиллагаа явуулж байна. Нисэх буудал нь ЗС ангиллын аэродромтой бөгөөд Өмнөговь аймгийн нутаг дэвсгэрт байрлах Оюутолгойн “Ханбумбат”, Гурван тэсийн “Овоот”, Цогтцэцийн “Тавантолгой”-н нисэх буудлууд болон хилийн боомтод үйлдэгдэж байгаа нислэгүүд, Батлан хамгаалахын, Онцгой байдлын, Түргэний зориулалтай нислэгүүд хүлээн авч өвлийн улиралд өдөртөө 2-4 зуны улиралд 4-6 нислэгт үйлчлэн ажилладаг. Жилд дунджаар 2000 орчим буулт хөөрөлтөд үйлчлэн, 1800 орчим агаарын хөлөгт бэлтгэл аэродромоор бэлэн байдал ханган, нислэгийн мэдээллийн болон газрын тусгай үйлчилгээ үзүүлэн нислэг техникийн осол зөрчил гаргалгүй ажиллаж байна.



1-р зураг Өмнөговь аймаг дахь “Гурван сайхан” нисэх буудал

Улсын Их Хурлын Чуулганы нэгдсэн хуралдаанаар Өмнөговь аймгийн нисэх онгоцны буудлыг Олон улсын зэрэглэлтэй болгох санал, 4D ангиллын шинэ

нисэх онгоцны буудалтай болох зорилгоор Өмнөговь аймагт, орчин цагийн хэрэгцээ шаардлагад нийцсэн олон улсын нисэх онгоцны буудал барьж байгуулах дэмжигдсэн [4]. 2024 оны 9 дүгээр сарын байдлаар нийт 635 өдөр шөнийн нислэгийг аэродромдоо хүлээн авч нисэхийн болон нислэгийн аюулгүй ажиллагаа найдвартай байдлыг ханган ажиллаж байна. Тус нисэх буудлын аэродром нь нислэгийн ачааллаас шалтгаалан хөөрч буух хучилттай зурвасын гадаргууд элэгдэл үүсч, засвар үйлчилгээ хийж хүчитгэх шаардлагатай байгаа тул 9-10-р сард хэсэгчилсэн засвар хийсэн. Өнгөрсөн оноос зорчигчийн болон жуулчны нислэг сэргэж, нисэх буудал өвлийн улиралд 7 хоногт 17-19 нислэг, зуны улиралд 7 хоногт дунджаар 30 нислэг хүлээн авсан. 2023 оны байдлаар “Хүннү эйр” ХХК, “Аэромонголиа” ХХК, МИАТ ТӨХК, Зэвсэгт хүчний 303 дугаар анги, Ардын арми, Онцгой байдлын 111 дүгээр анги, “Геосан” ХХК зэрэг авиакомпаниудтай хамтран ажиллаж, өөрийн аэродром дээр 986 агаарын хөлөг хүлээн авч, 1972 хөөрөлт буултад үйлчилсэн. Мөн Өмнөговь аймгийн Ханбогд суманд байрлах “Ханбумбат”, Цогтцэций суманд байрлах “Таван толгой”, Гурван тэс суманд байрлах “Овоот” нисэх буудлуудын районы нислэгт бэлтгэл аэродромоор ажиллаж, нийт 1737 агаарын хөлөгт нислэгийн мэдээллийн үйлчилгээ үзүүлсэн. Өмнөговь аймаг бол аялал жуулчлал, уул уурхайн гол бүс нутаг учир говь нутгийг зорьсон гадаад, дотоодын аялагч, жуулчид, уул уурхай дагасан зорчигчдын хөдөлгөөн жил ирэх тутам нэмэгдэж байна. Үүнтэй холбоотойгоор нислэгийн тоо нэмэгдэж, нисэх буудлын хүчин чадлыг нэмэгдүүлэх Олон улсын нисэх буудал болгох шаардлага бусад орон нутгийн нисэх буудлуудыг бодвол илүү хурдацтай эрчимтэй тавигдаж байгаа [5].

#### IV. НИСЭХ БУУДАЛД ТАВИГДАХ ШААРДЛАГА СТАНДАРТ

##### Нисэх буудлын стандарт

Нисэх буудлын стандарт нь аюулгүй байдал, үйл ажиллагаа, үйлчилгээний чанар, орчны хамгаалал зэрэг олон чиглэлд төвлөрдөг. Дараах үндсэн стандартуудыг агуулдаг:

*Аюулгүй байдал:* Нисэх буудлууд аюулгүй байдлын олон давхар шалгалт, хяналттай байх ёстой. Энэ нь зорчигчдыг шалгах, ачааг шалгах, террорист халдлагаас сэргийлэх системүүдийг агуулна.

*Үйл ажиллагаа:* Нисэх буудлын үйл ажиллагаа нь нислэгийн хуваарь, газрын үйлчилгээ, ачаа дамжуулах систем зэргийг агуулдаг. Энэ нь нисэх буудлын ажилтнуудын сургалт, үйл ажиллагааны стандартуудыг хэрэгжүүлэх шаардлагатай.

*Зорчигчийн үйлчилгээ:* Нисэх буудалд зорчигчдын тухтай, аюулгүй байдал, үйлчилгээг хангах ёстой. Энэ нь төлбөрийн систем, мэдээллийн самбар, дамжуулах үйлчилгээ зэргийг агуулдаг. Нисэх буудлууд нь байгаль орчны стандарт, орчны

хамгаалах дүрэм, хог хаягдлыг боловсруулах арга хэмжээ зэрэгт нийцэх ёстой.

*Техникийн стандарт:* Нисэх буудлын инженерийн бүтэц, тоног төхөөрөмж, нисэх буудлын зам, буудлын тавцан зэрэг техник, технологийн стандартуудыг хангах шаардлагатай.

Эдгээр стандартууд нь олон улсын болон үндэсний хэмжээнд тогтоогдсон байж болох бөгөөд нисэх буудлын үйл ажиллагааг аюулгүй хангах зорилготой.

### Нисэх буудлын ангилал

Нисэх онгоцны буудал олон улсын стандарт болон дүрмийг дагаж мөрдөх хэрэгтэй.

#### НИСЭХ БУУДЛЫН АНГИЛАЛ

1-р ХҮСНЭГТ

Зэрэглэл	Нисэх онгоцны төрөл	Нислэгийн тоо (өдөрт)	Зурвас (м)	Буудлын талбай (м <sup>2</sup> )	Ачааны талбай (м <sup>2</sup> )	Паркинг (зогсоол)	ICAO стандарт
1-р зэрэглэл	Жижиг оврын онгоц (Cessna 172)	10-20	800-1200	500-1000	100-200	5-10	ICAO Annex 14, Volume I
2-р зэрэглэл	Дунд оврын онгоц (Bombardier Q400)	20-40	1200-1800	1000-3000	200-400	10-20	ICAO Annex 14, Volume I
3-р зэрэглэл	Том оврын онгоц (Boeing 737)	40-60	1800-2500	3000-7000	400-800	20-30	ICAO Annex 14, Volume I
4A	Маш том оврын онгоц (Airbus A320)	60-100	2500-3000	7000-10000	800-1200	30-50	ICAO Annex 14, Volume I
4B	Маш том оврын онгоц (Boeing 777)	60-100	3000-3500	10000-15000	1200-1600	50-100	ICAO Annex 14, Volume I
4C	Маш том оврын онгоц (Airbus A330)	60-100	3500-4000	15000-20000	1600-2000	100-150	ICAO Annex 14, Volume I
4D	Маш том оврын онгоц (Boeing 787)	60-100	4000-с дээш	20000-с дээш	2000-с дээш	150-с дээш	ICAO Annex 14, Volume I

ICAO (International Civil Aviation Organization) нь нисэх онгоцны буудлын стандарт, шаардлагыг тодорхойлсон. Нисэх онгоцны буудлуудын зэрэглэлийг ICAO стандартын дагуу ангилдаг [6] (1-р хүснэгт).

Нислэгийн тоо - Нисэх онгоцны буудалд өдөрт хийж болох нислэгийн тоо.

Зурвас - Нисэх онгоцны буудлын нисэх онгоц буух зурвасын урт.

Буудлын талбай - Зорчигчид болон үйлчилгээний зориулалттай байршлын нийт талбай.

Ачааны талбай - Ачаа тээврийн үйлчилгээний зориулалттай талбай.

Паркинг - Нисэх онгоцны буудалд зогсоолын тоо.

1-р хүснэгт нь ICAO-ийн стандартын дагуу нисэх онгоцны буудлуудын шаардлага, хүчин чадал, үйлчилгээг нэгтгэн харуулсан. Тухайн улсын нөхцөл, шаардлагаар эдгээр параметрууд өөрчлөгдөж болдог. Агаарын хөлгийн ангиллыг ICAO стандартын дагуу 4A, 4B, 4C, 4D зэрэглэлээр ангилах нь нисэх онгоцны хүчин чадал, технологи, ашиглалтын зориулалтаас хамаарна (2-р хүснэгт).

#### НИСЭХ ОНГОЦНЫ АНГИЛАЛ

2-р ХҮСНЭГТ

ангилал	Нисэх онгоц	Жин, кг	Нислэгийн хурд, км/цаг	Суудал	Нислэгийн зай, км
4C	Embraer 190	35000	850	90-114	4500
4C	Boeing 737	79000	842	162-189	5500
4C	Airbus A320	77000	840	140-240	6500
4D	Boeing 777	242000	905	314-396	14000
4D	Airbus A330	230000	860	250-300	13000
4D	Boeing 787	250000	913	242-290	14800

Энэ ангилал нь агаарын хөлгийг тодорхойлох, стандартчилах, зах зээлийн судалгаа, нисэх онгоцны парк, агаарын тээвэрлэлт зэрэг олон зорилгоор ашиглагддаг.

#### V. ӨМНӨГОВЬ АЙМАГ ДАХЬ “ГУРВАН САЙХАН” НИСЭХ БУУДЛЫГ 4D АНГИЛАЛД ӨРГӨТГӨХ

Өмнөговь аймгийн “Гурван сайхан” нисэх буудлыг 3C ангиллаас 4D ангиллын шинэ нисэх онгоцны буудал руу шилжүүлэх:

*Байгууллагын хүчин чадал*

4D ангиллын нисэх буудалд нэмэлт аэродромын үйлчилгээ, аюулгүй байдал, техник үйлчилгээ шаардлагатай. Зорчигчийн танхим, ачаа тээшний үйлчилгээ, аюулгүй байдлын шалгалт зэрэг байгууламж ийг шинэчлэх шаардлагатай.

*Техникийн хүчин чадал*

4D ангиллын нисэх буудалд ихэнхдээ 3,000 метрээс дээш урт хөөрч буух зурвас шаардлагатай. Шөнийн нислэгийн тоног төхөөрөмж: “Луч-2” системийн хүчин чадлыг шинэчилж, шөнийн нислэгийн аюулгүй байдлыг сайжруулах хэрэгтэй. Нислэгийн удирдлагын шинэ тоног төхөөрөмж, программ хангамжийн шинэчлэл шаардлагатай.

*Нислэгийн аюулгүй байдал*

4D ангиллын нисэх буудалд зорчигчийн аюулгүй байдлын стандартыг өндөрсгөх, аюулгүй байдлын тоног төхөөрөмжийг сайжруулах шаардлага гарна. Олон улсын нисэхийн стандартад нийцсэн, нарийвчилсан төлөвлөгөө боловсруулна.

*Нислэгийн үйлчилгээ*

4D ангиллын нисэх буудалд өдөрт 10-20 нислэг хүлээн авах хүчин чадалтай байх шаардлагатай. Ачаа тээшний үйлчилгээний хүчин чадлыг нэмэгдүүлэх шаардлагатай.

**ГУРВАН САЙХАН НИСЭХ БУУДЛЫГ 4D АНГИЛАЛД ӨРГӨТГӨХ ТООЦОО**

3-р ХҮСНЭГТ

Үзүүлэлт	Тайлбар	Зардал (ам.доллар)
<b>1. Нисэх зурвас өргөтгөх зардал</b>	Зурвас урт нэмэгдэнэ (2.4 км → 3.6 км)	15 сая ам.доллар/км
Одоогийн нисэх зурвас нь 2.4 км урттай. 4D ангилалд хүрэхийн тулд энэ зурвасыг 3.6 км болгож өргөсгөх шаардлагатай.	Урьдчилсан тооцоолоор: 1,200 м нэмэгдэнэ	18 сая ам.доллар
<b>2. Техникийн үйлчилгээ</b>	-Аюулгүй байдал, холбоо, гэрэлтүүлэг зэрэг тоног төхөөрөмжүүд (хяналт, нисэх буудлын холбооны систем): 5 сая ам.доллар -Гэрэлтүүлэг, радиолокаци: 2 сая ам.доллар -Нисэх буудлын аюулгүй ажиллагаа, ажлын зардал: 3 сая ам.доллар	10 сая ам.доллар
<b>3. Барилга байгууламжийн өргөтгөл</b>	-Терминалын өргөтгөх зардал: 3 сая ам.доллар -Хүлээлгийн талбай, ачаа тээшний хэсгийн өргөтгөл: 2 сая ам.доллар шаардлагатай.	5 сая ам.доллар
<b>4. Нэмэлт тоног төхөөрөмж</b>	Агаарын тээвэр, техникийн үйлчилгээний шинэчлэлт, тоног төхөөрөмжийн зардал.	3 сая ам.доллар
<b>Нийт өртөг</b>	<b>Бүх зардал</b>	<b>36 сая ам.доллар</b>

“Гурван сайхан” нисэх буудлыг 4D ангилалд өргөтгөхөд шаардлагатай нэмэлт тоног төхөөрөмж, барилга байгууламжийн зардлыг тооцоолон 3-р хүснэгтэд харуулав. Эдгээр зардлууд нь тухайн нисэх буудлын барилга байгууламжийн төсөв, стандарт, ханш зэрэг хүчин зүйлсийн үндсэн дээр тооцогддог. Нисэх буудлын зурвасыг өргөсгөх нь хамгийн том зардал бөгөөд агаарын тээвэрт аюулгүй байдал, үр

ашигтай үйл ажиллагааг хангахад чухал үүрэгтэй. Техникийн шинэчлэлт, аюулгүй байдал, тоног төхөөрөмжүүд нь өндөр стандарттай ба 4D ангилалд орох нисэх буудал нь олон улсын нислэгийн үйл ажиллагааг хариуцдаг. 4D ангилалд орох нисэх буудлын терминал болон үйлчилгээний талбай, хүлээлгийн талбай, ачаа тээшний хэсэг, ажилчдын байр, үйлчилгээний байгууламжуудыг өргөтгөх хэрэгтэй.

Нисэх буудлын 4D ангилалд өргөжүүлэхэд шаардлагатай нийт зардал нь 36 сая ам.доллар. Бодит тооцоолол, төслийн зураг төсөл, инженерийн судалгаа, салбарын стандартуудыг ашиглан нарийвчилсан тооцоолол хийх шаардлагатай.

**VI. ЦААШИД ХИЙХ СУДАЛГААНЫ ЧИГЛЭЛ**

Өмнөговь аймгийн “Гурван сайхан” нисэх буудлыг 4D ангилалд шилжүүлэх нь олон улсын нислэгүүдийг хүлээн авах чадварыг нэмэгдүүлнэ. Үүний тулд инженерийн зураг төсөл, аюулгүй ажиллагаа зэрэг хүчин зүйлсийг нарийвчилсан төлөвлөгөө гарган хэрэгжүүлэх шаардлагатай.

**СУДАЛГААНЫ ЧИГЛЭЛҮҮД**

4-р ХҮСНЭГТ

№	Судалгааны чиглэл	Үйл ажиллагаа
1	Техникийн шаардлага, инженерийн судалгаа	Нисэх зурвас өргөтгөх боломж, геодезийн нөхцөлийг тодорхойлох, Шөнийн нислэгийн аюулгүй байдал, гэрэлтүүлэг
2	Эрчим хүч, байгаль орчны нөлөө	Байгаль орчны нөлөөлөл, Агаарын бохирдол, хог хаягдлын менежментийн судалгаа хийх. Эрчим хүчний хэрэглээ, Тогтвортой эрчим хүчний хангамж, салхи, нарны эрчим хүч, усан хангамжийн судалгаа.
3	Нисэх буудлын хүчин чадлыг үнэлэх	Зорчигчийн эрэлт, зорчигчдын тоог тооцох, Говийн бүсийн уул уурхайн төсөл, эдийн засгийн өсөлт, тээвэр, ложистикийн хэрэгцээ.

4-р хүснэгтэд “Гурван сайхан” нисэх буудлын олон улсын 4D ангилалд шилжих судалгааны чиглэлүүд болон цаашид хийх ажлуудыг харуулав. Эдгээр судалгааны үр нь “Гурван сайхан” нисэх буудлын аюулгүй байдал, үйл ажиллагааны хүчин чадал, экологийн нөлөөлөл, мөн эдийн засгийн ач холбогдлыг тодорхойлоход туслах болно.

**ДҮГНЭЛТ**

Нисэх буудлыг 3C ангиллаас 4D ангилал руу шилжүүлэх нь техник технологи, стандарт, хүний нөөц, санхүүжилт зэрэг олон хүчин зүйлээс хамаарах бөгөөд Өмнөговь аймгийн “Гурван сайхан” нисэх буудлын үйл ажиллагааг олон улсын стандартын дагуу өргөжүүлэх, аюулгүй байдал, үйлчилгээний чанарыг сайжруулахад чухал ач холбогдолтой. Нисэх буудлын бүтэц, үйл ажиллагаа нь ИCAO-ын шаардлагад нийцсэн байх шаардлагатай. Энэ нь аюулгүй байдал, үйлчилгээний чанарыг сайжруулна.

4C, 4D ангиллын нисэх буудалд шаардлагатай техник, тоног төхөөрөмжийг шинэчилснээр нислэгийн аюулгүй байдал, үйлчилгээний чанар сайжирна.

Өмнөговь аймгийн “Гурван сайхан” нисэх буудал 4D ангиллын олон улсын нисэх буудал болсноор гадаадын хөрөнгө оруулалт, аялал жуулчлалын орлого нэмэгдэх боломжтой. Энэ нь бүс нутгийн эдийн засгийг хөгжүүлэхэд чухал үүрэгтэй.

#### **АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ**

- [1]. Монгол Улсын Засгийн газрын 2020-2024 оны үйл ажиллагааны хөтөлбөр, Монгол Улсын Их Хурлын тогтоол 2020 оны 08 сарын 28 өдөр, Дугаар 24, Улаанбаатар хот

- [2]. <https://montsame.mn/en/read/314719>  
[3]. <https://ncac.mcaa.gov.mn/mn/news/post/892>  
[4]. <https://mrt.gov.mn/i/3744>  
[5]. <https://vip76.mn/p/96430?year=2024&id=11382>  
[6]. ICAO Annex 14, Volume I  
[7]. Монгол Улсын Засгийн газрын 2023 оны 7 дугаар сарын 5-ны өдрийн 253 дугаар тогтоол  
[8]. Агаарын навигаци-2024 стратеги төлөвлөгөө, 2017-09-22, ИНЕГ-ын даргын А-605-р тушаал  
[9]. Иргэний нисэхийн тухай хуулийн хэрэгжилтийн үр дагаварын үнэлгээний тайлан, 2022.  
[10]. Статистикийн Эмхэтгэл, Иргэний Нисэхийн Ерөнхий Газар 2023  
[11]. John Doe. Aviation Communication Systems and Technologies. AirTech Publishing, 2021.  
[12]. Jane Smith. Aircraft Communication and Navigation Systems. Aerospace Solutions, 2022.

## ЭНГИЙН БҮТЭЦТЭЙ ХОС ТУЙЛШРАЛТАЙ ЦАХИЛГААН СОРОНЗОН ЭНЕРГИ ХУРИМТЛУУЛАХ ГАДАРГУУГИЙН СУДАЛГАА

Амгаланбаатарын БАТНЯГТ<sup>1</sup>, Пүрэвдоржийн УУГАНБАЯР<sup>2</sup>

<sup>1</sup>-Монгол улс, Улаанбаатар, Шинжлэх Ухаан Технологийн Их Сургууль, Холбооны салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: p.uuganbayar@must.edu.mn<sup>1\*</sup>*

**Хураангуй:** энгийн бүтэцтэй хос туйлшралтай цахилгаан соронзон энерги хуримтлуулах гадаргууд хийсэн тоон анализ

**Түлхүүр үг:** Хос туйлшрал, цахилгаан соронзон долгион, энерги хуримтлуулах гадаргуу, мета гадаргуу

### I. УДИРТГАЛ

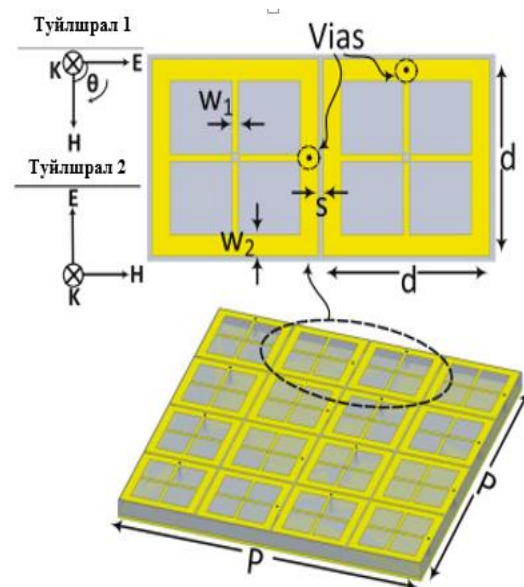
Өөрийн судалгааны хүрээнд цахилгаан соронзон долгионы энергийг цуглуулах хос туйлшралтай мета гадаргуу, түүний загвар дизайныг танилцуулж байна. Тус загвар нь ажлын давтамж 2.4 GHz байх үед тусгалын янз бүрийн өнцгүүдээс энерги цуглуулахын тулд хувьсах гүйдлийн чиглүүлэгч нүх буюу (via) холболттой зэргэлдээ үүрнүүдээс бүтсэн 4x4 супер үүрийг ашиглан соронзон долгион цуглуулна. Ингэснээр хувьсах гүйдлийг тогтмол гүйдэл болгон хувиргах процессийн үг дүнг 80%-90% болж сайжруулж байгааг харуулахыг зорьсон.

### II. ЭНЕРГИ ХУРИМТЛУУЛАХ ГАДАРГУУГИЙН ЗАГВАР

Хос туйлт энерги цуглуулагчийн нэгж үүр нь 4x4 супер үүрнээс бүрддэг. Супер үүр нь  $\tan\delta = 0.0009$  алдагдлын тангенстай,  $\epsilon_r = 2.2$  диэлектрик тогтмолтой 3.175 мм зузаантай RT/duroid 5880 Рожерс диэлектрик субстрат дээр байрласан байдаг. Долгион үүрээр дамжин өнгөрөхөөс сэргийлж газрын хавтгайг ашигладаг. Үүр тус бүр нь газрын хавтгай болон хамгийн дээд талын давхарга хоёрын дунд байрласан ачааллын эсэргүүцэлтэй байх бөгөөд энэ нь хэлхээ хоорондын “гүүр” буюу чиглүүлэгч нүх (via)-р холбогдсон байдаг. Зэргэлдээх үүр тус бүрийн хувьд чиглүүлэгч нүх (via)-ны байршил өөр өөр байх нь ялгаатай өнцгүүдээс ирсэн долгионыг барих боломжыг олгодог. Үүр тус бүр нь  $d=17$  мм,  $w_1=0,6$  мм,  $w_2=1,85$  мм,  $s=0,5$  мм хэмжээтэй, зэсийн зузаан  $t=35$  мкм, хажуугийн урт нь  $P=70$  мм, эзлэх талбай  $A=49$  см<sup>2</sup> байна. Супер үүрэнд хэдэн үүр байх нь тэжээлийн хэлхээний хувьд маш чухал.

Зураг 1-г чиглүүлэгч нүх буюу (via) нь өөр өөр газар байрласан хоёр үүр бүхий бүтэц болон хоёр туйлт туйлшралыг харуулсан байна. Өөрөөр хэлбэл ялгаатай туйлшрал бүхий 2 үүр нь нийлж нэг бүлэг болон ажиллах бөгөөд цаашлаад үелэн давтагдсан олон тооны хос үүрүүдийн тусламжтайгаар босоо болон хөндлөн туйлшралтай долгионуудыг нэг ижил хугацаанд

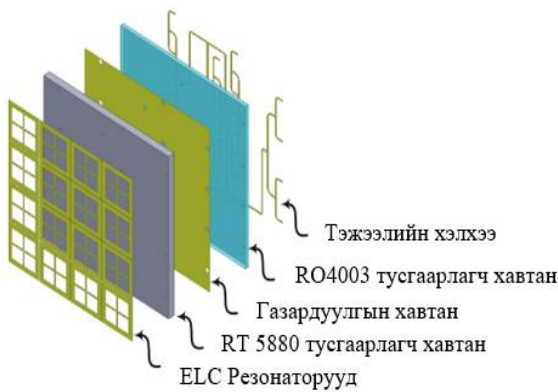
орчны радио энергээс цуглуулж, цуглуулсан энергээ цааш нь хүчдэл болгон хувиргах байдлаар энэ бүтэц ажиллах юм.



Зураг 1 Мета материал энерги цуглуулагч төхөөрөмжийн супер үүрийн схем

Үүний тулд зөвхөн орчноос энерги цуглуулах метагадаргуугаас гадна тэжээл хуваарилах хэлхээ, шулуутгах хэлхээ зэргийг нэмж загварчилснаар орчны радио долгионоос эцсийн тогтмол хүчдэлийг гарган авах бүтэц цогцоороо бэлэн болж байгаа гэж ойлгож болно. Зураг 2-г энэхүү цогт энерги хуримтлуулах гадаргуугийн бүтцийг нарийвчлан давхарга нэг бүрээр нь задлан харуулсан байгааг харж болно.

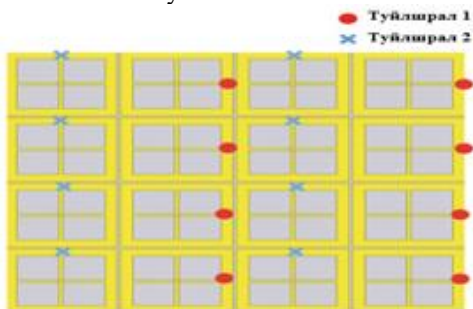
Үүнд: метагадаргууг бүрдүүлж буй үелсэн бүтэц бүхий метал резонаторууд, резонаторуудыг газардуулгын хавтангаас тусгаарлаж буй тусгаарлагч хавтан (RT 5880), метал газардуулга хавтан, газардуулгын хавтанг тэжээлийн хэлхээнээс тусгаарлаж буй тусгаарлагч хавтан (RO4003), тэжээлийн хэлхээ зэрэг багтана.



Зураг 2 Метаматериал ашигласан энерги хуримтлуулагч гадаргуугийн бүрэлдэхүүн хэсгүүд

Орчны радио энергийг цуглуулж хуримтлуулах системд зориулсан олон төрлийн антеннууд хийгдсэн, судлагдсан байдаг ч ихэвчлэн долгионыг туйлшралаар нь ялган цуглуулахад чиглэж загварчлагдаагүй учир тухайн давтамж дээр орчноос энерги хуримтлуулж түүнийгээ цахилгаан энерги болгох процесст оруулах үйл явцын ашигт үйлийн коэффициент нь харьцангуй сул байдаг.

Энд яригдаж байгаа бүтцийн хувьд ялгаатай туйлшралыг хүлээн авах хос үүрийн комбинацаар босоо болон хэвтээ туйлшралтай долгионуудыг туйлшралаар нь ялгаж хүлээн авч, цуглуулж байгаа тул энерги цуглуулах ашигт үйлийн коэффициент нь илүү сайжирсан байгаа юм. Гэхдээ энэ загварт ялгаатай 2 туйлшралтай долгионуудыг хүлээн авч цааш хуваарилах тэжээлийн хэлхээ, түүний зохиомж ихээхэн чухал байна.

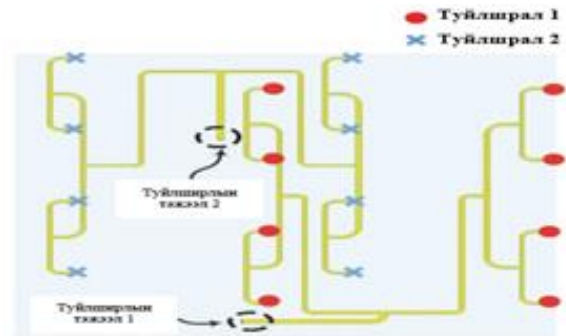


Зураг 3 Энерги хуримтлуулах гадаргуугийн тэжээлийн цэгүүдийн байршил (урд тал)

Зураг 3-т энерги хуримтлуулах метагадаргуугаар цуглуулагдсан босоо болон хэвтээ туйлшралтай долгионуудын энэргийн цааш хуваарилах тэжээлийн хэлхээтэй холбогдох цэгүүдийн байршлыг туйлшралаар нь ялган метагадаргуугийн нүүрэн тал буюу урд талаас харуулсан байна.

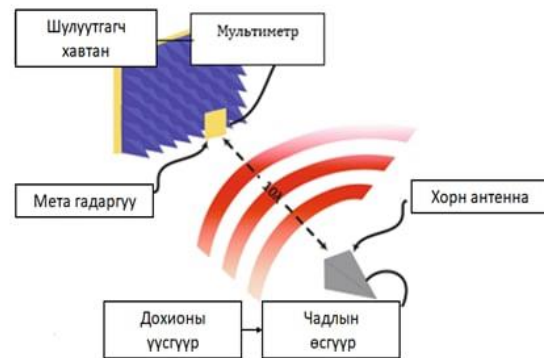
Өөрөөр хэлбэл орчин дахь босоо болон хэвтээ туйлшралтай долгионуудыг ялган цуглуулж цааш тэжээлийн хэлхээнд өгөх цэгүүдийг хос үүр тус бүрт улаан блон цэнхэр өнгийн тэмдэгтээр тэмдэглэжээ.

Харин Зураг 4-ийн хувьд тэжээлийн хэлхээ байрлах ард талаас буюу метагадаргуугийн эсрэг талаас харуулсан бөгөөд мөн хос үүр тус бүрээс ялгаатай туйлшралтай энерги цуглуулж авах цэгүүдийг өмнөхийн адил өнгөөр ялгаж харуулсан байна.



Зураг 4 Энерги хуримтлуулах гадаргуугийн тэжээлийн цэгүүдийн байршил (ард тал)

Санал болгож байгаа радио долгионоос энерги хуримтлуулах төхөөрөмжийн ажиллагааг туршихын тулд Зураг 5-д харуулсан зарчмаар турших боломжтой юм.



Зураг 5 Энерги хуримтлуулах метагадаргуугийн туршилтын схем

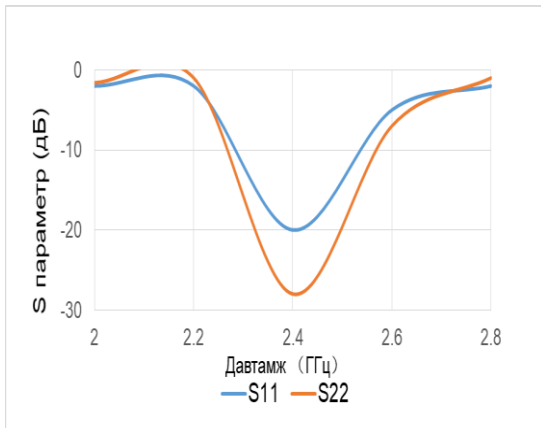
Энд эхлээд тусгайлан байгуулсан цахилгаан соронзон долгионы орчинд тодорхой давтамжийн долгионыг генератороос үүсгэж, чадлын өсгүүрээр өсгөн чиглэлтэй антенаар цацах юм. Хүлээн авах талд санал болгож байгаа метагадаргуу байрлах бөгөөд чөлөөт орон зайд цацсан радио долгионы энергийг цуглуулж авах юм. Цуглуулсан энергийг тэжээл хуваарилах хэлхээгээр дамжуулах шулуутгах схемд өгсөнөөр тогтмол хүчдэл гарч түүнийг хэмжүүрийн багажаар хэмжих боломжтой болно.

### III. РАДИО ДОЛГИОНЫГ ТОГТМОЛ ГҮЙДЭЛ БОЛГОН ХУВИРГАХ

Судалгааны ажлаар санал болгож энгийн бүтэцтэй хос туйлшралтай цахилгаан соронзон энерги хуримтлуулах гадаргууг дараах аргуудаар тоон анализ хийн шинжиллээ.

**А. Цацрагийг АС хувьсах гүйдэл болгон хувиргах ажлын үр дүнд хийсэн тоон анализ**

Нэгж үүрийг судлахын тулд бүрэн долгионы симулятор HFSS-г ашигласан. Супер үүрний шингээлтийг тооцоолохын тулд туйлшрал тус бүрийн тархалтын параметрийг ашиглана.

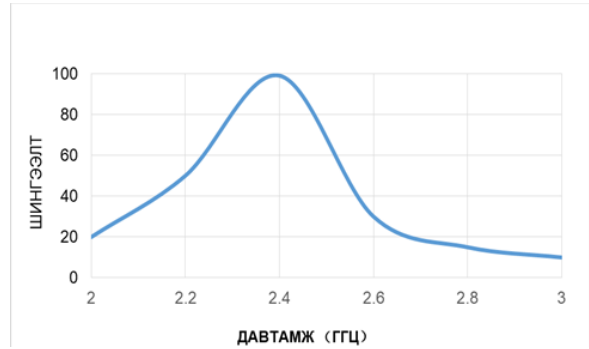


Зураг 6 Метагадргуугийн S<sub>11</sub> параметрийн үр дүн /туйлшрал тус бүрээр/

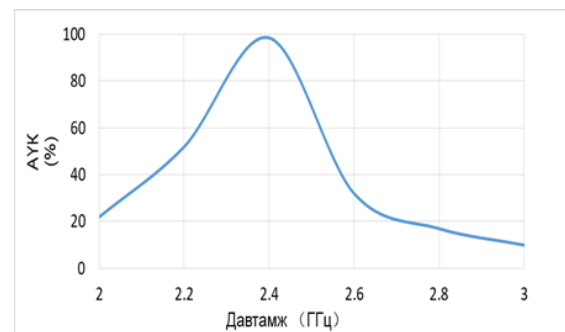
Супер үүрний шингээлтийг  $A(\omega)=1-[S_{11}]^2-[S_{21}]^2$  дараах томъёогоор тооцоолж гаргах бөгөөд газрын хавтгай байгаагаас шалтгаална  $[S_{21}]^2=0$ . Үүр тус бүрийн ачааллын эсэргүүцлийн хязгаар нь  $R=175 \Omega$  бол супер үүр нь ойролцоогоор 2.4 GHz резонансын давтамжтай оролтын долгионыг бүрэн шингээдэг. Системд шингээгдсэн болон тархсан долгион нь субстрат материалд алдагдахаас илүүтэй түүнийг хэрэгтэй зориулалтын дагуу ашиглах нь чухал бөгөөд системд хадгалагдсан энергийг дараа нь диод буюу шулуутгагч хэлхээгээр АС хувьсах гүйдлийг DC тогтмол гүйдэл болгон хувиргадаг. Дараах графикт нэгж үүрийн шингээлтийг давтамжийн функцээр харууллаа.

Зураг 7-д метагадргуугийн супер үүрийн шингээлтийг хувиар илэрхийлэн харуулж байна. Шингээлтийн ашигт үйлийн коэффициент нь 2.4 ГГц давтамж дээр 98 хувь үзүүлэлттэй байгаа нь загварчилсан метагадргуу нь орчны радио долгионыг туйлшрал тус бүрийн хувьд өндөр үзүүлэлттэй хүлээн авч байгааг илэрхийлж байна.

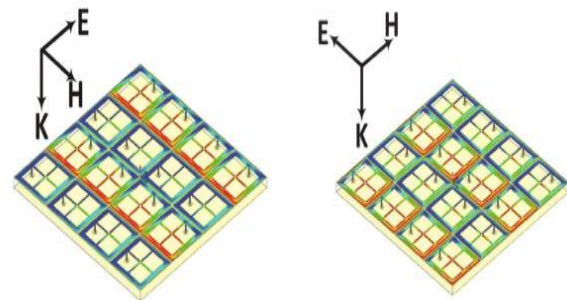
Зураг 7 болон Зураг 8 -д зурагт Зураг-1-т үзүүлсэн босоо болон хэвтээ туйлшралын үр дүнг харуулсан бөгөөд супер үүр нь өндөр симметртай байдгаас шалтгаалан дэд зураг тус бүр дээр зөвхөн нэг муруйг харуулсан. Өөрөөр хэлбэл туйлшрал тус бүрийн хувьд симуляцийн үр дүн яв цав таарч давхцаж байгаа юм.



Зураг 7 Супер үүрийн шингээлт /давтамжийн функцаар/



Зураг 8 Супер үүрийн ашигт үйлийн коэффициент (давтамжийн функцаар)



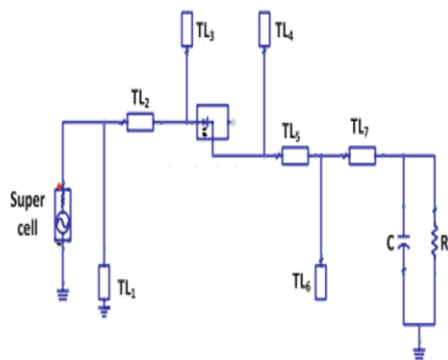
Зураг 9 Супер үүр дээрх цахилгаан соронзон долгионы тархалт

Графикаас харахад, цахилгаан соронзон орон зөвхөн улаан өнгөөр дүрсэлсэн 8 үүрт хүчтэй нөлөө үзүүлж байна. Цахилгаан соронзон оронтой паралель чиглүүлэгч нүх буюу via-тай, улаан өнгөөр тэмдэглэгдсэн 8 үүр нь хоёр туйлшралын хоёулангынх нь хувьд цахилгаан соронзон орны өндөр концентраттай байгаа нь графикаас тодорхой харагдаж байна. Цуглуулсан эрчим хүчний 98% нь зөвхөн 8 үүрээр дамжин тархаж байгааг туйлшрал тус бүрийн симуляцаас ажиглаж болно. Энергийн тархалтад үүрэг гүйцэтгээгүй нөгөө 8 үүрээр дамжин өнгөрч байгаа цахилгаан гүйдэл нь нийт энергийн шингээлтэд чухал хувь нэмэр оруулж байгаа үүрнүүдтэй холбогдсон. Ингэснээр тэжээлийн сүлжээ нь бүх 16 үүрнээс бус харин туйлшрал тус бүрд зөвхөн 8 үүрнээс энерги хуримтлуулах боломж олгон тэжээлийн сүлжээг улам хялбар энгийн болгож байна. Сувагчлалын механизмыг ийнхүү хялбаршуулснаар тэжээлийн

сүлжээн дэх эрчим хүчний алдагдлыг багасгаж байна. Үүнийг хийснээр зэс замын тоо багасна.

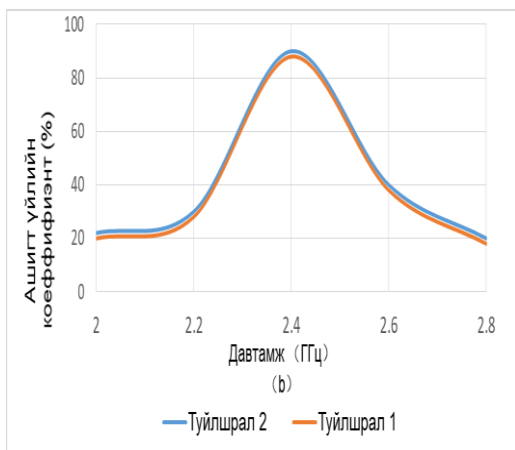
**В. AC хувьсах гүйдлийг DC тогтмол гүйдэл болгон хувиргах ажлын үр дүнд хийсэн тоон анализ**

Хувьсах гүйдлийг тогтмол гүйдэл болгон хувиргах гол хэсэг нь шулуутгах хэлхээ юм. Тжр дундаа 2,4 ГГц давтамж дээр ажиллах шулуутгах хэлхээг загварчлах нь энэ ажлын нэг хэсэг юм. Зураг 10-т шулуутгах хэлхээг ADS симуляцын програм ашиглан загварчилсан байгаа байдлыг харууллаа. Энд метагадаргууг төлөөлүүлэн ADS програмын сан дах Super cell элементийг ашиглан симуляц хийсэн.



Зураг 10 Шулуутгах хэлхээг Keysight ADS өндөр давтамжийн хэлхээний симуляцийн програм дээр угсарсан байдал

Зураг 11-т супер үүр болон шулуутгах хэлхээг холбосны дараах симуляцийн үр дүнг харууллаа.



Зураг 11 Шулуутгах хэлхээг метагадаргуутай холбосон үеийн энерги хуримтлуулах АУК

Шулуутгах хэлхээг холбохоос өмнө энерги хуримтлуулагч гадаргуун ашигт үйлийн коэффициент 98 хувь байсан бол шулуутгах хэлхээг холбосноор 90 хувь болон буурч байгаа нь зургаас харагдаж байна. Гэсэн хэдий ч энэ үзүүлэлт

нь бусад энэ төрлийн төхөөрөмжүүдтэй харьцуулахад өндөр байгаа юм.

**ДҮГНЭЛТ**

Бид олон туйлшралаас бичил долгионы энерги цуглуулах чадалтай загварыг танилцууллаа. 4x4 супер үүрийг бүтээж, цацрагийг AC буюу хувьсах гүйдэл болгон хувиргах максимум хүчин чадлыг тодорхойлсон. Цуглуулсан энергийг AC болон DC сувагчлалын сүлжээг нэгтгэсэн гибрид сувагчлалын механизмыг ашиглан ачааллын эсэргүүцэл рүү дамжуулсан. Үүний дараа цуглуулсан AC хувьсах гүйдлийг DC тогтмол гүйдэл болгон хувиргахын тулд шулуутгагчийг өөр өөр давхарга дээр тэжээлийн сүлжээтэй холбосон.

Санал болгож буй энерги цуглуулагч нь өөр өөр туйлшралаас ирсэн долгионыг маш сайн барих чадвартай хэдий ч нарийн зурвастай байгаа нь түүний сул тал болж байна.

**АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ**

[1]. Zhai, S, et al. Inverse doppler effects in broadband acoustic metamaterials. Scientific Reports 6 (2016)  
 [2]. Lezec, H J., Dionne, J. A & Atwater, H. A. Negative refraction at visible frequencies. Science 316, 430–432 (2007)

## СҮЛЖЭЭНИЙ ЧАНАРЫН ҮЙЛЧИЛГЭЭНИЙ ХАРЬЦУУЛСАН СУДАЛГАА

Цогнэмэх ЦОГТБААТАР<sup>1</sup>, Тогоохүү БУЛГАНМАА<sup>2</sup>, Ямхин ДАШДОРЖ<sup>3</sup>

<sup>1</sup> Монгол улс, Улаанбаатар, Мобинет ХХК

<sup>2</sup> Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ, аюулгүй байдлын салбар

*Холбогдох зохиогчийн и-мэйл хаяг: dashdorj@must.edu1\**

**Хураангуй:** Энэ судалгаагаар интернэт үйлчилгээгээр хангаж буй интернэтийн үйлчилгээ үзүүлэгч компанийн сүлжээний чанарыг хэрхэн шалгах, шинээр нэвтэрч буй 5G сүлжээний чанар, холболтын төрөл бүр дээр (QoS)-ын олон улсын стандартыг хангаж байгаа эсэхийг шалгах судалгаан дээр үндэслэсэн. Хэрэгжүүлэлтийг хийхдээ сүлжээгээр дамжин цуглуулсан өгөгдөл Wireshark, iPerf, PingPlotter хэрэгслийг ашиглан дүн шинжилгээ хийж үр дүнг тодорхойлсон. Судалгааны ажлын үр дүнгээс харахад эцсийн хэрэглэгч дээр үйлчилгээний чанар ямар түвшинд байгааг олон улсын стандартын хангаж чадаж байгаа эсэхийг шалгаж, хэрэглэгч өөр дээрх хэрэгслүүдийн тусламжтай өөрийн сүлжээний чанарын шалгаж үзэх боломжтойг харуулсан. Мөн газар зүйн байрлал болон гадаад улсууд руу холбогдож байгаа интернэтийн гарцууд өөр өөр байгааг харуулахыг зорьсон. Бидний хэрэгжүүлэлтээр Монгол улс дотор серверүүд рүү туршилт хийхэд (хоцролт 22.4мс) (хэлбэлзэл 18мс) сүлжээний чанар маш сайн, Герман улс руу хийхэд (хоцролт 133.3мс), (хэлбэлзэл 125-200мс) байгаа нь сүлжээний чанарын үзүүлэлтүүд дунд түвшинд байгааг ялган харуусан.

**Түлхүүр үг:** Үйлчилгээний чанар (QoS), 5G сүлжээ, үйлчилгээний чанарын хэмжүүр үзүүлэлтүүд, стандарт, харьцуулалт (ITU-T, IETF RFC, ISO, MPLS)

### I. УДИРТГАЛ

Харилцаа холбооны ихэнх төхөөрөмжүүд интернэт протокол(IP) сууртай технологи дээр суурильж байгаатай холбоотой сүлжээний тасралтгүй найдвартай ажиллагаа хамгийн чухал зүйл болсон. Сүлжээний найдвартай ажиллагаа нь бэлэн байдал, гүйцэтгэл, аюулгүй байдал гэсэн хэсгүүдээс бүрдэнэ. Сүлжээний бэлэн байдал нь тухайн сүлжээний систем, үйлчилгээ, дэд бүтэц нь ашиглагдаж байгаа эсвэл шаардлагатай үедээ ажиллах боломжтой байдал юм. Энэ нь хэрэглэгчид болон үйлчилгээнд нэвтрэх, мэдээлэл дамжуулах, системийн хэвийн ажиллагааг хангахтай холбоотой. Сүлжээний бэлэн байдлыг хангахын тулд сүлжээний тоног төхөөрөмж, программ хангамжийн алдааг засах, нөөцийг хуваарилах, давхарласан системүүдийг бий болгох зэрэг олон арга хэмжээг авч хэрэгжүүлдэг. Сүлжээний бэлэн байдлыг хэмжихийн тулд дараах зүйлсийг авч үздэг. Үүнд:

1. **Хэрэглэгчийн нэвтрэх боломж:** Сүлжээ нь хэрэглэгчид ямар ч үед нэвтрэх боломжтой байх хэрэгтэй.

2. **Үйлчилгээний тасалдал:** Сүлжээний үйлчилгээ удаан хугацаагаар тасалддаггүй байх.

3. **Гүйцэтгэл:** Сүлжээний хурд, хариу өгөх хугацаа зэргийг мөн тооцоолдог. Сүлжээний гүйцэтгэл нь сүлжээний системийн хурд, үр ашиг, итгэлцлийн түвшинг тодорхойлох параметруудийг агуулдаг. Сүлжээний гүйцэтгэлийг сайжруулахын тулд хэт ачаалалтай үед төхөөрөмжийг нэмэгдүүлэх, сүлжээний архитектурыг сайжруулах, программ хангамжийн алдааг засах зэрэг арга хэмжээг авч хэрэгжүүлдэг.

Үйлчилгээний чанар (Quality of Service) гэдэг нь сүлжээ эсвэл харилцаа холбооны системийн ерөнхий гүйцэтгэл, ялангуяа өгөгдөл дамжуулалтыг үр

ашигтайгаар удирдаж, тодорхой үйлчилгээнд тавигдах гүйцэтгэлийн шаардлагыг хангасан байх чадварыг хэлнэ. Үйлчилгээний чанар нь сүлжээгээр дамжуулж буй янз бүрийн төрлийн өгөгдлийн урсгалуудыг зохицуулан, хэрэглэгчдэд хүлээгдэж буй чанарыг хангах зорилготой. Жишээ нь, видео дуудлага, дуу дамжуулалт зэрэг тасралтгүй урсгал шаарддаг үйлчилгээнүүдэд хугацаа алдалт болон өгөгдлийн алдагдлыг бууруулахад тусалдаг. Үйлчилгээний чанарыг судлах болсон нь Монгол улсын интернэтийн үйлчилгээ үзүүлэгч компанийн үйлчилгээ нь олон улсын стандартууд, шаардлагыг хангаж байгаа эсэхийг үйлчилгээний чанарын шалгалт (QoS Testing), гүйцэтгэлийн үнэлгээ (Performance Evaluation) олон улсын арга аргачлалаар туршилт хийх хэрэгтэй байна.

### II. ҮЙЛЧИЛГЭЭНИЙ ЧАНАРЫН ҮНДСЭН ҮЗҮҮЛЭЛТҮҮД

Үйлчилгээний чанарын тодорхойлдог хамгийн нийтлэг гүйцэтгэлийн хэмжүүрүүдийг олон улсын стандартаар баталдаг. Үүнд:

1. ITU-T Y.1541 стандарт[1]: Олон Улсын Цахилгаан Холбооны Холбоо (ITU)-ын Телекоммуникацийн Стандарчлалын Салбар (ITU-T)-аас гаргасан бөгөөд өгөгдлийн дамжуулалтын чанарын үйлчилгээний шаардлагыг тодорхойлдог. Энэхүү стандарт нь өгөгдөл, дуу, видео зэрэг төрөл бүрийн үйлчилгээний чанарыг хангахын тулд сүлжээний хоцролт, гүйцэтгэл, алдаа засах чадвар зэрэг үзүүлэлтүүдийг барих шаардлагыг тогтоосон.

2. ITU-T G.1010 стандарт[2]: Энэ стандарт нь хэрэглэгчийн туршлага дээр үндэслэн үйлчилгээний чанарын шаардлагыг тодорхойлдог. Энэхүү стандарт нь дуу, видео, өгөгдөл зэрэг харилцаа холбооны олон төрлийн үйлчилгээнд зориулж үйлчилгээний чанарын үзүүлэлтүүдийг тохируулах суурь

удирдамжийг гаргаж өгдөг. G.1010 стандарт нь дижитал үйлчилгээний хэрэглэгчдийн чанарын шаардлагыг ойлгох, хэмжих, сайжруулах үндсэн хэрэгсэл болдог ба энэ нь олон улсын түвшинд QoS шаардлагыг тогтоон, нийтлэг ойлголттой болгох чухал ач холбогдолтой.

3. RFC 4594 стандарт[3]: Энэхүү стандарт нь “Ялгавартай үйлчилгээний салбарыг тодорхойлох гарын авлага” нэртэй стандарт бөгөөд сүлжээнд өгөгдлийн урсгалыг ангилж, ангилал бүрд тохирсон үйлчилгээний чанарын шаардлагыг хангах боломжийг олгодог. Энэ стандарт нь 2006 онд (IETF) байгууллагаас гаргасан бөгөөд сүлжээнд өгөгдлийн урсгалыг үр дүнтэй хуваарилж, сүлжээний нөөцийг оновчтой ашиглах замаар ялгаатай үйлчилгээний чанарын үзүүлэлтийг хангах аргачлалыг тодорхойлдог.

**A. Хоцролт**

Бодит цагийн үйлчилгээний хувьд latency 150 мс хүртэл бол сайн гэж тооцогддог. Дунд ангилалд дуу, видео зэрэг үйлчилгээний чанарт бага зэрэг сөргөөр нөлөөлж болох ч хүлцэхүйц түвшинд байна.

1-Р ХҮСНЭГТ ҮЙЛЧИЛГЭЭНИЙ ЧАНАРЫН УТГА БОЛОН ХУВЬ

QoS Үзүүлэлт	Сайн	Дунд	Муу
<b>1 Latency (Хоцролт)</b>	≤ 150 мс	150 - 300 мс	> 300 мс
<b>2 Jitter (Хэлбэлзэл)</b>	≤ 30 мс	30 - 75 мс	> 75 мс
<b>3 Bandwidth (Өргөн зурвас)</b>	Хэрэглээнд тохирсон хангалттай өргөн зурвас	Зарим үйлчилгээ дэмжих боломжтой	Сүлжээний шаардлагыг хангахгүй
<b>4 Throughput (Дамжуулах чадвар)</b>	Bandwidth-тай ойролцоо эсвэл өндөр	Bandwidth-аас бага	Bandwidth-аас их бууралттай
<b>5 Packet Loss (Багц алдагдал)</b>	≤ 1%	1 - 3%	> 3%

$$\text{Дамжуулах хоцролт} = \frac{\text{Пакетын хэмжээ}}{\text{Сүлжээний хурд}} \quad (1)$$

$$\text{Дамжуулах хоцролт} = \frac{10,000,000 \text{ бит}}{100,000,000 \text{ секунд}} = 100 \text{ миллисекунд}$$

**Б. Хэлбэлзэл**

30 мс-ээс бага хэлбэлзэлтэй үед бодит цагийн дамжуулалт найдвартай, тасралтгүй байх боломжтой. 30-75 мс хүртэлх хэлбэлзэл нь чанарт бага зэрэг сөрөг нөлөөтэй ч зарим үйлчилгээний хувьд хүлцэж болох түвшинд тооцогддог. 75 мс-ээс дээш хэлбэлзэл нь чанарын доголдол үүсгэдэг тул муу гэж үздэг. Хэлбэлзэл дараах томъёогоор тооцдог.

$$\text{Хэлбэлзэл} = \sqrt{\frac{1}{N} \sum_{i=1}^N (D_i - D)^2} \quad (2)$$

- $N$  : Нийт өгөгдлийн тоо буюу хэмжилтийн тоо.

- $D_i$  :  $i$  –р өгөгдлийн утга

- $D$  : Бүх өгөгдлийн дундаж утга

$$(D = \frac{\sum_{i=1}^N D_i}{N})$$

- $\sum$  : Бүх  $N$  өгөгдлийн утгаас дундаж утгыг хасах замаар тухайн өгөгдлийн дундажтай харьцуулах зөрүү.

Жишээ нь: Монгол улсын сервер рүү уг томъёоны дагуу шалгахад:

Өгөгдөл: {50, 55, 60,65,70} Стандарт хэлбэлзэл нь 12 мс байна.

**В. Өргөн зурвас**

Энэ үзүүлэлт нь ашиглах хэрэгцээ болон үйлчилгээний онцлогоос хамаарна. Хангалттай өргөн зурвастай байвал сүлжээний үйлчилгээг тасралтгүй, чанартай дэмжиж чадна.

$$\text{Өргөн зурвас} = \frac{\text{Өгөгдлийн хэмжээ(битээр)}}{\text{Хугацаа (секундээр)}} = \frac{50,000,000 \text{ бит}}{10 \text{ секунд}} = 5,000,000 \text{ бит/секунд} \quad \square \square$$

**Г. Дамжуулах чадвар**

Өргөн зурвастай ойролцоо дамжуулах чадвар нь сайн, хэт бага дамжуулах чадвар нь муу гэж тооцогдоно.

$$\text{Дамжуулах чадвар} = \frac{\text{Бодитоор дамжуулсан өгөгдлийн хэмжээ}}{\text{Хугацаа}} = \frac{200,000,000 \text{ бит}}{5 \text{ секунд}} \quad (4)$$

**Д. Багц алдагдал**

Бодит цагийн үйлчилгээний хувьд багц алдагдал 1%-аас бага байх нь сайн үзүүлэлт юм. 1-3% нь хүлцэж болох түвшинд, 3%-аас дээш бол үйлчилгээ тасалдах, чанар муудах эрсдэлтэй тул муу гэж үнэлэгдэнэ

$$\text{Багц алдагдал} = \frac{\text{Алдагдсан пакетуудын тоо}}{\text{Нийт илгээсэн пакетуудын тоо}} \times 100\% = \frac{1}{1000} \times 100 = 0,1\% \quad (5)$$

**III. ҮЙЛЧИЛГЭЭНИЙ ЧАНАРЫН ХЭРЭГЛЭЭ**

Сүлжээний чанарыг баталгаажуулах шаардлагатай тохиолдолд ашигладаг бөгөөд ялангуяа дараах төрлийн үйлчилгээ, программууд дээр түгээмэл хэрэглэгддэг. Үүнд:

- Интернет протоколын дээгүүр дуудлага хийх: Дууны чанарыг хадгалах
- Видео дамжуулалт: Тасралтгүй дүрс, чанарыг хангах
- Онлайн тоглоом: Хугацааны алдагдлыг багасгах

- Бизнесийн чухал өгөгдөл: Чухал өгөгдөл дамжуулалтыг баталгаажуулах
- 5G сүлжээнд: 5G сүлжээ нэмэгдэж байгаатай холбогдуулан үйлчилгээний чанар нь асар их өгөгдлийн урсгалыг удирдахад, ялангуяа хэт өндөр нарийвчлалтай видео дамжуулалт, машинаас машин хоорондын харилцаа холбоо зэрэг программуудад чухал ач холбогдолтой юм. Трафикийг эрэмбэлэх, үйлчилгээний түвшний гэрээг хадгалахын тулд үүлэн үйлчилгээний чанарын хяналт, трафик профайл зэрэг техникийг ашигладаг. 5G-д гол зорилгын нэг нь өндөр зурвасын өргөн, бага хоцролт шаарддаг үйлчилгээнд хангалттай дэмжлэг үзүүлэх явдал юм.
- Утасгүй сүлжээнд: Энэ сүлжээ нь хязгаарлагдмал зурвасын өргөн, хэлбэлзэлтэй дохионы чанар зэрэг өвөрмөц сорилтуудтай тулгардаг. Эдгээр сүлжээнд тогтвортой гүйцэтгэлийг хадгалахын тулд дасан техникийг ашигладаг.
- Дотоод сүлжээнд:(LAN Local Area Network) Локал сүлжээнд үйлчилгээний чанар нь төхөөрөмжүүдийн хооронд хурд, ачаалал болон ашиглалтын хугацааг хянадаг.
- Өргөн бүсийн сүлжээнд:(WAN Wide Area Network) Үйлчилгээний чанар нь олон төрлийн холболт (интернэтийн шууд холболт, олон протоколын шошго дамжуулалт гэх мэт) хоорондын чанарыг хянаж, холболтын багцын урсгалын давтамж, чиглэлээр ангилал хийдэг.

#### IV. ҮЙЛЧИЛГЭЭНИЙ ЧАНАРЫН АСУУДЛУУД

- Сүлжээний халалт: Сүлжээний хэмжээ, ашиглалтын хувьд ачаалал нь ноцтой асуудал болдог. Үйлчилгээний чанар нь трафик урсгалыг хянаж, өндөр ач холбогдолтой программууд хангалттай нөөцийг хүлээн авах замаар түгжрэлийг бууруулахад тусалдаг. Өөрөөр хэлбэл нэн чухал программууд дээр ач холбогдол өгч трафикийг саадгүйгээр дамжуулах боломж олгоно.
- Өргөжих чадвар: Сүлжээг өргөжүүлэхийн хэрээр том дэд бүтэц, трафикийг зохицуулах нь улам хүндрэлтэй болж байгаа тул үйлчилгээний чанарыг удирдах нь программ хангамжаар шийдэх зэрэг илүү боловсронгуй механизмуудыг ашиглах шаардлагатай.
- Олон төрлийн сүлжээ: Орчин үеийн сүлжээнүүд, ялангуяа 5G-тэй, өргөн хүрээний төхөөрөмж, холболтыг (зүйлсийн интернэт, гар утас гэх мэт) агуулдаг. Ийм олон янзын тохиргоонд үйлчилгээний чанарыг хангах нь эцүү байдаг, ялангуяа төхөөрөмжүүд өөр өөр зурвасын өргөн болон хоцрогдолтой байх үед.

#### V. ХЭРЭГЖҮҮЛЭЛТ

Судалгааг хийхдээ 4-н өөр холболтын төрөл ашиглаж харьцуулан судалгааны үр дүнг гаргахыг зорьсон. Монгол улсын интернэт үйлчилгээ үзүүлэгч

компаниас шилэн кабель, радио интерфейс, утасгүй сүлжээ, гар утас дээрх хөдөлгөөнт интернэт гэсэн өөр өөр интерфейсээр үйлчилгээ авч байгаа нь олон улсын стандартууд, IP давхарыг хангаж байгаа эсэхийг шалгах аар зорьсон.

Уг тестийг хийхэд 202.21.112.200/30 IP хаягтай хурдны хязгааргүй сүлжээ үүсгэн Герман, Япон, Хонг-Конг, Монгол улс гэсэн 4-н улс руу хандалт хийж шалгасан.

Хандалт хийхдээ *lg.he.net* сайтаас *Looking Glass* ашиглаж өөрийн IP хаяг руу хандаж шалгах, өөрийн сүлжээнээс тухайн улсад байрлаж байгаа *Hurricane Electric LLC*-ны серверүүд рүү хандан шалгаж үйлчилгээний чанар хэр байгааг шалгасан.

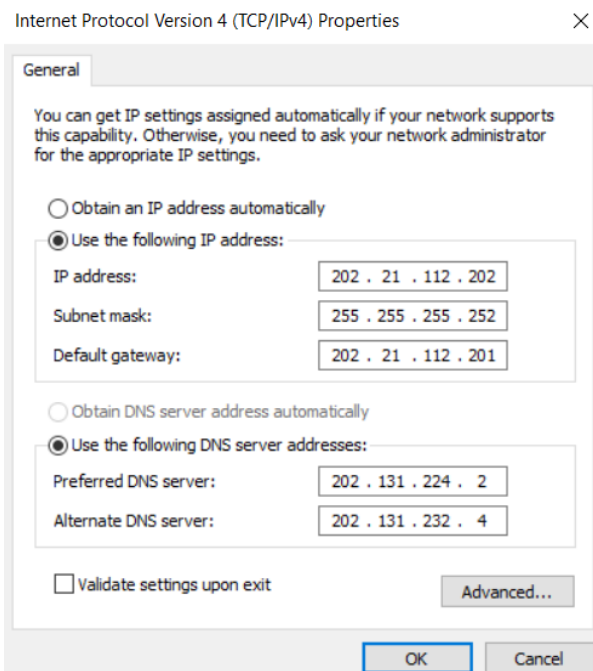
Уг тестийг хийхдээ Jitter, Latency, Error Rate, Packet Loss-ыг PingPlotter Pro програмын тусламжтайгаар хэмжилт хийж шалгасан бол Bandwith болон Throughput-ыг тухайн серверүүд рүү Wireshark, Speedtest, IPerf ашиглан шалгасан.

#### VI. ТУРШИЛТ

1. Интернэт үйлчилгээ үзүүлэгч компаниас интернэт хэрэглэгч байгуулагд зориулсан 1 гигабитийн интерфейс тэй хязгааргүй хурдтай тестийн үзүүр ашиглан шууд холболт үүсгэн туршилт хийсэн.



1-р зураг. Direct холболтыг тестийн орчинд хийсэн топологи зураг

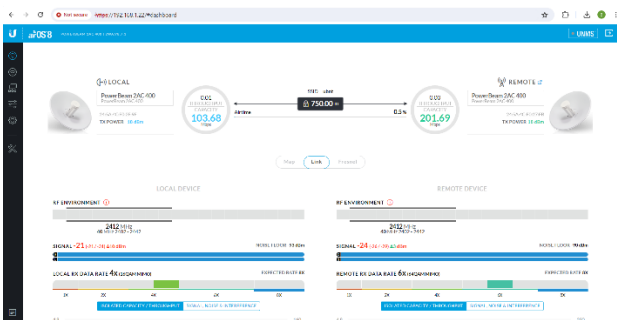


2-р зураг. Тест хийхэд зориулан үүсгэсэн тусгай зориулалтын бодит интернэт протокол хаяг юм. Үүнийг тест хийж буй компьютер дээр гараар тохируулсан.

2. Интернэт үйлчилгээ үзүүлэгч компаниас интернэт хэрэглэгч байгуулагд зориулсан 1 гигабитийн интерфейстэй хязгааргүй хурдтай тестийн үзүүр дээр радио дахин дамжуулах байрлуулан холболт үүсгэн туршилт хийх (Туршилтын Ubiquiti PBE-5AC-Gen2 загварын 2 ширхэг радио модем ашиглан хийж гүйцэтгэсэн)



3-р зураг. Дахин дамжуулах радио модем ашиглаж буй холболтын топологи



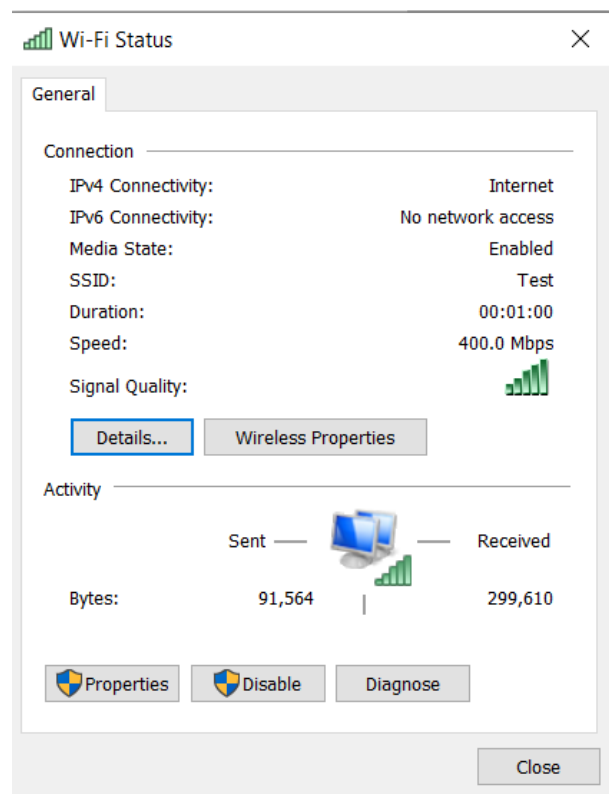
4-р зураг. Дахин дамжуулах радио модемын тохируулсан байдал Радио сигнал-24dBm, Дамжуулах чадвар (103.68-201.69Mbps)

Дахин дамжуулах 2 радио модем дээр тус бүрт нь тохиргоо хийж дамжуулах болон хүлээн авах байдлаар тохируулан 40MHz өргөн зурвас үүсгэсэн.

3. Интернэт үйлчилгээ үзүүлэгч компаниас интернэт хэрэглэгч байгуулагд зориулсан 1гигабитийн интерфейстэй хязгааргүй хурдтай тестийн үзүүр дээр утасгүй нэвтрэх цэг суурилуулан утасгүй сүлжээнд (Unifi U6 mesh) загварын утасгүй нэвтрэх цэг ашиглан туршилт хийж гүйцэтгэсэн.



5-р зураг. Утасгүй нэвтрэх цэг ашиглан утасгүй сүлжээнд хийсэн тестийн топологи

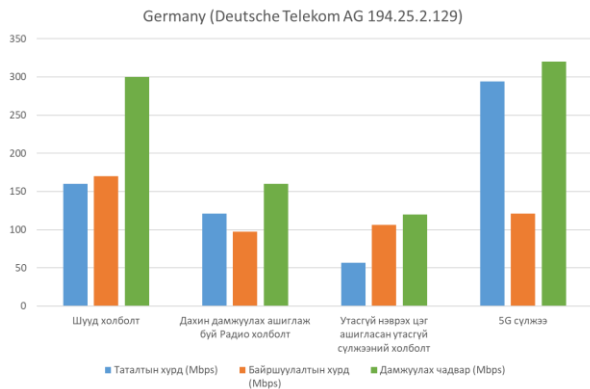


6-р зураг. Утасгүй сүлжээний холболт үүсгэсэн байдал. Утасгүй нэвтрэх цэгийн компьютертэй шууд холболт үүсгэж байгаа дамжуулах чадвар(400Mbps) байна.

4. Гар утасны үүрэн холбооны 5G сүлжээ ашиглан туршилт хийсэн. Мобиком корпорацийн төв оффис дээр суурилуулсан байгаа тестийн 5G сүлжээг ашиглан тест хийж шалгасан.

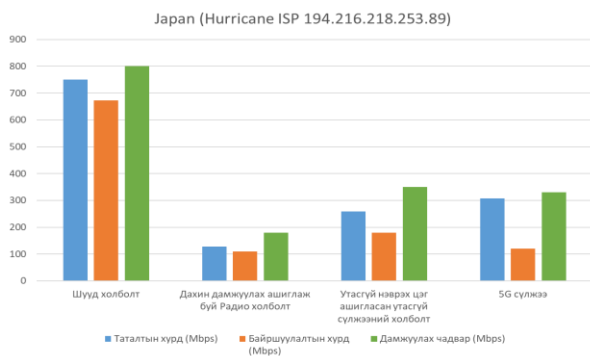


7-р зураг. 5G сүлжээ ашиглан тест хийсэн топологи зураг



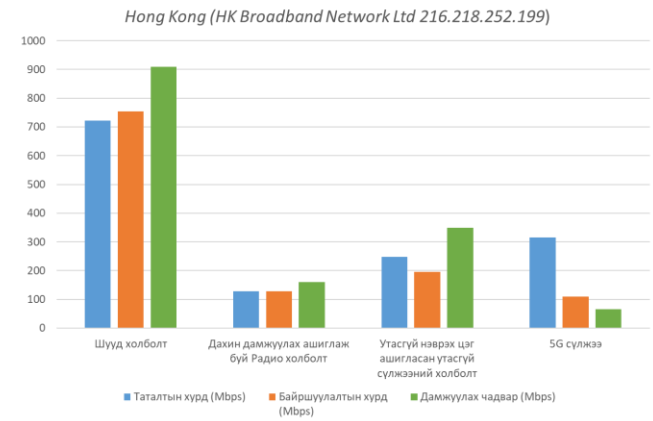
8-р зураг. Герман улсын сервер рүү хандалт

Туршилтын үр дүнд хоцролт (0.9-133.3 мс), хэлбэлзэл(125-200мс), багц алдагдал (0%) байна. Энэ нь үйлчилгээний чанарын стандартын дагуу үйлчилгээний чанар дундаж байна.



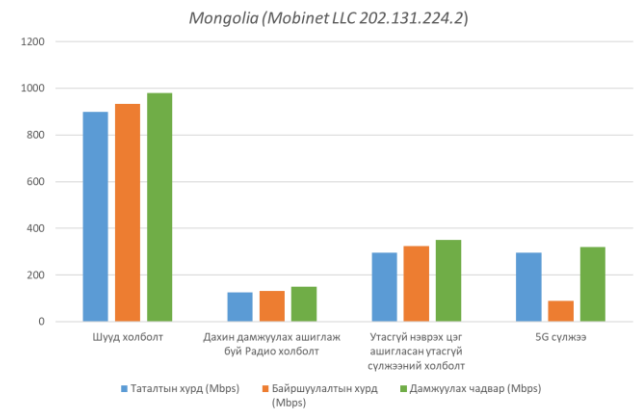
9-р зураг. Япон улсын сервер рүү хандалт

Туршилтын үр дүнд хоцролт (0.9-89.4 мс), хэлбэлзэл(60-80мс), багц алдагдал (0%) байна. Энэ нь үйлчилгээний чанарын стандартын дагуу үйлчилгээний чанар сайн байна.



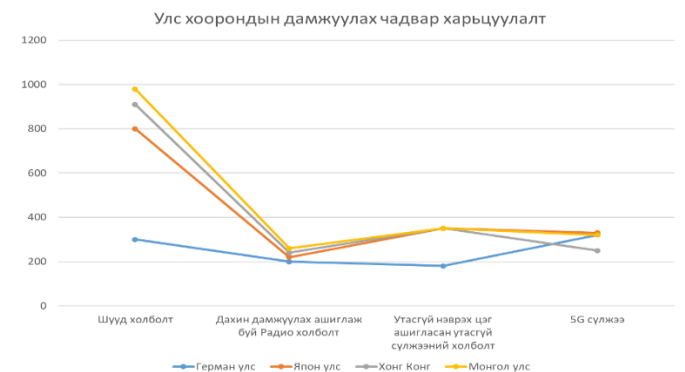
10-р зураг. Хонг Конг улсын сервер рүү хандсан хандалт

Туршилтын үр дүнд хоцролт (0.7-141.1 мс), хэлбэлзэл(120-135мс), багц алдагдал (0%) байна. Энэ нь үйлчилгээний чанарын стандартын дагуу үйлчилгээний чанар дундаж байна.



11-р зураг. Монгол улсын дотоод сервер рүү хандсан хандалт

Туршилтын үр дүнд хоцролт (0.7-22.4 мс), хэлбэлзэл(1-18мс), багц алдагдал (0%) байна. Энэ нь үйлчилгээний чанарын стандартын дагуу үйлчилгээний чанар сайн байна.



12-р зураг. 4-н улсын дамжуулах чадвар

Туршилтын үр дүнд татах болон байршуулах хурдны хамгийн гол үзүүлэлт болох дамжуулах чадварын харьцуулан харуулсан байгаа. Дээрх 3-н улс руу шууд холболтын үед (800-990Mbps) хурдаар холбогдох боломжтой байгаа. Герман улсын хувьд олон улсын гарцын ачаалал болон дахин дамжих алхмуудаас хамаарч дамжуулах чадвар бага байна. Дахин дамжуулах холболт, утасгүй сүлжээний холболт, 5G холболтын хувьд дамжуулах чадвар нь дээд тал нь (400Mbps) байгаа учир холболтын хурд өсөх боломжгүй байна.

### ДҮГНЭЛТ

Энэхүү судалгааны ажлаар дөрвөн өөр төрлийн холболтоор интернэт үйлчилгээ авч байгаа хэрэглэгчийн сүлжээний үйлчилгээний чанарыг үнэлж үзэхэд олон улсын ITU-T Y.1541[1], ITU-T G.1010[2], RFC 4594[3] стандартын шаардлагыг хангаж байгааг тооцоо хийж үр дүнг зураг болон хүснэгтээр үзүүлсэн. Туршилтын үр дүнгээс холболтын төрөл болон өөр улсуудын серверүүд рүү холбогдож байгаа интернэтийн олон улсын гарцаас шалтгаалан холболтын чанар ялгаатай байгааг харьцуулан харуулсан. Шууд холболт болон 5G холбогдож буй тохиолдолд интернэтийн хурд болон бусад үзүүлэлтүүд нь чанарын шаардлага хангалттай хангаж байна. Харин дахин дамжуулах радио модем болон утасгүй сүлжээний холболтын үед тухайн төхөөрөмжийн дамжуулах чадвар, багтаамжаас хамаарч хоцролт, хэлбэлзэл өсөж үйлчилгээний чанарын хүснэгтийн дунд түвшинд хамаарагдаж байна.

Харилцан адилгүй байршилтай 4-н улс руу хандаж хэмжүүр үзүүлэлтийг шалгахад физик холболт болон зайнаас хамааран Монгол улс руу үйлчилгээний чанар хамгийн сайн байна. Азийн орнууд болох Япон, Хонг Конг руу үйлчилгээний чанарын түвшин сайн байгаа. Монгол улс дотор татах хурд 898.89 Mbps хэлбэлзэл 1.5мс, Хонг Конг руу 721.83 Mbps хэлбэлзэл 125мс, Япон улсруу 750.16

Mbps хэлбэлзэл 60мс, Герман улс руу 160.15 Mbps хэлбэлзэл 125 мс байгаа нь Герман улс руу үйлчилгээний чанарыг дунд түвшинд байна гэж туршилтын үр дүнгээс дүгнэж байна. Үүнийг сайжруулахын тулд олон улсын гарцуудыг өргөтгөх, дамжих алхамыг цөөлөх, сүлжээний оновчтой замчлал бий болгох шаардлагатай гэж үзэж байгаа.

### ТАЛАРХАЛ

Энэхүү судалгааны ажлыг хийж гүйцэтгэхэд гүн туслалцаа үзүүлсэн ШУТИС- Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн сүлжээ, аюулгүй байдлын салбарын Т.Булганмаа, Я.Дашдорж багш нар, судалгааны төстийн орчин бүрдүүлэхэд туслалцаа үзүүлсэн Мобинет ХХК болон Техникийн албаны сүлжээний инженер Л.Анхбаяр, М.Цэнджав нарт талархал илэрхийлье.

### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] [Itu-t y.1540] telecommunication standardization sector of itu (07/20/2016)
- [2] [itu-t y.1010] recommendation itu-t y.1010 (2001), SERIES g: transmission systems and media, digital systems and networks Quality of service and performance.
- [3] [RFC 4594.] "Differentiated Services Field (DS Field 2006) IETF (Internet Engineering Task Force)  
<https://www.rfc-editor.org/rfc/pdf/rfc4594.txt.pdf>
- [4] <https://www.mdpi.com/2073-8994/15/2/513> Quality of Service (QoS) Performance Analysis in a Traffic Engineering Model for Next-Generation Wireless Sensor Networks
- [5] <https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service> 2024 оны 10-р сарын 16-нд хандсан
- [6] <https://ieeexplore.ieee.org/document/9559087> 2024 оны 11-р сард хандсан.
- [7] [https://www.researchgate.net/publication/229008214\\_QoS\\_Requirements\\_of\\_Network\\_Applications\\_on\\_the\\_Internet](https://www.researchgate.net/publication/229008214_QoS_Requirements_of_Network_Applications_on_the_Internet) 2024 оны 11-р сард хандсан.
- [8] <https://hemantra.medium.com/exploring-5g-quality-of-service-qos-unlocking-the-potential-of-next-generation-networks-2166ca2f7302> Qos for 5G 2024 оны 11-р сард хандсан

## ЛИНУКС СУУРЬТАЙ ҮЙЛДЛИЙН СИСТЕМ ДЭЭРХ ХОРТ ПРОГРАММЫГ МАШИН СУРГАЛТЫН АЛГОРИТМ АШИГЛАН ИЛРҮҮЛЭХ, ТҮҮЛ ХӨГЖҮҮЛЭХ

**Батчулуун БААСАНЖАРГАЛ<sup>1</sup>, Шүрэнцэцэг НАНДИНДУЛАМ<sup>1</sup>, Бат-Эрдэнэ МӨНХБАЯР<sup>2</sup>**  
<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, МХТС, Мэдээллийн Сүлжээ, Аюулгүй Байдлын салбар  
*Холбоо барих зохиогчийн и-мэйл хаяг: munkhbayar.b@gmail.com<sup>1\*</sup>*

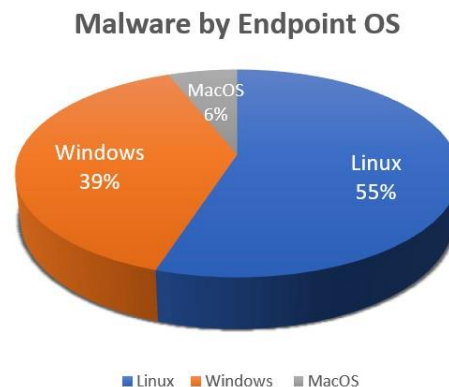
**Хураангуй**—Энэхүү судалгааны ажил нь машин сургалтын аргыг ашиглан хорт программ илрүүлэх системийн гүйцэтгэлийг сайжруулахад чиглэнэ. Хорт программ хангамжийн хувьслын талаарх бусад судалгааны ажлуудад дурдсанаар гарын үсэгт суурилсан статик шинжилгээ нь дахиж ашиглагдахгүй болсныг харуулж байсан. Иймд, зан төлөвт суурилсан динамик шинжилгээг машин сургалтын аргатай хослуулан ашигласан. Туршилтад Decision Tree (DT), Random Forest (RF), N-Grams зэрэг алгоритмуудыг 5560 хортой, 9476 хоргүй программаас бүрдсэн өгөгдлийн багц дээр хэр нарийвчлалтай илрүүлж байгааг шинжилсэн. Туршилтын үр дүнд DT 96.6%, RF нь 98.3% -н нарийвчлалтай гарсан. Энэхүү судалгаа нь хорт программыг илрүүлэх, хамгаалалтыг сайжруулахын тулд зан төлөвт суурилсан машин сургалтын аргуудыг хэр сайн нэгтгэж болохыг онцлон харуулав. Мөн тухайн алгоритмыг ашиглан линукс суурьтай үйлдлийн систем дээрх хорт программыг илрүүлэх программыг хөгжүүлсэн.

**Түлхүүр үг**—Хорт программ хангамж, хорт программыг илрүүлэх, машин сургалт, линукс хорт программ

### I. УДИРТГАЛ

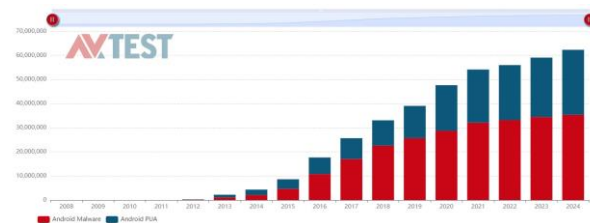
Орчин үеийн технологийн салбарт кибер халдлага нь хамгийн тулгамдсан асуудал болоод байна. Сүлжээ, компьютерын систем эсвэл дижитал төхөөрөмжид зөвшөөрөлгүй нэвтрэх замаар өгөгдөл, программууд болон бусад хөрөнгийг хулгайлах, задруулах, өөрчлөх, идэвхгүй болгох, устгах зорилготой аливаа оролдлогыг кибер халдлага гэнэ. Хорт программ нь кибер халдлагын нэгэн жишээ юм. Хорт программ бүтээгчид хортой код зохиохдоо хамгийн өргөн хэрэглэгддэг антивирус программ хангамжууд дээр туршиж үзсэний эцэст тарааж эхэлдэг. Уг хортой код цахим ертөнцөд хор хөнөөл учруулж эхлэх үед тухайн хортой кодыг судалгааны лабораториуд авч судлан хортой кодын өгөгдлийн баазад бүртгэх хүртэл хугацаанд гарын үсэгт суурилсан илрүүлэлт /signature-based detection/, эвристик дээр суурилсан илрүүлэлт /heuristic-based detection/ зарчмаар ажилладаг антивирус программ хангамжуудад илрэх боломжгүй байдаг. Өөрөөр хэлбэл, уламжлалт вирусийн эсрэг системүүд полиморфик, метаморфик болон шинээр бий болсон хорт программуудын төрлийг шууд илрүүлэх чадваргүй юм. Иймд, судлаачид эдгээр хорт программ илрүүлэх аргуудыг зан төлөвт суурилан шинжлэх аргатай хослуулан ашиглах болсон. Бид энэхүү судалгааны ажлаараа программын ашиглаж буй функц, гаргаж буй үйлдлээр нь хортой программ байж болох магадлалыг өөрсдийн сургасан машин сургалтын алгоритмуудыг ашиглан тооцоолох болно. Хорт программ хангамж нь янз бүрийн үйлдлийн систем дээр хийгддэг ба 2023 оны Elastic-н судалгаанаас авч үзэхэд бүх хорт программын 55% нь

Линукс төгсгөлийн төхөөрөмжүүд дээр хийгдсэн байдаг бол, 39% нь Виндөүз төхөөрөмжүүд дээр харин үлдсэн 6% нь MacOS дээр хийгдсэн байна.



1-р зураг. Төгсгөлийн төхөөрөмжүүд дээрх хортой программын судалгаа, Elastic, 2023[1]

Мөн Линукс үйлдлийн систем дээрх хорт программ болон PUA-ийн тоо хэмжээ 2008-2024 оны хооронд 20193-аас 4745535 хүртэл буюу 234.9 дахин өссөн байгаа юм.



2-р зураг. Линукс үйлдлийн систем дээрх хорт программын тоо хэмжээ.[2]

Үүнээс харахад Линукс үйлдлийн систем дээрх хорт программ хангамжид зайлшгүй анхаарал хандуулах

шаардлага үүсээд байна. Энэхүү судалгаа нь Линукс үйлдлийн систем дээр хорт программыг илрүүлэхэд ашиглаж болох хамгийн өндөр нарийвчлалтай машин сургалтын алгоритмыг туршилтаар тодорхойлох ба түүнийг ашиглан Malware detector tool хөгжүүлэх зорилготой юм. Энэ судалгаанд бид хорт программыг ангилах, илрүүлэх найдвартай, үр дүнтэй аргыг боловсруулахын тулд машин сургалтын 3 алгоритмд дүн шинжилгээ хийсэн.

## II. ОНОЛЫН ОЙЛГОЛТ

### A. Хорт программ гэж юу вэ?

Malware /Хорт программ/ гэсэн нэр томъёо нь "Malicious" ба "Software" гэсэн хоёр үгийг нэгтгэснээс үүссэн [3]. Хорт программ нь мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй холбоотой компьютерын системийн аюулгүй байдлын бодлогыг зөрчих зорилгоор ашигладаг программ хангамж бөгөөд өнөөг хүртэл хорт программыг бүрэн илрүүлэх арга техникийг нээгээгүй байгаа юм. Өөрөөр хэлбэл, гарын үсэгт суурилсан, зан төлөвт суурилсан, үүлэн технологит суурилсан зэрэг хорт программыг илрүүлэх аргууд нь 100% үр дүнтэй илрүүлэх боломжгүй. Иймд хамтад нь ашиглах, шинэ арга техник боловсруулах замаар хорт программ илрүүлэх чадамжийг нэмэгдүүлэхийг зорьж байна.

### B. Хорт программыг илрүүлэх аргууд [4]

Хорт программыг илрүүлэх арга техникийг гарын үсэгт суурилсан илрүүлэлт /signature-based detection/, зан төлөвт суурилсан илрүүлэлт /heuristic-based detection/, тодорхойлолтод суурилсан илрүүлэлт /specification-based detection/ гэж ангилж болно.

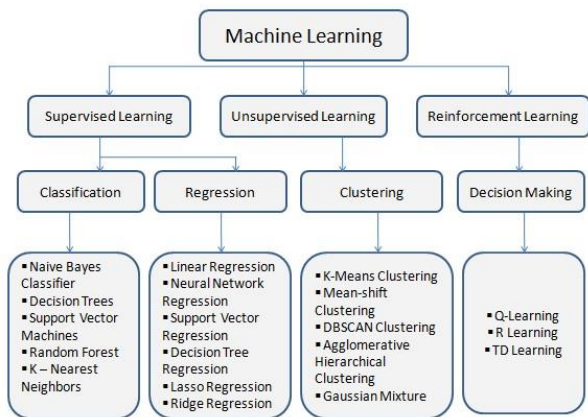
- Гарын үсэгт суурилсан илрүүлэлт: Энэ нь гарын үсгийн санг хадгалдаг бөгөөд тухайн өгөгдлийн сан дахь хэв маягтай харьцуулах замаар илрүүлэлтийг хийнэ. Ихэнх вирусийн эсрэг программууд энэ төрлийн илрүүлэлтийн техник дээр суурилсан байдаг. Гарын үсгүүд нь хорт программын хоёртын тооллоор задалсан кодоор үүсгэгддэг. Энэхүү задалсан кодыг анализ хийн шинж чанаруудыг гарган авна. Эдгээр шинж чанаруудыг хорт программын тодорхой нэг төрөлд зориулан гарын үсгийг хадгална. Улмаар вирусийн эсрэг программ хангамж хөгжүүлэгч байгууллага өгөгдлийн санд шинэчлэлт хийснээр энэхүү техник зөв илрүүлэлт хийх боломжтой болдог. Өгөгдлийн сан дахь шинж чанаруудын дагуу хурдан, зөв илрүүлэлт хийх, цөөн нөөц шаардагдах гэх мэт давуу тал олонтой ч шинэ төрлийн эсвэл үл мэдэгдэх хортой программыг илрүүлэх боломжгүй сул талтай.

- Зан төлөвт суурилсан илрүүлэлт: Өөрөөр мөн хэвийн бус шинж чанарт суурилсан илрүүлэлт гэж нэрлэгддэг бөгөөд гол зорилго нь мэдэгдэх болон үл мэдэгдэх хортой программын зан төлөвийг анализ хийх юм. Зан төлөвийн параметр нь хортой программын очих хаяг, хавсралтын төрлүүд зэрэг тоологдох боломжтой статистик шинж чанаруудаас бүрдсэн олон төрлийн эх үүсвэрээс бүрдэнэ. Энэ нь ихэвчлэн сургалтын болон илрүүлэлтийн үе шатуудад хуваагдана. Сургалтын үе шатанд халдлага байхгүй үед системийн хэвийн зан төлөв ажиглагдаж, ийм хэвийн зан үйлийн дүр төрхийг бий болгохын тулд машин сургалтын техникийг ашигладаг. Илрүүлэх үе шатанд шалгагдах программыг хадгалж авсан хэвийн зан үйлтэй харьцуулж, ялгааг болзошгүй халдлага гэж тэмдэглэнэ. Энэ аргын давуу тал нь мэдэгдэж байгаа болон шинэ, үл мэдэгдэх хортой программуудыг илрүүлж чаддаг бөгөөд үл мэдэгдэх халдлагыг илрүүлэхийн тулд системийн үйл ажиллагаанд анхаарлаа хандуулдаг. Энэ аргын сул тал нь системийн төлөв байдал, статистикийг тодорхойлсон өгөгдлийг шинэчлэх шаардлагатай байдаг боловч энэ нь том хэмжээтэй байдаг. Үүнд CPU-ийн цаг, санах ой, дискийн зай гэх мэт илүү их нөөц шаардлагатай бөгөөд худал эерэг түвшин /false positive/ өндөр байна.

- Тодорхойлолтод суурилсан илрүүлэлт: Энэ нь халдлагын тодорхой хэлбэрийг илрүүлэхээс илүүтэйгээр программын гүйцэтгэлийг хянах, тэдгээрийн зан төлөвийн тодорхойлолтоос өөр байдлыг илрүүлэх юм. Энэ техник нь аномали илрүүлэхтэй төстэй боловч ялгаа нь машин сургалтын арга техникт найдахын оронд системийн зан төлөвийг харуулсан гараар боловсруулсан техникийн үзүүлэлтүүд дээр суурилдаг. Энэ аргын давуу тал нь хорт программын мэдэгдэж байгаа болон үл мэдэгдэх тохиолдлуудыг илрүүлж, худал эерэг түвшин бага боловч хуурамч сөрөг түвшин өндөр бөгөөд шинэ халдлагыг илрүүлэхэд үр дүнтэй биш юм.

Дээрх хорт программыг илрүүлэх аргуудийн давуу болон сул талыг авч үзсэнээр өмнө нь дурдсанчлан нэг ч алдаагүй үнэн зөв илрүүлж чадах техник байхгүй гэдгийг харж болно. Иймд бид бодит цагт илрүүлэлт хийх, шинэ болон хуучин хувилбарт гээд аль ч төрлийн программыг шинж чанарт

Reinforcement learning: Агент орчинд үйлдэл хийж, орчноос ирсэн шагнал (reward) дээр үндэслэн суралцдаг. Жишээ нь, тоглоом тоглох робот.



3-р зураг. Машин сургалтын алгоритмын төрлүүд[6]

тулгуурлан шинжлэх чадвартай, өөрийгөө тасралтгүй сайжруулж байх зан төлөвт суурилсан илрүүлэлтийг ашиглахаар сонгосон. Үүний тулд, ашиглах машин сургалтын алгоритмууд дээр судалгаа хийх шаардлагатай.

### III. СУДАЛГААНЫ ХЭСЭГ

#### A. Машин сургалтын алгоритмууд

Машин сургалт нь үндсэндээ 3 парадигмаас бүрдэнэ [5]. Үүнд:

**Supervised learning:** Хяналттай сургалтын алгоритмууд нь оролт болон хүссэн гаралтыг хоёуланг нь агуулсан өгөгдлийн багцыг ашиглана. Сургалтын өгөгдлийн багцаас /training dataset/ гарган авсан шинж чанар, векторуудын тусламжтай төстийн өгөгдлийн багц /testing dataset/-г шинжилдэг.

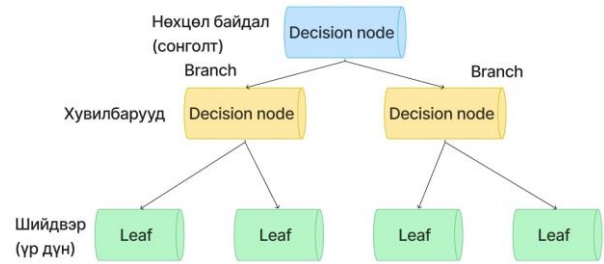
**Unsupervised learning:** Гаралтыг урьдчилан заагаагүй өгөгдөл дээр суралцаж, өгөгдлийн дотоод бүтцийг ойлгох. Жишээ нь, кластерчлэл, өгөгдлийн хамаарлыг олох.

#### B. Өмнө судлагдсан ажлууд

Машин сургалтын алгоритмуудын талаар үндсэн ойлголтыг авсны дараагаар хорт программ илрүүлэлтэд ашиглагддаг хамгийн өндөр нарийвчлалтай гэж туршилтаар тодорхойлогдсон N-Grams, Decision Tree, Random Forest алгоритмуудыг сонгосон. Өмнө судлагдсан ажлуудын мэдээллийг “1-р хүснэгт”-д үзүүлэв.

#### C. Мотиваци

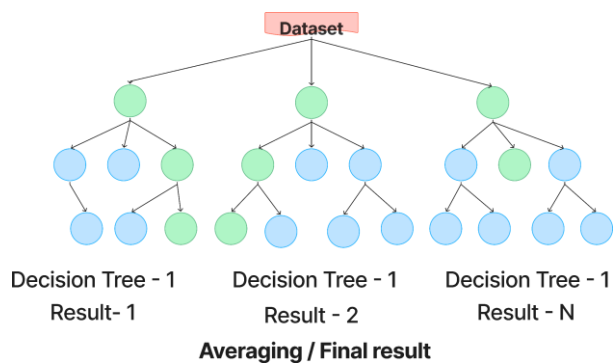
Өмнө нь судлагдсан ажлуудаас харахад машин сургалтын алгоритмыг ашиглан хорт программыг



4-р зураг. Шийдвэрийн мод алгоритм

#### • Random Forest:

Санамсаргүй ой нь шийдвэрийн модны олон хувилбаруудыг нэгтгэж, олон төрлийн шийдвэр гаргах боломжийг нэмэгдүүлдэг алгоритм юм. Энэ алгоритм нь илүү хүчтэй, алдааг багасгасан шийдэл гаргахад ашиглагддаг. Санамсаргүй ойн алгоритм нь олон шийдвэрийн мод үүсгэж, эдгээр мод тус бүр нь өөр өөр өгөгдлийн санг ашиглан боловсруулдаг. Эцсийн үр дүнг гаргахдаа, бүх модны саналыг нэгтгэж дүгнэдэг. Энэ арга нь overfitting буюу хэт тохируулагдсан асуудлыг бууруулдаг.



5-р зураг. Санамсаргүй ой алгоритм

илрүүлэх ажлууд хийгдсэн хэдий ч тэдгээрийн үр дүнд тулгуурлан хөгжүүлсэн хорт программ илрүүлэх программ хангамж байхгүй байгаа юм. Тиймээс Линукс үйлдлийн систем дээр хорт программыг илрүүлэхэд ашиглаж болох хамгийн өндөр нарийвчлалтай машин сургалтын алгоритмыг нэгтгэн Malware detector tool хөгжүүлэх.

### IV. ТУРШИЛТЫН ХЭСЭГ

Өмнө судлагдсан ажлуудаас хамгийн өндөр үзүүлэлттэй байсан DT, RF, N-Grams алгоритмуудыг сонгон авч туршилтыг гүйцэтгэсэн. Юуны өмнө эдгээр алгоритмуудын ажиллах зарчим, онцлогуудын талаар ерөнхий ойлголтыг авч үзье:

#### • Decision Tree:

[7]Шийдвэрийн мод нь өгөгдлийг ангилах эсвэл таамаглахад ашиглагддаг мод хэлбэрийн загвар юм. Энэ алгоритм нь өгөгдөл дээрх шинж чанаруудыг ашиглан, тодорхой шийдвэр гаргах логикийг дүрслэхэд зориулагдсан. Үндсэн санаа нь өгөгдлийн

сангийн шинж чанаруудыг авч үзэн тэдгээрээс хамгийн чухал онцлогийг олж тодорхойлоод, тэдгээрээр өгөгдлийг ялгаж ангилдаг. Модны үүр нь тухайн онцлог шинж чанаруудыг илэрхийлж, салаа нь шийдвэрийн нөхцөл байдал болдог. Үр дүнд модны эцсийн навч дээр шийдвэр эсвэл таамаглал гардаг.

• N-Grams:

N-грамм нь текстийг боловсруулж, өгөгдлийг анализ хийхэд ашигладаг хэл шинжлэлийн арга юм. Энэ нь N үгийн дарааллыг илэрхийлдэг ба хэлний загварыг тодорхойлохдоо текстийн бүтэцтэй холбоотой мэдээллийг ашигладаг. Жишээлбэл, 2-грамм нь текстийн 2 дараалсан үг дээр тулгуурлаж, 3-грамм нь 3 дараалсан үг дээр тулгуурлана. Энэ аргыг машин сургалтад текстийн өгөгдөл боловсруулах үед ашигладаг.

N1:	This	is	a	sentence	this, is, a, sentence	← Unigrams
N2:	This	is	a	sentence	this is, is a, a sentence	← Bigrams
N3:	This	is	a	sentence	this is a, is a sentence	← Trigrams

6-р зураг. N-грамм алгоритм

A. Өгөгдлийн багцын мэдээлэл

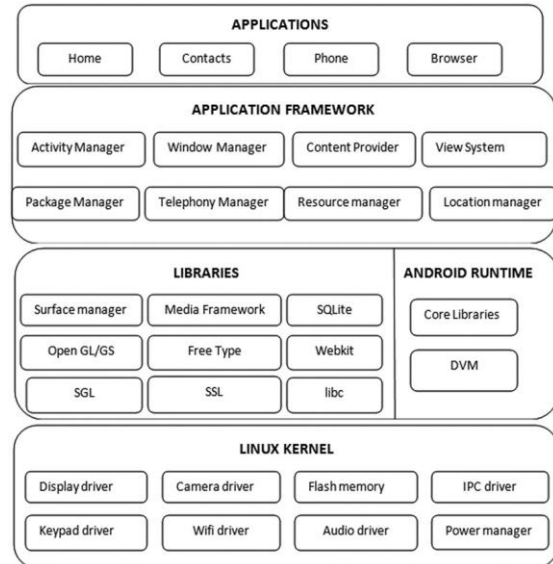
Сонгож авсан алгоритмууд нь хяналттай сургалтын төрөлд хамаарагдана. Өөрөөр хэлбэл, оролт болон хүссэн гаралтыг хоёуланг нь агуулсан өгөгдлийн багцыг ашиглана гэсэн үг. Алгоритмаа сургахад ашигласан өгөгдлийн багц нь Drebin төслийн 15036 программаас (5560 хортой программ, 9476 хоргүй программ) гаргаж авсан 215 API /Application Programming interfaces/ calls шинж байвал 1, үгүй бол 0 гэсэн хоёртын тооллоос бүтсэн ба 15036 мөр бүрийн төгсгөлд хортой, хоргүйг зааж өгсөн байна. Өөрөөр хэлбэл, хяналттай сургалтын чанарын векторуудаас бүрдсэн. API call нь аппликейшнаас явуулж буй үйлдлийн систем эсвэл программын тодорхой функцийг ажиллуулахыг шаардсан хүсэлтийг хэлнэ. Жишээлбэл, программын зорилгоос хамааран өгөгдлийн сан, интернэттэй холбогдох, мессеж илгээх, банкны аппликейштай холбогдох болон камерт хандах зэрэг функцүүдийг ажиллуулах API call-ийг ашигладаг.

transact	onServiceConnected	bindService	attachInterface	ServiceConnection	android.os.Binder	class
0	1	0	1	1	1	S
0	0	0	0	1	1	B
1	1	1	1	1	0	S
0	0	0	0	1	1	B

7-р зураг. Өгөгдлийн багцын формат

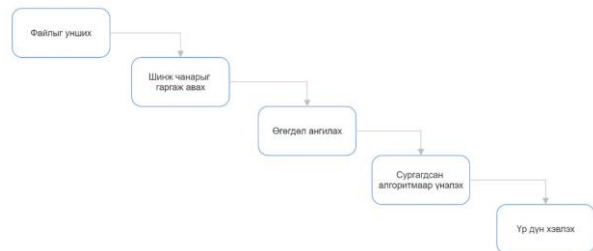
Өгөгдлийн багц нь тухайн API call-г ашиглаж алгоритмууд ашиглах учир оролт болон хүссэн гаралтыг хоёуланг нь агуулсан өгөгдлийн багцыг ашигласан гэсэн үг.

Тухайн өгөгдлийн багц нь Андроид үйлдлийн системийн өгөгдлийн багц бөгөөд андроидын кернел нь Linux Long Term Supported (LTS) кернел дээр суурилдаг. Өөрөөр хэлбэл, Андроид бол Линуксийн кернелийн өөрчилсөн хувилбар буюу Linux юм. Тиймээс андроидын өгөгдлийн багцыг ашиглаж болно гэж үзсэн.

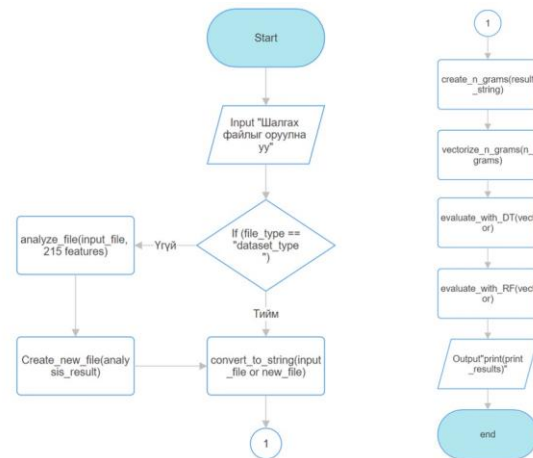


8-р зураг. Андроид үйлдлийн системийн архитектур [9]

B. Программын ажиллах зарчим



9-р зураг. Программын бүтцийн схем



10-р зураг. программын алгоритм

C. Туршилтын гүйцэтгэл

## 1. Сургалтын хэсэг

Псевдо код:

```

1: procedure
MalwareDetection(data_path)
2:   Import libraries
3:   data ← Load CSV from data_path
4:   Define
create_feature_string(row): return
joined feature names where row[col] =
1
5:   data['feature_string'] ← Apply
create_feature_string to each row 6:
7:   vectorizer ← TfidfVectorizer
(n-gram range 1-3)
8:   X ← Fit and transform
data['feature_string'] with vectorizer
9:   Map data['class'] values: 'B' →
0, 'S' → 1
10:  X_train, X_test, y_train, y_test
← Split data
11:  X_train_smote, y_train_smote ←
Apply SMOTE to X_train, y_train 12:
13:  rf_classifier ← Tune and train
RandomForestClassifier with
X_train_smote, y_train_smote
14:  dt_classifier ← Tune and train
DecisionTreeClassifier with
X_train_smote, y_train_smote
15:
16:  rf_predictions ←
rf_classifier.predict(X_test)
17:  dt_predictions ←
dt_classifier.predict(X_test)
18:  Print reports and accuracy for
rf_predictions and dt_predictions 19:
20:  Save vectorizer, rf_classifier,
dt_classifier to files
21: end procedure

```

## 2. Шинэ өгөгдлийн багц дээрх туршилт Псевдо

код:

```

1: procedure
MalwareDetectionEvaluation(test_data_p
ath, vectorizer_path, rf_model_path,
dt_model_path)
2:   Import libraries 3:   Define
generate_ngrams(text, n): return list
of n-grams if text is valid 4:
5:   test_data ← Load CSV from
test_data_path
6:   Define
create_feature_string(row): return
joined feature names where row[col] =
1

```

```

7:   test_data['feature_string'] ←
Apply create_feature_string to each
row
8:
9:   vectorizer ← Load vectorizer
from vectorizer_path 10:
rf_classifier ← Load random forest
model from rf_model_path 11:
dt_classifier ← Load decision tree
model from dt_model_path 12:
13:  X_test ← Transform
test_data['feature_string'] with
vectorizer
14:  y_test ← Map 'class' column
values: 'B' → 0, 'S' → 1
15:
16:  rf_predictions ←
rf_classifier.predict(X_test) 17:
dt_predictions ←
dt_classifier.predict(X_test) 18:
19:  Print classification reports and
accuracy for rf_predictions and
dt_predictions
20: end procedure

```

## 3. Хөгжүүлэлтийн хэсэг Псевдо

код:

```

1: Initialize Flask app with
configuration:
- Set UPLOAD_FOLDER to '/tmp' and
ALLOWED_EXTENSIONS to {'apk'}
2: Define allowed_file(filename)
- Return True if file has an
allowed '.apk' extension
3: Define index route ('/')
- Render and return 'index.html'
4: Define predict route ('/predict',
methods=['POST'])
- Check if 'apkfile' is in
request.files
- If not, return "No file
uploaded!" (400) - Get 'apkfile' and
validate it:
- If filename is empty, return
"No selected file!" (400)
- If valid, save file to apk_path
in UPLOAD_FOLDER
- Try prediction with
predict_apk_malware(apk_path):

```

```

- Get rf_result, dt_result,
avg_benign_percentage,
avg_malware_percentage
- If error, set results to "Error"
- Delete uploaded file after
prediction

- Render 'result.html' with
prediction results

- If file type invalid, return
"Invalid file type! Upload a .apk"
(400)

5: Start Flask app in debug mode if run
directly
    
```

**V. ҮР ДҮН БА ХЭЛЭЛЦҮҮЛЭГ**

*A. Сургалтын хэсгийн үр дүн*

Random Forest: 98.3%

Decision Tree: 96.6%

Random Forest Classifier Report:				
	precision	recall	f1-score	support
0	0.98	0.99	0.99	2827
1	0.99	0.96	0.98	1684
accuracy			0.98	4511
macro avg	0.98	0.98	0.98	4511
weighted avg	0.98	0.98	0.98	4511
Random Forest Accuracy: 0.9831522943914874				
Decision Tree Classifier Report:				
	precision	recall	f1-score	support
0	0.97	0.97	0.97	2827
1	0.99	0.96	0.98	1684
accuracy			0.97	4511
macro avg	0.96	0.96	0.96	4511
weighted avg	0.97	0.97	0.97	4511
Random Forest Accuracy: 0.9665262691199291				

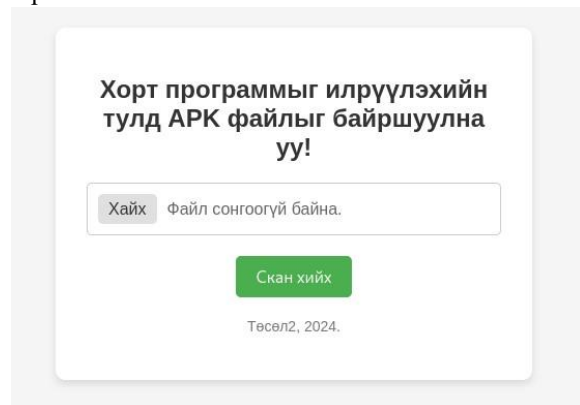
*B. Шинэ өгөгдлийн багц дээрх туршилтын үр дүн*

Random Forest: 89.6%

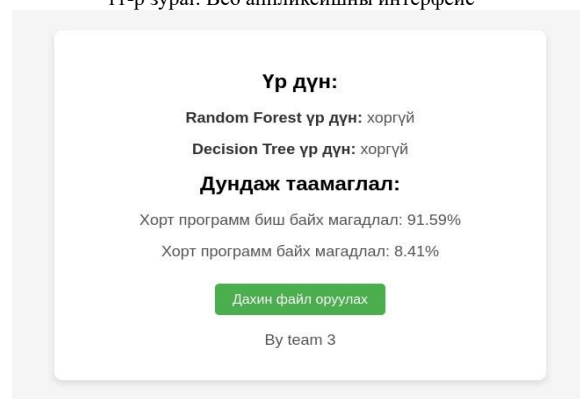
Decision Tree: 86.7%

Random Forest Classifier Report:				
	precision	recall	f1-score	support
0	0.87	1	0.93	2539
1	1	0.69	0.81	1260
accuracy			0.9	3799
macro avg	0.93	0.84	0.87	3799
weighted avg	0.91	0.9	0.89	3799
Random Forest Accuracy: 0.8960252698078441				
Decision Tree Classifier Report:				
	precision	recall	f1-score	support
0	0.88	0.92	0.9	2539
1	0.83	0.76	0.79	1260
accuracy			0.87	3799
macro avg	0.86	0.84	0.85	3799
weighted avg	0.87	0.87	0.87	3799
Random Forest Accuracy: 0.8670702816530665				

Сургалтын хэсгийн үр дүн болон шинэ өгөгдлийн багц дээр туршиж үзсэн хувь өндөр байгаа хэдий ч шалгаж буй API calls-н тоо хангалттай биш гэж үзэж байна. Тиймээс API calls-н тоог нэмэх шаардлагатай. Мөн тухайн файлаас 215 шинж чанарыг гаргаж авахад хугацаа их зарцуулж байгаа ба энэ нь илрүүлэх явцыг удаашруулж байна. Иймд нэг шинж чанарт илгээгдэх хүсэлтэд хугацааны хязгаар тавьж өгөх замаар энэхүү асуудлыг шийдэх боломжтой гэж харж байна.



11-р зураг. Веб аппликейшны интерфэйс



12-р зураг. Үр дүнгийн харагдах байдал

## VI. ДҮГНЭЛТ

Бид энэхүү судалгааны ажлаараа машин сургалтын алгоритмуудыг нэгтгэн /хослуулан ашиглах байдлаар/ хорт программыг илрүүлэх зан төлөвт суурилсан аргыг санал болгосон. Тестийн үр дүнг илэрхийлэхдээ хэдэн хувийн хортой болон хоргүй шинж чанар агуулагдаж байгааг харуулсан нь өмнө судлагдсан ажлуудад байгаагүй шинэлэг санаа юм. Одоогоор моделиуд нь .apk өргөтгөлтэй файлаас хэрхэн 215 шинж чанарыг гаргаж авахыг сурсан байгаа бөгөөд цаашид хорт программын байж болзошгүй файлын төрлүүдээр хөгжүүлэлтийг хийнэ. Үүнд .exe, .dll, .js, болон .ру зэрэг орно. Ингэснээр шинээр бий болсон, төрөл бүрийн форматтай гээд бүхий л хорт программыг шинжлэх боломжтой болох юм. Уламжлалт илрүүлэлтийн программууд тодорхой хэмжээний өртөгтэй, мөн зөвхөн өөрсдийн өгөгдлийн баазад байх гарын үсэгтэй харьцуулж үздэг байсан бол манай программыг ашигласнаар шалгаж буй файлынхаа үйлдлийн систем болон бусад аппликейшнүүдээс ямар функц, зөвшөөрлүүд шаардаж буйгаас үндэслэн бодит орчинд ажиллуулж үзэхээс өмнө шалгах боломжийг олгож байгаа юм.

## ТАЛАРХАЛ

Энэхүү төслийн ажлыг хийж гүйцэтгэх явцыг удирдан явуулсан удирдагч багш доктор (Ph.D) Б.Мөнхбаяр болон ШУТИС-ийн Мэдээлэл Холбоо Технологийн Сургуулийн Мэдээллийн сүлжээ, аюулгүй байдлын салбарын багш нартаа талархсанаа илэрхийлье.

## НОМ ЗҮЙ

- [1] Malware Statistics. Available from <https://portal.atlas.org/malware/statistics>
- [2] Malware Report. Available from [https://igtr.kb.us-east-1.aws.found.io:9243/s/gtr/app/canvas/workpad/cebd15f0-21e2-41b7-8d20-9f4a079fb07e/page/2?\\_fullScreen=true](https://igtr.kb.us-east-1.aws.found.io:9243/s/gtr/app/canvas/workpad/cebd15f0-21e2-41b7-8d20-9f4a079fb07e/page/2?_fullScreen=true)
- [3] Naseer, M., Rusdi, J. F., Shanono, N. M., Salam, S., Muslim, Z. B., Abu, N. A., & Abadi, I. (2021, April). Malware detection: issues and challenges. In *Journal of Physics: Conference Series* (Vol. 1807, No. 1, p. 012011). IOP Publishing.
- [4] Gormont, N. Z., Selamat, A., Cheng, L. K., & Krejcar, O. (2023). Machine learning algorithm for malware detection: Taxonomy, current challenges, and future directions. *IEEE Access*, 11, 141045-141089.
- [5] Akhtar, M. S., & Feng, T. (2023). Evaluation of machine learning algorithms for malware detection. *Sensors*, 23(2), 946.
- [6] Gavriluț, D., Cimpoeșu, M., Anton, D., & Ciortuz, L. (2009, October). Malware detection using machine learning. In *2009 International multiconference on computer science and information technology* (pp. 735-741). IEEE.
- [7] Ahmad Mantoo, B., & Ali Khan N, Z. (2024). Static, Dynamic and Intrinsic Feature Based Android Malware Detection Using Machine Learning: A Technical Review. *International Journal of Computing and Digital Systems*, 16(1), 1-13.
- [8] Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. *Symmetry*, 14(11), 2304.
- [9] Koli, J. D. (2018, March). RanDroid: Android malware detection using random machine learning classifiers. In *2018 Technologies for Smart-City Energy Security and Power (ICSESP)* (pp. 1-6). IEEE.
- [10] Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. *IEEE access*, 8, 6249-6271.
- [11] Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research (IJSR)*. [Internet], 9(1), 381-386.
- [12] Batta Mahesh "Machine Learning Algorithms - A review" in *International Journal of Science and Research (IJSR)*, 2018

## ӨМНӨ СУДЛАГДСАН АЖЛУУДЫН МАТРИЦ

I-Р ХҮСНЭГТ

Судалгааны ажил	Хувь нэмэр	Дүгнэлт	Ашигласан алгоритм	Accuracy (%)
Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. Symmetry, 14(11), 2304.	Энэхүү судалгааны ажил нь уламжлалт илрүүлэх аргуудаас зайлсхийхийн тулд гарын үсгээ байнга өөрчилдөг хорт программ хангамжийг илрүүлэх шинэ аргыг танилцуулсан. Нарийн төвөгтэй хорт программын аюулыг үр дүнтэй илрүүлж, бууруулах замаар кибер аюулгүй байдлын арга хэмжээг сайжруулахад машин сургалтын алгоритмуудыг ашиглах боломж байгааг харуулж байна.	Энэхүү судалгааны ажил нь хорт программыг илрүүлэхэд машин сургалтын (ML) алгоритмуудыг ашиглах сонирхол эрчимтэй өсөж байгааг онцолсон. Судалгаагаар хэд хэдэн машин сургалтын алгоритмуудыг үнэлж, хамгийн тохиромжтой аргачлалыг тодорхойлсон. Үр дүн нь DT хамгийн өндөр илрүүлэх нарийвчлалтай алгоритм (99%) байсан ба дараагаар нь CNN (98.76%) болон SVM (96.41%) орсон байна. Хуурамч эерэг хувь хэмжээгээр DT 2.01% үзүүлэлттэй байсан бол, CNN 3.97%, SVM 4.63% үзүүлэлттэй байв. Эдгээр ML загваруудыг Канадын Кибер аюулгүй байдлын хүрээлэнгээс авсан өгөгдлийн багцаар сургаж туршсан бөгөөд Portable Executable (PE) файлын өгөгдөл дээр суурилсан статик шинжилгээгээр онцлог шинж чанаруудыг гаргаж авсан. Судалгааны үр дүн нь хортой файлыг ажлуулахгүйгээр илрүүлэх боломжийг олгодог тул хортой өгөгдлийг танихад ихээхэн давуу талтай болохыг харуулж байна.	DT	99
			CNN	98.76
			SVM	96.41
			KNN	95.02
			Random Forest	92.01
			Naïve Byes	89.71
Akhtar, M. S., & Feng, T. (2023). Evaluation of machine learning algorithms for malware detection. Sensors, 23(2), 946.	Энэ судалгааны ажил нь хорт программыг илрүүлэхэд зориулсан машин сургалтын алгоритмуудыг харьцуулан шинжилж, тэдгээрийн үр дүнг нарийвчлал, санамсаргүй илрүүлэлт, болон F1-оор үнэлсэн. Судалгаа нь хорт программын автомат илрүүлэлтийг сайжруулахад хамгийн тохиромжтой алгоритмуудыг тодорхойлохыг зорьсон.	Энэхүү судалгаа нь хорт программыг илрүүлэхийн тулд Random Forest (RF), Adaptive Subgradient (ASG), Extra Trees болон Gaussian Naive Bayes (NB) загваруудыг хослуулсан шинэчлэгдсэн neural network-г санал болгосон. Энэхүү хосолсон арга нь сургах болон туршилтын шатанд F1 оноо, нарийвчлал, recall, нарийвчлалын хувьд төгс үр дүнд хүрсэн. Эдгээр загваруудыг нэгтгэснээр дараалал бүхий загварыг илрүүлж, урт хугацааны хамаарлыг суралцаж хортой программыг илрүүлэх нарийвчлалыг мэдэгдэхүйц	RF	100
			SGD	100
			Extra Tree Classifier	100
			Gaussian NB	100

		сайжруулсан байна. Алдааг багасгах, илрүүлэх хурдыг нэмэгдүүлэхийн тулд олон судлаачид сургалтын багц багцад өгөгдлийг хуваах машин сургалтын аргуудыг ихээр ашиглаж байна.	DT	99
			AdaBoost	99
<p>Gorment, N. Z., Selamat, A., Cheng, L. K., &amp; Krejcar, O. (2023). Machine learning algorithm for malware detection: Taxonomy, current challenges, and future directions. IEEE Access, 11, 141045-14 1089.</p>	<p>Энэхүү судалгаа нь 2017-2022 оны хооронд хорт программыг илрүүлэх арван машин сургалтын алгоритмыг системтэйгээр судлах аргачлал (SLR) ашиглан харьцуулсан болно. Энэ нь хамгийн сүүлийн үеийн арга техникийг судалж, өмнөх судалгааны ажлуудын дутагдалтай талуудыг судалж, хортой программыг илрүүлэхэд зориулсан машин сургалтын ирээдүйн чиг хандлагыг санал болгосноороо онцлогтой.</p>	<p>Машин сургалт нь шинэ технологи болон том өгөгдөл /big data/-ийн хөгжлийн улмаас кибер аюулгүй байдалд, ялангуяа хортой программыг илрүүлэхэд чухал хэрэгсэл болж байна. Энэхүү судалгаа нь хортой программыг илрүүлэхэд ашиглагдах машин сургалтын аргуудыг авч үзэн, 77 өөр судалгааны ажлыг харьцуулж, ангиллын техник, шинжилгээний төрөл, тулгарч буй бэрхшээлүүдийг системчилж гаргасан байна. Эмпирик/туршлага дээр үндэслэсэн/ шинжилгээгээр бага болон их хэмжээний өгөгдлийг ашиглахад SVM, Decision Trees (DT), N-grams-ийн нарийвчлалын түвшин 100%-аас 98%-ийн орчимд буурч байгааг тогтоосон. Шинж чанарт суурилсан ангилал болон динамик эсвэл хосолсон шинжилгээний арга нь гарын үсэгт суурилсан болон статик аргуудаас илүү үр дүнтэй байсан. Цаашид онцлог шинж чанарыг гаргаж авах, ангиллын арга болон шинжилгээний төрлийг сайжруулахад анхаарах төлөвтэй байна.</p>	N-Grams	97.8
			KNN	92.72
			DT	92.23
			SVM	90.55
			K-Means	89

## НАРНЫ ЭРЧИМ ХҮЧНИЙ ТООЛУУРЫН СИСТЕМИЙН ХӨГЖҮҮЛЭЛТ

Б.Цэрэнтогтох<sup>1</sup>, А.Одгэрэл<sup>2</sup>

<sup>1,2</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн сургууль, Электроникийн салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: odgerel55@must.edu.mn*

**Хураангуй:** Судалгааны ажлаар ~1КВт хүртэлх чадалтай нарны панелаас ирж буй нарны эрчим хүчний хэмжиж GSM модемоор мэдээллийн төв серверт илгээх эмбэддэд төхөөрөмжийг хөгжүүлж туршсан. Уг судалгаа нь хөдөө орон нутагт нарны бага чадалтай системүүд (1КВт хүртэлх) ашигладаг малчин өрхүүд ногоон эрчим хүч үйлдвэрлэж хүлэмжийн хийг бууруулахад хувь нэмэр оруулж байна гэж үзэн үйлдвэрлэсэн эрчим хүчээ мэдээллийн төвд илгээж карбон кредит болгож бирж дээр арилжаанд оруулж орлого олох боломжийг бүрдүүлэх ажлын эхлэжээ. 1 карбон кредит нь 1 тонн CO<sub>2</sub> бөгөөд үнэ нь дэлхийн зах зээл дээр 60\$-80\$-н хооронд хэлбэлзэж байна. 1КВт чадалтай нарны систем нь жилдээ 0.73 тонн орчим CO<sub>2</sub> ялгаруулалтыг нөхдөг. Малчин өрхүүдийн хэрэглэж байгаанарны системийн чадлыг дунджаар 0.6КВт, 1 Карбон кредитийн дунджаар 70\$ гэж үзвэл жилдээ ~120.000 төг орлогоолохоор байна. Эмбэддэд тоолуурын төхөөрөмжийг төвийн эрчим хүчний системд холбохоос сэргийлж байршлын координатыг мэдээллийн төв дээр бодит хугацаанд хянана. Туршилтаар 12Вт-н чадалтай нарны панелыг сонгон ACS712A гүйдлийн мэдрэгч, NEO-6M GPS модуль, ESP32 микроконтроллер ашиглан SIM800 GSM модемоор мэдээллийн серверт өгөгдөлөө дамжуулсан. Төхөөрөмжийг хөдөө орон, нутаг болон төв суурин газрын ~1КВт хүртэлх чадалтай нарын систем ашиглаж байгаа айл өрх, албан газруудад ашиглах боломжтой.

**Түлхүүр үг:** Эмбэддэд төхөөрөмж, GPS/GSM модуль, ESP32, карбон кредит, нарны панел

### I. УДИРТГАЛ

Монгол улсын эрчим хүчний 1 жилийн хэрэглээ 9 орчим тэрбум кВт.ц бөгөөд энэ тоо жил бүр 6-8%-р нэмэгдэж байна. Үүнээс 9%-г нь сэргээгдэх эрчим хүч буюу нар, салхи, усан цахилгаан станцаас гарган авч байна [1]. Монгол улсын ерөнхийлөгч У.Хүрэлсүх манай улс НҮБ-ын уур амьсгалын өөрчлөлт, хүлэмжийн хийг бууруулах конвенцид нэгдсэнийг зарласан бөгөөд цаашид сэргээгдэх эрчим хүчний үйлдвэрлэл болон технологийг дэмжиж ажиллахыг Монгол улсын хөгжлийн алсын хараа 2050 бичиг баримтад тусгасан билээ [2]. Дэлхийн өндөр хөгжилтэй болон хөгжиж буй улсууд нь хүлэмжийн хий ялгаруулж байгаль орчин бохирдуулж байгаагаа КАРБОН КРЕДИТ ашиглан төлдөг шинэ ойлголт, төлбөрийн систем бий болж байна. Өөрөөр хэлбэл ногоон буюу сэргээгдэх эрчим хүч үйлдвэрлэж байгаа улсууд үйлдвэрлэсэн эрчим хүчээ кредит болгон борлуулдаг арилжааны платформууд үүсч байна. Үүссэн кредитийг байгаль орчин бохирдуулж хүлэмжийн хий ялгаруулж байгаа улс орон, компани, үйлдвэрүүд худалдан авдаг тогтолцоо бий болж байна. Монгол улсад URECA [3] компани энэ төрлийн арилжааны платформыг хөгжүүлэн эхний туршилтуудаа хийж эхэлсэн.

Хөдөө нарны панелтай айл нь үйлдвэрлэж байгаа эрчим хүчний хэмжээгээ мэдээллийн төвд илгээж КРЕДИТ болгон хувиргаж орлого олох боломж нээгдэх юм. Манай улсад ашиглаж байгаа өрхийн хэмжээний нарны (1КВт чадал хүртэлх) системүүд нь тоолуур байхгүй. 1КВт-с дээш системүүдэд тоолуур байгаа боловч мэдээллийг нь авахын тулд үйлдвэрлэгчээс зөвшөөрөл авч нэмэлт төлбөр төлөх болдог. Айл өрх, албан байгууллагуудад суурилуулсан сэргээгдэх эрчим хүчний үүсгүүрийн (нар, салхи, ус) үйлдвэрлэж байгаа эрчим хүчийг хэмжих төхөөрөмжийг хөгжүүлж мэдээллийн төвд

илгээж тооцоолох ажлын эхлүүлэх нь уг судалгааны ажлын зорилго юм.

Энэ судалгаанд ашигласан SIM800 GSM/GPRS модем нь цуваа холболтоор микроконтролёртой холбогдон AT командыг ашиглан мэдээллийг дамжуулдаг. Модем нь командыг хүлээн авсныхаа дараа үр дүнг буцаан илгээдэг. Технологи хөгжихийн хэрээр шинэчлэгдсэн хувилбарууд гарч байна. Монголд улсад түгээмэл байдаг модуль нь: GSM shield 900, GSM shield 900A, GSM shield 800, A7, A6 юм. Эдгээр нь хоорондоо өгөгдөл дамжуулах хурдаараа ялгаатай.

NEO-6M GPS нь 1.5Гц давтамж дээр ажилладаг бага чадлын, хурд, хугацаа болон байршлын нарийвчлал сайтай модуль юм. GPS (Global positioning system) гэдэг нь дэлхийгээс 7440 км зайд байрлах орбит замаар явах 24 хиймэл дагуулуудаас бүрдэнэ. Эдгээр хиймэл дагуулууд нь дэлхийг өдөрт 2 удаа тойрон эргэж, дэлхийн аль ч цэгт байгаа GPS хүлээн авагчтай хэрэглэгчийн байрлалыг цаг хугацаа болон байрлалыг тодорхойлж өгдөг сансарын хиймэл дагуулуудын систем юм. GPS үйлчилгээ нь анх цэргийн зориулалтаар гарсан боловч иргэний болон арилжааны чиглэлээр илүү өргөн ашиглагдаж байна. Энэ системийн дагуулуудаас ирэх дохиолол тасралтгүй бөгөөд хэрэглэгч, хүлээн авагчийн тоонд хязгаар байхгүй, мөн үйлчилгээ үзүүлсэний төлбөр гэж байдаггүй. GPS технологийн үндэс нь маш өндөр нарийвчлалтай цаг хугацаа болон байрлалын талаархи мэдээлэл байдаг. Хиймэл дагуулууд газрын станцаас ирэх дохиоллыг хэмжин өөрийн байрлалыг нарийвчлан тооцоолж, энэ мэдээллээ тасралтгүй цацдаг.

GPS хүлээн авагчийн байрлал тодорхойлоход 3-аас багагүй хиймэл дагуул ашиглана. Нэг доор хүлээн авсан мэдээлэл анализ хийж өөрийн байгаа байрлалыг (уртраг, өргөрөг) гэсэн хоёр хэмжээсээр тодорхойлно. Харин дөрөв ба түүнээс олон хиймэл

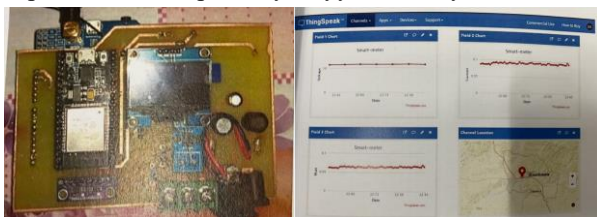
дагуулаас хүлээн авсан дохиоллын тусламжтайгаар байрлалыг (уртраг, өргөрөг, далайн түвшинтэй харьцуулан өндөрлөг) гурван хэмжээсээр тодорхойлдог. GPS-г дэлхийн хаана ч ашиглаж болох боловч агуй, хонгил, машины граж, усан дор зэрэг газар GPS-н сигналыг дамжуулах боломжгүй байдаг [4].

GPS систем гурван хэсгээс тогтоно.

- ✓ Сансрын хэсэг
- ✓ Удирдлагийн хэсэг
- ✓ Хэрэглэгчийн хэсэг

**II. СУДЛАГДСАН БАЙДАЛ**

HCS-LTS-25A гүйдлийн мэдрэгч, ESP32 микроконтроллёр болон SIM808 GPS/GSM shield ашиглан хөгжүүлсэн сэргээгдэх эрчим хүчний хяналтын системийг [5]-д хөгжүүлсэн. Мэдээллийг ThingSpeak бэлэн сервер ашиглан хүлээн авч харуулсан. Уг судалгааны ажилд ашигласан гүйдлийн мэдрэгч нь contact-less буюу дамжуулагч кабелийг мэдрэгч дундуур сүвлэж явуулдаг нь аюулгүй байдал талаасаа сайн боловч мэдрэгчийн нарийвчлал нь харьцангуй муу байдаг сул талтай.



1-р зураг. Төсөөтэй ажил-1: төхөөрөмж ба вэбийн харагдах байдал [5]

Beijing Lewei IOT Technologies компани Wi-Fi модул бүхий цахилгаан тоолуурын төхөөрөмжийг хөгжүүлж зах зээлд гаргасан [6]. Компани нь өөрсдийн хөгжүүлсэн вэб сервертэй бөгөөд тоолуурууд нь утасгүй сүлжээнд холбогдон мэдээллээ Интернетийн сүлжээ ашиглан серверт илгээн графикаар болон хүснэгтээр харуулж статистик тооцооллыг хийдэг.



2-р зураг. Төсөөтэй ажил-2: тоолуур болон вэб серверийн харагдах байдал [6]

PIC18F4550 микроконтроллёр ашиглан нар болон салхины үүсгүүрээс ирж байгаа энергийг том хэмжээний батерейнд хадгалах судалгааны ажлыг [7]-д хийсэн. Нарны энергийн AC буюу хувьсах гүйдэл рүү хувиргаж (grid inverter) төвийн эрчим хүчний шугамд нийлүүлэх системийг хөгжүүлж туршсан судалгааны ажлыг [8]-д хийсэн. Өгөгдлөө GSM-ийн модемоор дамжуулж, LCD дэлгэц дээр

системийн бүх үзүүлэлтийг гаргаж хянасан. ATmega-2560 микроконтроллёр ашигласан IoT-д суурилсан SCADA системээр сэргээгдэх эрчим хүчийг хянах судалгааны ажлыг [9]-д хийсэн. Уг ажил нь Матлаб програм дээр симуляци хийж ThingSpeak бэлэн серверт өгөгдөлөө Wi-Fi модул ашиглан дамжуулж харуулсан.

**III. СИСТЕМИЙН ДИЗАЙН БА ШИЙДЭЛ**

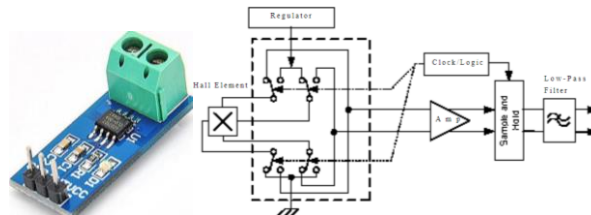
Системийн ерөнхий бүтцийн схемийг дараах зурагт харуулав. 12Вт-н нарны панел, ACS712 гүйдлийн мэдрэгч, хүчдэл хуваагч, OLED дэлгэц, SIM800 GSM модем, бага чадлын NEO-6M GPS модулуудыг төхөөрөмжийг хөгжүүлэхэд ашигласан. GSM модем нь AT командууд ашиглан мэдээллээ дамжуулдаг. ESP32 2 цөмтэй микроконтроллэрыг удирдлагаар ашигласан.



3-р зураг. Системийн бүтцийн схем

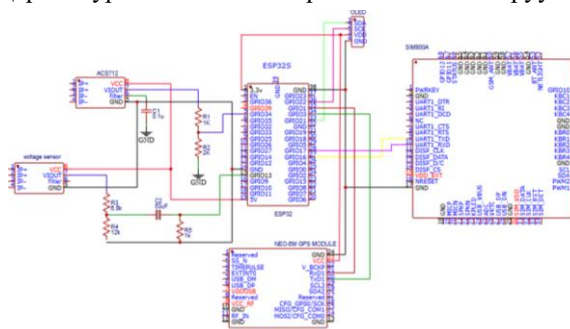
Энэ контроллёр нь RISC-V архитектуртай, өөртөө Bluetooth болон Wi-Fi модул агуулсан бөгөөд IoT хэрэглээнүүдэд илүү тохиромжтой. Тэжээлээр нь LiPo төрлийн 7.4В, 450mAh-н багтаамжтай батерейг сонгон ашигласан.

Гүйдлийн мэдрэгчээр ACS712 төрлийн мэдрэгчийг сонгосон. Энэ мэдрэгч нь аналого гаралттай бөгөөд гүйдэлтэй шугам дээр цуваа холбож ашигладаг. Гүйдэл урсахад үүссэн соронзон оронгын нөлөөллөөр хүчдэлийн өөрчлөлт үүсгэх зарчмаар ажилладаг.



4-р зураг. ACS712 гүйдэл мэдрэгчийн гадаад болон дотоод бүтэц

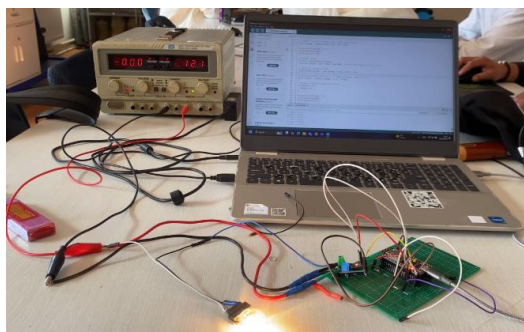
Дараах зурагт системийн зарчмын схемийг харуулав.



5-р зураг. Төхөөрөмжийн зарчмын схем

#### IV. ТУРШИЛТ, ҮР ДҮН

Сонгож авсан элемент, модулуудыг угсарч туршилт хийсэн загварыг дараах зурагт харуулав. Эхний туршилтаар нарны панелиг холболгүй гүйдэл мэдрэгчийн оролтонд шууд тэжээлийн блокоос гүйдлийг өгч өөрчлөн эмбэддэд төхөөрөмж гүйдлийн мэдрэгчийн тооцоолж байгаа утга болон мултиметрийн заалттай харьцуулсан туршилт хийсэн. Дараах зурагт төхөөрөмжийг тэжээлийн блоктой холбон туршилт хийж байгааг харуулав.



6-р зураг. Эмбэддэд төхөөрөмжийг тэжээлийн блоктой холбон туршилт хийж байгаа байдал

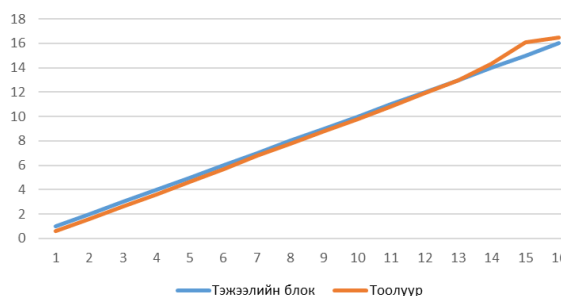
Дээрх зургаас харахад дээд буюу цэнхэр өнгөтэй шугам нь мултиметрийн утга, доорх буюу улбар шар өнгөтэй шугам нь эмбэддэд төхөөрөмжийн бодсон гүйдлийн утга юм. Мултиметрийн алдааг 0 гэж үзвэл гүйдлийн мэдрэгч ACS712 нь 1.7% орчмын алдаатай гэж харагдаж байна.



7-р зураг. Гүйдэл мэдрэгчийн утгыг мултиметрийн утгатай харьцуулсан график

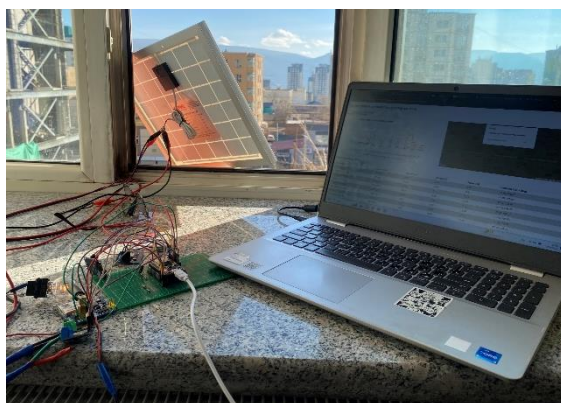
Зураг 8-д хүчдэлийн утгыг харьцуулж харуулав. Дээд буюу цэнхэр өнгөтэй шугам нь тэжээлийн блокоос өгч буй хүчдэлийн утга, доорх буюу улбар шар өнгөтэй шугам нь эмбэддэд тоолуурын бодсон хүчдэлийн утга юм. Тэжээлийн блокын алдааг 0 гэж үзвэл хүчдэл хуваагуур мэдрэгч нь 9.7% орчмын алдаатай байгаа нь харьцангуй их байна.

Хүчдэлийн харьцуулалт



8-р зураг. Хүчдэл мэдрэгчийн утгыг мултиметрийн утгатай харьцуулсан график

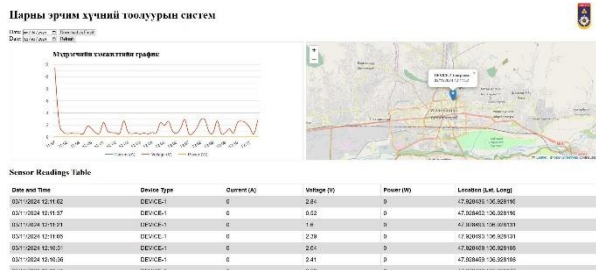
Дараах зурагт 12В-ын нарны панелиг эмбэддэд төхөөрөмжид бодитоор холбож туршилт хийж байгааг харуулав. Карбон кредит тооцох үед төхөөрөмжийг төвийн эрчим хүчний системд холбож хуурамч өгөгдөл илгээхээс сэргийлэхийн тулд GPS ашигласан. GPS нь төхөөрөмжийг анхны байршлаасаа хөдөлсөн эсэхийг хянах бөгөөд хөдөлсөн тохиолдолд мэдээллийн төв дээр дохиолол өгнө.



9-р зураг. Нарны панелиг холбож бодит туршилт хийж байгаа байдал

Нарны панелиг урд зүгт 45 градусын налууугаар байрлуулна. Эмбэддэд тоолуурын төхөөрөмжөөс GSM-н модемоор нарны панелаас ирж буй гүйдэл хүчдэл, чадал, төхөрөмжийн дугаар, огноо болон байршлын уртраг, өргөрөгийн мэдээллийг мэдээллийн серверт илгээнэ. Ирсэн уртраг өргөрөгийн мэдээллийг Google map-д холбож сервер дээр харуулна.

Дараах зурагт мэдээллийн серверийн харагдах байдлыг харуулсан. Гүйдэл, хүчдэл, чадлыг графикаар болон хүснэгтээр харуулсан. Мөн Google map дээр төхөөрөмжийн одоогийн байршлыг харуулсан. Мөн өгөгдлийг хугацааны интервалаар эксел файлаар авах функцтэй. Ашиглаж буй NEO-6M GPS модулын нарийвчлалаас хамаарч байршлын алдаа 1-5м дотор байсныг туршилтаар тогтоосон.



10-р зураг. Мэдээллийн серверийн харагдах байдал

## ДҮГНЭЛТ

Судалгааны ажлаар ~1КВт хүртэлх чадалтай нарны системийн үйлдвэрлэж байгаа чадлын мэдээллийн төвд GSM сүлжээ ашиглан дамжуулах эмбэддэд төхөөрөмжийг хөгжүүлж туршсан. Төхөөрөмжийг төвийн эрчим хүчний шугамд байнга холбоотой байхаас сэргийлж анхны байршлыг тогтоож, хөдөлгөсөн тохиолдолд Google Map-р хянаж дохиолол өгөхөөр програмчилсан. Ашигласан гүйдлийн мэдрэгч ACS712-н алдаа нь 1.7%, харин хүчдэл хуваагчийн алдаа нь 9.7% байсан нь харьцангуй их байна гэж дүгнэж цаашид алдааг багасгах тал дээр анхаарах шаардлагатай гэж үзсэн. NEO-6M GPS модулын нарийвчлалаас хамааран байршлын алдаа нь 1-5м дотор байсан.

Судалгааны ажлаар хөгжүүлсэн эмбэддэд тоолуурын төхөөрөмжийг хөдөө Монгол гэрт болон, аймаг сумын төвд ~1КВт хүртэлх чадалтай нарны эрчим хүч ашиглаж байгаа айл, өрхүүд шууд ашиглах боломжтой болно. Монгол улсад 2022 оны тооллогоор 305,000 орчим малчин өрх бүртгэгдсэн бөгөөд үүний 1/3 орчим нь буюу 100,000 орчим нь өрхийн нарны бага чадлын эрчим хүч ашиглан ТВ, хөргөгч, гэрэлтүүлэгээ шийдэж байна. Нэг эмбэддэд төхөөрөмжийн үнэ нь ойролцоогоор 300,00~350,000 төг болно гэж тооцсон. 100,000 малчин өрх \* 320,000төг=32 тэрбум төг зах зээл байна гэж үзэж байна. Эдгээр айллууд нь өөрсдийн сэргээгдэх эрчим

хүчний төхөөрөмжөөр үйлдвэрлэсэн цахилгаан энергийн хэмжээгээ мэдээллийн төвд илгээн баталгаажуулж КАРБОН КРЕДИТ болгон арилжаалах боломж үүсэх юм. 1 КАРБОН КРЕДИТ нь 1 тонн CO<sub>2</sub> бөгөөд үнэ нь дэлхийн зах зээл дээр 60\$-80\$-н хооронд хэлбэлзэж байна. 1КВт чадалтай нарны станц нь жилдээ 0.73 тонн орчим CO<sub>2</sub> ялгаруулалтыг нөхдөг гэсэн судалгаа байна [10]. Малчин өрхүүдийн хэрэглэж байгаа нарны системийн чадлыг дунджаар 0.6КВт, 1 Карбон кредитийн дунджаар 70\$ гэж үзвэл 2 жилийн дотор төхөөрөмжийн үнээ төлөөд цаашдаа энэ хэмжээний орлого олох боломжтой байна.

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Эрчим хүчний зохицуулах хороо <https://erc.gov.mn/>
- [2] “Алсын хараа 2050” Монгол улсын урт хугацааны хөгжлийн бодлого, МУ-ын ЗГ, УБ хот, 2019 он
- [3] Юрека ХХК, ureca.com
- [4] Н.Өсөхбаяр, Б.Баасандорж, Э.Эрхбилгүүн “GSM сүлжээ дээр суурилсан осол, гэмтлээс урьдчилан сэргийлэх систем” Бакалаврын төгсөлтийн ажил, “Хүрээ” Мэдээлэл холбооны технологийн дээд сургууль, 2018 он
- [5] Л.Саруулбуян бакалаврын дипломын ажил “Сэргээгдэх эрчим хүчний тоолуурын хөгжүүлэлт” 2022 он
- [6] Beijing Lewei IOT Technologies компани <https://www.iammeter.com/>
- [7] Ersan Kabalci, Alper Gorgun, Yasin Kabalci "Design and implementation of a renewable energy monitoring system" 4th International Conference on Power Engineering, Energy and Electrical Drives, 21 Oct 2013, DOI: 10.1109/PowerEng.2013.6635759
- [8] Ahmed Shah Rasheed Tajwar, Abir Ahmed, Md. Rifat Hazari, Mohammad Abdul Mannan "Solar Photovoltaic-Based Smart Metering System" 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), 05-07 Jan 2021, DOI: 10.1109/ICREST51555.2021.9331098
- [9] Md Ohirul Qays, Musse M. Ahmed, M. A. Parvez Mahmud "Monitoring of renewable energy systems by IoT - aided SCADA system", Journal of Energy Science Engineering, Feb 2022
- [10] <https://www.quora.com/>

## УХААЛАГ ХӨТӨЧ

Мөнхбаяр ТҮМЭН-АЮУШ<sup>1</sup>, Чулуунжин МИЧИДГОО<sup>2</sup>, Сүхбаатар БАТМӨНХ<sup>3</sup>, Соном-Очир ӨЛЗИЙБАЯР<sup>4</sup>  
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: ulziibayar@must.edu.mn<sup>1\*</sup>*

**Хураангуй** — Мэдээллийн технологийн хөгжил нь хүн бүрийн өдөр тутмын амьдралд дэвшил авчирч байгаа энэ цаг үед харааны бэрхшээлтэй иргэд ч эдгээр дэвшилтэт технологийг хүртэн, өөрт тохирсон шийдлээр хангагдах шаардлагатай. Энэхүү судалгаагаар бид Монгол орны нөхцөлд тохирсон, харааны бэрхшээлтэй иргэдийн аюулгүй байдал, бие даасан байдлыг хангах зорилгоор ухаалаг хөтөч системийг хөгжүүлэхэд анхаарлаа хандуулсан. Бид гар утасны камерыг ашиглан объект илрүүлэх (object detection), объектын зай тодорхойлох (object distance estimation), текстийг яриа болгон хувиргах (text-to-speech) зэрэг машин сургалтын загвар, техникүүдийг ашиглан харааны бэрхшээлтэй иргэдэд хэрэглэхэд хялбар, үнэ төлбөргүй, орон зайн мэдээллийг аудио хэлбэрээр дамжуулах боломжтой системийг боловсрууллаа. Судалгааны эхний шатанд Монгол улсын явган хүний зам дээрх гол объектуудыг илрүүлэх YOLOv5 загварт суурилсан объект таних алгоритмыг ашиглан 90 - 120 секундний урттай 20 бодит замын бичлэг дээр туршилт хийж, объект илрүүлэх болон зай тодорхойлох модулиудыг 98.58% болон 98.36%-ийн нарийвчлалтайгаар тус тус баталгаажуулсан. Аудио мэдээлэх чадвар нь шаардлагын дагуу 98%-ийн үнэлгээтэй гарсан бөгөөд ярианы хурд, өнгийг тохируулах боломж бүхий API ашиглан текстийг аудио файлд хөрвүүлэх процессыг амжилттай хэрэгжүүлсэн. Энэ үр дүн нь системийн бодит цагийн туршилтад хэрэглэхэд найдвартай бөгөөд Монгол улсын нөхцөлд хэрэглэгчдийн аюулгүй, бие даасан байдлыг хангахад дэмжлэг болох боломжтойг харууллаа. Цаашид GPS-ийн функцийг нэмж, асран хамгаалагчид бодит цагийн байршлын мэдээлэл дамжуулах бүрэн ажиллагаатай, харааны бэрхшээлтэй иргэдэд зориулсан үнэ төлбөргүй программ болгон хөгжүүлэхээр зорьж байна.

**Түлхүүр үг** — *object distance estimation, object detection, харааны бэрхшээлтэй иргэн, YOLOv5, TTS*

### I. УДИРТГАЛ

Ухаалаг хөтөч систем нь харааны бэрхшээлтэй иргэдийн өдөр тутмын хэрэгцээнд нийцсэн, аюулгүй зорчих боломжийг бүрдүүлэх зорилготой технологийн шийдэл юм. Дэлхийн Эрүүл Мэндийн Байгууллагын (ДЭМБ)-ын мэдээлснээр, дэлхий даяар 246 сая хүн харааны бэрхшээлтэй байгаагийн 36 сая нь хараагүй, 210 сая нь хараа муутай байдаг [1]. Монгол Улсад ойролцоогоор 11,400 орчим харааны бэрхшээлтэй хүн амьдардаг бөгөөд үүний 3 мянга орчим нь Улаанбаатар хотод оршин суудаг [2]. Эдгээр иргэд өдөр тутамдаа цагаан таяг ашиглан зорчдог ч тэдний аюулгүй байдал, зорчих нөхцөл бүрэн хангагдаагүй байна. Иймээс, ухаалаг хөтөч системийг боловсруулсан бөгөөд энэ нь орчин үеийн технологийн дэвшлийг ашиглан харааны бэрхшээлтэй иргэдийн амьдралын чанарыг дээшлүүлэх чухал шийдэл болж байна. Тийм ч учраас судлаачид энэ төрлийн судалгааг сүүлийн жилүүдэд маш эрчимтэй өрнүүлж байна. Тэдгээр судалгаануудыг ашигласан технологи, арга аргачлалаас хамааруулан дүрсийн боловсруулалтад суурилсан арга, төхөөрөмжид суурилсан арга болон эдгээр аргын хосолсон арга гэсэн гурван бүлэгт хувааж үздэг. Бид эдгээр аргуудаас хамгийн өртөг багатай боловч, үр дүн сайтай арга болох дүрсийн боловсруулалтад суурилсан аргаар хийхээр зорьсон.

Өмнөх судалгаануудад Convolutional Neural Networks (CNN)-г ашиглан объект илрүүлж, таних системүүдийг бүтээхэд бага зардалтай ч давуу талтай гэж үзсэн байдаг. Гэвч эдгээр судалгаанд хэд хэдэн сул талууд илэрсэн. Тухайлбал, [3] дугаартай судалгаанд CNN болон LSTM ашиглан хязгаарлагдмал зураг дээрх объектыг танин, аудио хэлбэр болгон хувиргах туршилтыг хийсэн байсан. Энэ систем нь тооцооллын хурд сайтай байсан боловч бодит цагийн үйлдлийг дэмждэггүй байсан нь бодит орчинд хэрэглэх боломжийг хязгаарласан.

2020 онд хийгдсэн бас нэгэн судалгаа [4]-д YOLOv5 ашиглан харааны бэрхшээлтэй хүмүүсийн хөдөлгөөнд дэмжлэг үзүүлэх зорилгоор орчны объект илрүүлэх системийг боловсруулсан. YOLOv5-ийн тусламжтайгаар илрүүлэх хурд сайжирсан хэдий ч уг систем нь зөвхөн хязгаарлагдмал өгөгдлийн сантай (8000 зураг) бөгөөд 16 төрлийн объектыг илрүүлэх боломжтой байсан тул хэрэглээний цар хүрээ багатай хэвээр байв. Үүнээс гадна уг систем нь илэрсэн объектын талаар дуу хоолойн мэдээлэл дамжуулах боломжгүй байсан нь хэрэглэгчдэд шууд мэдээлэл хүргэх тал дээр дутагдалтай хэвээр байлаа.

Иймд, ухаалаг хөтөч систем нь дээр дурдсан асуудлуудыг шийдвэрлэх, аюулгүй зорчих орчныг бүрдүүлэх ач холбогдолтой. Судалгааны ажил 1-Building a voice based image caption generator with deep

learning, 2021 Судалгааны ажил 2- Indoor objects detection and recognition for an ict mobility assistance of visually impaired people, 2020

## СУДАЛГААНЫ АЖЛУУДЫН ХАРЬЦУУЛАЛТ

1-Р ХҮСНЭГТ

Судалгааны ажил	Судалгааны ажил 1	Судалгааны ажил 2
Модель	CNN болон LSTM	YOLO v5
Аудио	Тийм	Үгүй
Сул тал	Архитектур дурдаагүй ба 5000 зурагтай өгөгдлийн багцыг ашигласан ба олон функцийг дэмжихгүй.	Доторх зургууд нь маш хязгаарлагдмал, цөөхөн (8000 зурагтай зөвхөн 16 доторх объектыг илрүүлэх боломжтой)

Эдгээр судалгааны ажлууд нь манай системийн үйл ажиллагаатай төстэй бөгөөд тус судалгаанд үндэслэн өөрийн системд сайжруулалт хийх шаардлагатай гол асуудлуудыг илрүүлэхэд тус болсон. Эндээс үзэхэд эдгээр хязгаарлалтуудыг үндэслэн бидний судалгааны ажилд YOLOv5 загварыг ашиглаж, илүү өргөн хүрээний объект таних, бодит хугацаанд мэдээллийг аудио хэлбэрээр дамжуулах боломжийг оруулснаар хэрэглэгчдэд илүү хүртээмжтэй, өргөн цар хүрээтэй системийг санал болгож байна. Мөн түүнчлэн дан ганц объект илэрүүлэн, уг объектыг тодорхойлохын зэрэгцээ тухайн объектын орон зайн байршил, хөдөлгөөний чиглэл, хурд зэрэг нэмэлт мэдээллийг харааны бэрхшээлтэй хүнд мэдээлсэнээр бодит орчноо илүү сайн ойлгож, шаардлагатай шийдвэр гаргахад туслах юм.

## II. ХЭРЭГЛЭГЧИЙН СУДАЛГАА

Харааны бэрхшээлтэй хүмүүс харааны хагас бэрхшээлтэй эсвэл хараа бүрэн алдсан байдаг. Энэ нь тэдний өдөр тутмын амьдралд ихээхэн нөлөөлж, хөдөлгөөн, ажил гүйцэтгэх чадвар, амьдралын чанарт нь нөлөөлсөөр байгаа. Ийм хөгжлийн бэрхшээлтэй хүмүүсийн дийлэнх нь 50-иас дээш насныхан байдаг.

Харааны эмгэгийн олон шалтгаан бий. Булчингийн доройтол мөн зарим генетикийн эмгэгүүд нь харааг муутгадаг. Нүд, толгой болон

бусад төрлийн гэмтэл нь нүдний өвчинд хүргэдэг бөгөөд энэ нь эмгэгийг үүсгэдэг. Нүдийг гэмтээж, харааны эмгэгт хүргэдэг бусад өвчинд чихрийн шижингийн ретинопати, катаракт (cataracts), глауком (glaucoma), насжилттай холбоотой доройтол орно. Хорт бодист өртөх, тод дэлгэц, хурц гэрлийг удаан хугацаагаар үзэх, контакт линзийг удаан хугацаагаар ашиглах зэрэг нь хараа бүрэн алдагдахад хүргэдэг. Энэ бол хэзээ алга болох асуудал биш бөгөөд хараа муудсан, хараагүй болсон ч эргэн тойрон, урд байгаа саад тотгорыг таних систем нэн шаардлагатай байгаа билээ.

Манай улсад автобус тэр бүр буудал дээрээ зогсдоггүй, чиглэлийг гадагшаа зарлаж, мэдээлдэггүй нь харааны бэрхшээлтэй хүн нийтийн тээврээр үйлчлүүлэхэд маш хэцүү. Явган хүний зам дагуух гэрлийн шон, модны мөчир, рекламн самбар, дугуй зэрэг нь харааны бэрхшээлтэй хүнийг нийгмийн харилцаанд ороход том саад болдог. Энэ талаар зохих байгууллагад удаа дараа мэдэгдсэн ч тодорхой үр дүнд хүрээгүйг МХҮХ-ны Ерөнхийлөгч Б.Ганзориг онцлов.[2]

Хэрэглэгчийн шаардлага [5] :

1. Аудио хэлбэрээр мэдээлэх
2. Объектын зайг тооцоолох
3. Объектын хөдөлгөөний чиглэлийг болон хурдыг мэдээлэх

Утасны ашиглалт ба яагаад шаардлагатай байгаа эсэх:

Харааны бэрхшээлтэй иргэд нь хэн нэгний тусламжгүйгээр хүссэн газар руугаа явах буцаж ирэх нь тэдний наад захын хүсэл байдаг ба үүний тулд таягийн сургалтад явж эхэлдэг. Харин манай төсөл нь таягтай хосолж ажиллах цаашлаад таяггүй явах ч боломжийг олгох боломжтой болно. Үүний хөгжүүлэх ч боломжтой.

- Хот төлөвлөлт, дэд бүтэц муу байгаа
- Гэмтэж бэртэж, осол авар гарах г.м

## III. СУДЛАГДСАН БАЙДАЛ

Системийг хөгжүүлэхдээ дэлхий дахинд болон Монголд ямар байдлаар судлагдсан, хэрэгжсэн талаар холбогдох дараах судалгааг хийсэн. Объектыг таних, орчиндоо дасан зохицох зэрэг үйл явц нь харааны бэрхшээлтэй иргэдэд олон сорилтыг бий болгодог бөгөөд эдгээр асуудлыг шийдвэрлэхийн тулд судлаачид компьютер болон хиймэл оюуны (AI) алгоритмуудыг өргөнөөр ашиглах болсон. Харааны бэрхшээлтэй хүмүүст зориулсан объект илрүүлэх

системүүдийн гол зорилго нь илрүүлэлтийн хурд, нарийвчлалыг сайжруулж, олон төрлийн объектыг бодит цагийн горимд зөв таньж илрүүлэхэд чиглэгддэг.

*A. Судалгааны ажил*

Энэхүү судалгаанд [6] YOLOv4 болон Resnet101 загваруудыг хослуулж, олон объект таних нарийвчлалтай системийг хөгжүүлэхэд анхаарсан. YOLOv4 нь объектыг илрүүлэх өндөр үр дүнтэй загвар бөгөөд хурд, нарийвчлалын үзүүлэлтээрээ нэр хүндтэй бол Resnet101 нь гүний сургалтын нейрон сүлжээний архитектур ашиглан илүү нарийн таних чадварыг бий болгосон. Судалгааны үр дүнд гарсан YOLOv4\_Resnet101-ийн өөрчилсөн хувилбар нь 4000 туршилт дээр 96.34%-ийн нарийвчлал, 0.073%-ийн алдааны үзүүлэлттэй байсан бөгөөд энэ нь харааны бэрхшээлтэй хүмүүст өдөр тутмын амьдралд тулгардаг объект таних асуудлыг шийдвэрлэхэд өндөр ач холбогдолтой болсон.

- Тус судалгаагаар дээрх объект илрүүлэх загварыг текстээс яриа руу хөрвүүлэх технологитой хослуулсан бөгөөд энэ нь харааны бэрхшээлтэй хүмүүст хүрээлэн буй орчноо бодит цагийн хоолойгоор дамжуулан ойлгож, мэдрэхэд тусалсан. Бодит цагийн туршилтууд болон хэрэглэгчийн судалгааны үр дүнд YOLOv4\_Resnet101 интеграцийн үр дүн, бодит байдал дээр ажиллах чадвар нь батлагдсан бөгөөд энэ нь харааны бэрхшээлтэй хүмүүст эргэн тойрны орчиндоо илүү дасан зохицох боломжийг нээж өгсөн.

*B. Судалгааны ажил*

Сүүлийн жилүүдэд текстээс яриа үүсгэх системүүд (TTS) нь хиймэл оюун ухаан болон гүний сургалтын (deep learning) аргачлалуудын тусламжтайгаар хурдацтай хөгжиж, хүн-компьютерийн харилцааны асуудлыг шийдэх чухал хэрэгсэл болж байна. TTS системүүд нь янз бүрийн хэлэнд зориулсан загваруудыг агуулдаг бөгөөд үүнийг сайжруулахад харилцааны хиймэл оюун ухаан, чатбот, intelligent speech interaction зэрэг олон төрлийн хэрэглээний хувилбарууд хөгжүүлэгдсээр байна. Энэ нь олон хэлний онцлогийг харгалзан үзэж, хэрэглэгчийн хувьд илүү дуу хоолойн уншлагыг бий болгоход тусалж байгаа юм.

- Дээрх судалгаанд TTS системийг хөгжүүлэхэд тулгарч буй гол

бэрхшээлүүдийг судалж, тэдгээрийг шийдвэрлэхэд ашиглагдаж буй аргачлалуудыг тоймлон багтаасан. Санах ой, машин сургалт, гүний сургалтын загваруудыг ашиглах нь TTS системийн чанарыг сайжруулж, текстээс яриа үүсгэх нарийвчлал, хурдыг нэмэгдүүлэх, хэлний суурьтай загваруудын үгийн алдаа болон санах ойд зарцуулах хэрэглээг бууруулахад онцгой үр дүнтэй болохыг харуулсан.

АШИГЛАСАН ТЕХНОЛОГИУД

*2-Р ХҮСНЭГТ*

Paper Title	Methods
A deep learning approaches in text-to-speech system: a systematic review and recent research perspective	<ul style="list-style-type: none"> <li>• таних хурд(rate),</li> <li>• нарийвчлал (accuracy),</li> <li>• TTS score,</li> <li>• precision, recall</li> <li>• F1-score зэрэг чанарын хэмжүүрүүд.</li> </ul>
Enhancing Object Detection for VIPs Using YOLOv4_Resnet101 and Text-to-Speech Conversion Model	<ul style="list-style-type: none"> <li>• YOLOv4_Resnet101</li> <li>• MS COCO dataset</li> </ul>

*C. Судалгааны ажил*

Судалгааны ажлуудын нэг болох "Third Eye" хэмээх энэ аргачлал нь YOLOv5 загвар болон текстээс яриа үүсгэх (TTS) технологийг ашиглан илүү өндөр нарийвчлалтай объект илрүүлж, хараагүй хүмүүст бодит цагийн мэдээлэл дамжуулах системийг хөгжүүлэх судалгаа юм.

Third Eye систем нь нийт 95 төрлийн объектыг таних чадвартай бөгөөд үүнд 15 төрлийн тусгайлсан объектыг агуулсан dataset болон MS COCO 2017 dataset-ийг ашигласан. Загварын илрүүлсэн объектыг текст болгон хувиргаж, дараа нь pyttsx3 болон gTTS зэрэг Python программчлалын хэл дээрх TTS сангуудын тусламжтайгаар аудио формат руу

хөрвүүлсэн. Эдгээр TTS сангуудыг харьцуулж туршсанаар pyttsx3 нь бодит цагийн горимд илүү өндөр хурдтай ажиллаж, илүү найдвартай үр дүн гаргасан нь харааны бэрхшээлтэй хүмүүст сонсголын хариу өгөх хугацааг багасгаж, мэдээллийг хурдан дамжуулахад онцгой үүрэгтэй болохыг баталсан.

- Аудио хэлбэрээр үүсгэх үед pyttsx3 нь ямар ч интернэт холболт шаарддаггүй, харин нөгөө талаас gTTS нь байнгын интернэт холболт шаарддаг болохыг ажигласан. Аудио файл үүсгэхийн тулд gTTS нь Google-ийн серверүүд рүү текст илгээж, дараа нь буцааж өгдөг. Тиймээс pyttsx3-ийг gTTS-ээс илүү ашигтай гэж үзсэн. Тус судалгааны ажлаас манай баг нь аудио бүтээхэд зарцуулах цаг хугацаа, саатал, lib, сүлжээний холболт зэргийг мөн харгалзан үзэх ёстойг анхаарсан. Учир нь бид муу сүлжээ гэх мэт гаднын хүчин зүйлийн нөлөөнд автахгүй бүтээхийг хүсч байна.

**D. Судалгааны ажил**

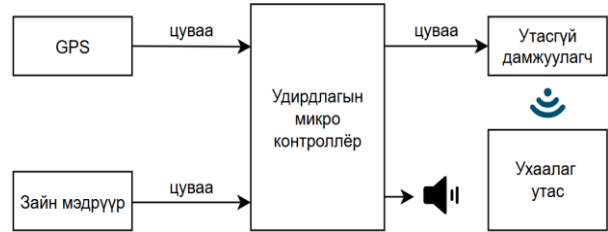
Дэлхий олон улсад хэрэглэж буй цагаан таягийг Монгол улсын нөхцөл байдалд зориулсан, ажиллагааны шинэлэг загвартай, ухаалаг болгох зорилгоор техникийн шийдэл гаргаж, програмчилсан байсан. [10] Уг таяг нь :

- Ультра - соник : Таяг дээр байрлах сенсор нь хэрэглэгчийн мөрнөөс дээш байрласан саадыг мэдрэч, хэрэглэгчийн програмд мэдээлнэ.
- GPS модуль : Асран хамгаалагч болон төөрсөн тохиолдолд товчлуурууд дарна өөрийн одоогийн байршлыг заасан мессежийг илгээнэ.
- Bluetooth : 2G дэмждэг СИМ суулгаснаар хаягийн мэдээлэл илгээгдэнэ.

Тухайн таягийн үзүүлэлт :

- Таягийн үнэ 2019 оны ханшаар 131,300 төгрөг болсон.
- Чийгийн мэдрүүр нь усны гүнийг мэдрэдэг
- Монгол хэл дээр ажилладаг.

Хэрэглэгчийн хариу : Өмнө өмнөх жилүүдэд ухаалаг таяг хийсэн олон оюутнууд байсан ба зөвхөн өмнө нь байгаа саадыг мэдрэх л үүрэгтэй байсан. Үүнийг цаашлаад сайжруулах хэрэгтэй байгаа.



1-р зураг. Системийн ерөнхий бүтэц

**IV. ТӨСЛИЙН ХЭСЭГ**

Төслийн үйл ажиллагаа:

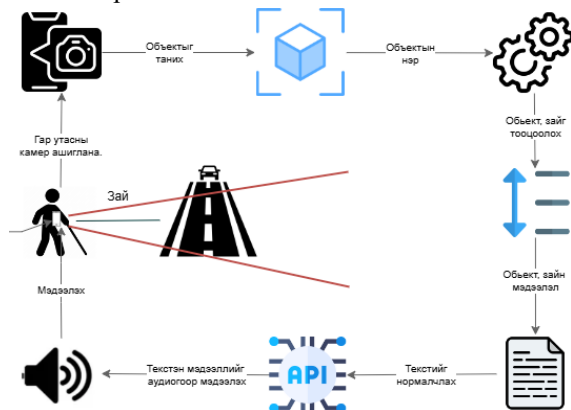
Төслийн үйл ажиллагаа нь харааны бэрхшээлтэй иргэдийн аюулгүй, бие даасан байдлыг хангахад чиглэсэн бөгөөд ухаалаг хөтөч системийг хөгжүүлэх, турших, хэрэглэгчдийн хэрэгцээнд нийцүүлэх ажлуудаас бүрдэнэ. Төслийн эхний шатанд Монгол Улсын нөхцөлд тохирсон хэд хэдэн объект таних, зайг тооцоолох технологиудыг судалж, YOLOv5 алгоритмыг ашиглан үндсэн загварыг боловсруулсан.



2-р зураг. Системийн ерөнхий ажиллагаа

Дараагийн шатанд системийн чанарыг сайжруулахын тулд туршиж үзэх, алдааг илрүүлэх, нарийвчлан хөгжүүлэх ажлууд хийгдэж байна.

Үүний зэрэгцээ, хэрэглэгчийн санал хүсэлтэд үндэслэн уг системийг текстэн мэдээллийг яриа руу хөрвүүлэх функцээр баяжуулж, харааны бэрхшээлтэй иргэдийн өдөр тутмын амьдралд туслах, хэрэглэхэд хялбар, үнэ төлбөргүй программ болгохоор ажиллаж байна.



3-р зураг. Системийн ерөнхий бүтэц

Дээрх зураг нь харааны бэрхшээлтэй иргэдэд зориулсан ухаалаг хөтөч системийн үйл ажиллагааны үндсэн үе шатуудыг харуулсан.

1. Гар утасны камер ашиглах: Хэрэглэгч гар утасны камерыг ашиглан зам болон орчны зураглалыг авдаг. Камераар дамжуулан тухайн орчны дүрслэлийг системд илгээдэг.
2. Объект таних: Камераар авсан дүрслэлийг систем анализ хийж, объект таних алгоритм ашиглан зам дээрх гол объектуудыг танина.
3. Объектын нэр, зайг тооцоолох: Систем таньсан объект бүрийн нэр болон хэрэглэгчээс хэр зайтай байгааг тооцоолж, тодорхойлсон мэдээллийг боловсруулахад бэлтгэдэг.
4. Объект болон зайны мэдээллийг дамжуулах: Тодорхойлогдсон объектын нэр, зайг API ашиглан дараагийн шат руу дамжуулна.
5. Текстийг нормалчлах: Дамжуулсан мэдээллийг текст хэлбэрт шилжүүлж, аудио мэдээлэлд бэлтгэнэ.
6. Текстэн мэдээллийг аудио болгох: Объектын нэр, зай зэрэг текстэн мэдээллийг Text-to-Speech (текстийг ярианд хөрвүүлэх) технологи ашиглан аудио болгон хөрвүүлж, хэрэглэгчид сонсголын хэлбэрээр хүргэнэ.

Энэ бүхэн нь харааны бэрхшээлтэй иргэдийг замын хөдөлгөөнд аюулгүй зорчих, орчны саад тогторыг таних, тэдгээрээс зайлсхийхэд туслах ухаалаг хөтөч системийг бүрдүүлж байна.

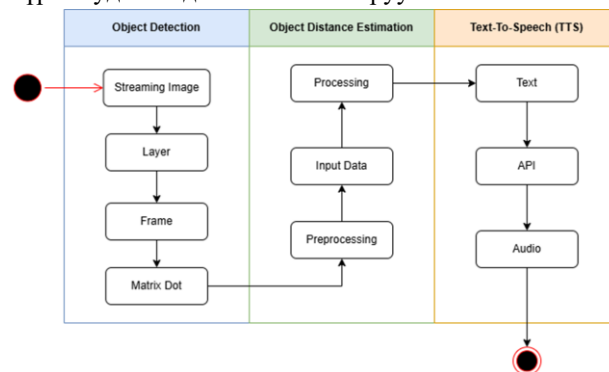
ТӨСЛИЙН ДАВУУ БОЛОН СУЛ ТАЛ

3-р ХҮСНЭГТ

Давуу тал	<ul style="list-style-type: none"> <li>• Offline орчинд ажиллах боломжтой.</li> <li>• Үнэгүй</li> <li>• Ашиглахад хялбар</li> <li>• Объект, зайн мэдээллийг аудио хэлбэрээр мэдээлэх</li> <li>• Харааны бэрхшээлтэй иргэдийн бие даасан байдлыг дэмжинэ.</li> <li>• Өргөтгөх боломжтой.</li> </ul>
Сул тал	<ul style="list-style-type: none"> <li>• Утасны ашиглалт, баттерей (зай) хурдан дуусах магадлалтай.</li> <li>• Орчны хамааралтай танихгүй байх.</li> <li>• Системийг цаг агаарын таагүй нөхцөлд ашиглахад бэрхшээлтэй байж болзошгүй.</li> </ul>

МОДУЛЬ

Манай систем нь object detection, object distance estimation, text-to-speech гэсэн гэсэн гурван үндсэн модулийг агуулсан бөгөөд тус бүрдээ дараах үйл явцуудаар дамжуулан харааны бэрхшээлтэй иргэдэд хүрэх аудио мэдээллийг боловсруулна.



4-р зураг. Модулиудын холбоо хамаарал

OBJECT DETECTION

YOLO-ийн ажлын урсгалын диаграм (workflow) YOLO framework-ийг ерөнхийд нь дөрвөн үе шатанд хуваадаг:

1. Input processing : Зурган дээрх объектуудын харьцааг гаргахын оролтын дүрсийг 416 x 416 пиксел гэх мэт тогтмол хэмжээтэй болгож өөрчилж хадгалдаг.
2. Neural Network: Энэ үе шатанд DCNN нь зураг дээрх объектуудын байгаа байдал, байршлын талаар таамаглал гаргахад ашиглагддаг. DCNN нь объектыг таних, тэдгээрийн хязгаарлах хэсгийг урьдчилан таамаглахад зургийг dataset ашиглагддаг.
3. Grid Cell Assignment : Энэ алхамд дүрсийг хуваадаг бөгөөд хуваалт нь зургийн тодорхой хэсэгт байгаа объектуудын байгаа байдал, байршлыг урьдчилан таамаглах үүрэгтэй. YOLO нь олон тооны хязгаарлах хэсгийг гаргаж, хэсэг бүрд байгаа объектуудын ангиллын магадлалыг тодорхойлдог.
4. Object Detection : Дараа нь эдгээр таамаглалыг ашиглан шүүж, давхцаж буй танилтыг хасаж эцсийн илрүүлэлтийн үр дүнг гаргана. Эцэст нь, тухайн хэсэгт илрүүлсэн объектын нэр, зайг хамт гаргадаг байна. Бүх үйл явц нь frame бүрийн хувьд давтагддаг бөгөөд энэ нь YOLO-д бодит цагийн объект илрүүлэх боломжийг олгодог. Мөн хэд хэдэн загвар (model) байдаг ба хувилбар бүр нь ялгаатай функцүүд агуулж болдог.



5-р зураг. Объект танилтын харагдац

ОБЪЕКТ ТАНИХ МОДЕЛИУДЫН ХАРЬЦУУЛАЛТ

4-Р ХҮСНЭГТ

Модель	Гүйцэтгэл (%)	FPS			Огюдлийн сан
		Tesla T4	1660 Ti	Jetson Nano	
YOLOv3	54.3	80	21	8	MS COCO 2017
YOLOv5s	37.6	100	28	15	MS COCO 2017
MobileNet-SSD V2	33.7	94	26	15	MS COCO 2017

OBJECT DISTANCE ESTIMATION

Object distance estimation нь аливаа объект болон тухайн объект руу харж буй гар утасны камер хоёрын хоорондын зайг тодорхойлох аргачлал юм. Энэ аргыг компьютерын хараа, робот техник, зураг боловсруулах, автомат жолоодлого, виртуал болон нэмэлт бодит байдал гэх мэт салбаруудад өргөнөөр ашигладаг.

- Triangulation – Объектын өнцөг болон зайг тодорхойлохдоо хоёр өөр байрлал эсвэл өнцгөөс авсан мэдээллийг ашигладаг. Энэ аргыг лазер болон stereo камерын мэдрэгчтэй хамт ашигладаг.
- Stereo Vision – Stereo камер ашиглан нэг объектыг хоёр өөр өнцгөөс дүрслээд, хоёр дүрсний хоорондын ялгааг (disparity) ашиглан зайг тооцдог.
- Monocular Method – Нэг камерын дүрслэлийг ашиглан объектын том, жижиг, тод, бүдгэрэл зэрэг шинж чанараар зайг тооцоолдог.
- LiDAR - Light Detection and Ranging – Лидар технологи ашиглан лазерын тусламжтайгаар гэрлийг объектоос цацаж, буцаж ирэх хугацааг хэмжин зайг тодорхойлдог.
- ToF – Гэрэл эсвэл дууны дохио ашиглан объектоос ойртон очоод буцаж ирэх хугацааг хэмжих замаар зайг тооцдог.

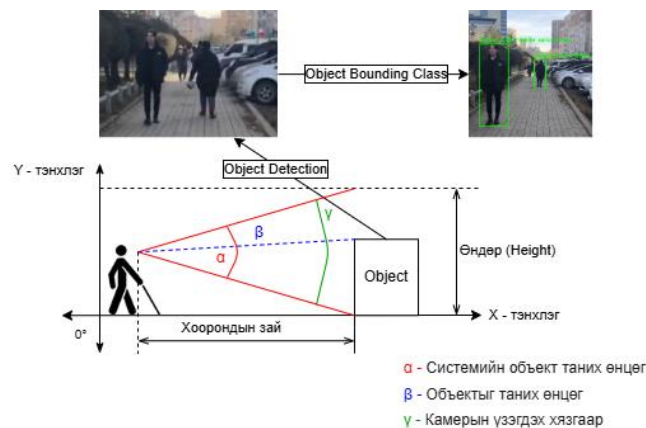
Эдгээр нь object distance estimation буюу зайг тодорхойлох аргуудын хамгийн түгээмэл хэрэглэгддэг аргачлалууд юм.

Объектын зайг тооцоолох томъёо[7]:

$$\text{object distance} = \frac{\text{focal length} * \text{real height of the object} * \text{image height}}{\text{object height} * \text{sensor height}}$$

- focal length - Камерын линзний фокусын урт, буюу линзний төвөөс мэдрэгч хүртэлх зай.
- real height of the object - Бодит объектын өндөр буюу тухайн объектын жинхэнэ өндөр хэмжээс.
- image height - Мэдрэгч дээр дүрслэгдсэн объектын дүрсний өндөр.
- object height - Дүрсэн дэх объектын өндөр.
- sensor height - Камерын мэдрэгчийн өндөр буюу мэдрэгчийн физик хэмжээсний нэг параметр.

Энэхүү томъёо нь тухайн объект мэдрэгч дээр хэр том хэмжээтэй дүрслэгдсэн, мөн мэдрэгчийн хэмжээ, линзний фокусын урт зэрэг хүчин зүйлсийг ашиглан объектын бодит зайг тооцоолдог.



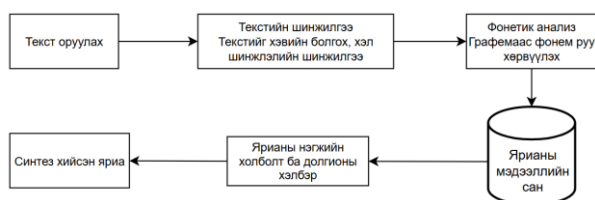
6-р зураг. Объектын зайг тооцоолох

TEXT-TO-SPEECH

TTS нь тухайн объектыг таньсан тохиолдолд дараагийн алхам буюу зорилтот хэрэглэгчид хэрхэн мэдэгдэх, мэдээлэхэд ашиглагдах арга техник юм. Тухайн шүүж гаргаж ирсэн мэдээллийг хэрэглэгчийн сонголтоор дамжуулан сэргийлүүлнэ. Илрүүлж байгаа объект нь эхний ээлжид хязгаарлагдмал байгаа ба тухайн объектыг нэр болон зайн мэдээллийг мэдээнэ.

Ярих, бичих нь хүмүүсийн текст эсвэл аман хэлбэрээр ашигладаг харилцааны үндсэн хэлбэр юм. Гэсэн хэдий ч ингэх чадваргүй хүмүүс эсвэл амархан уншиж, тайлж чаддаггүй хэл, үг байдаг. Үүний үр дүнд өгөгдсөн текстээс хүний хэлийг задлан шинжилж, ойлгож, үүсгэж чадах системийг зохион бүтээх нь чухал юм. Тиймээс, үүн дээр ажиллахын тулд яриа, хэл боловсруулах энэхүү судалгааны ажил нь компьютерт хүний хэлээр бичсэн эсвэл хэлсэн мэдээллийг ойлгох боломжийг олгоно.

Үндсэндээ машинд хүний хэлийг боловсруулах талаарх тооцооллын загварыг боловсруулдаг бөгөөд энэ нь машинаар хүний яриаг зохиомлоор бий болгож байна гэсэн үг юм. TTS нь бичгийн текстийг яриа болгон хувиргах механизм юм. Энэ арга нь текстийн шинжилгээ (text analysis), ярианы долгион (speech waveform) үүсгэх гэсэн хоёр үндсэн үе ажиллагаатай. Сүүлийн хэдэн жилийн хугацаанд Text-to-Speech технологи нь хиймэл оюун ухаан, машин сургалт зэрэг төрөл бүрийн технологийн тусламжтайгаар хамгийн сайн хувилбар нь гарсаар байгаа. Машин сургалтын технологийг ашиглан TTS дахь яриаг нь хүнтэй төстэй байдлаар дүрслэхэд хувь нэмрээ оруулсаар байгаа. Зах зээл дээр шинэ програмууд нэмэгдэж байгаа тул ярианы хэлбэрийн хэрэгцээ улам бүр нэмэгдсээр байгаа.



7-р зураг. Text - to - speech

### ХАРЬЦУУЛАЛТ

YOLOv5 загварыг ашиглан объект илрүүлэлт хийхдээ, сургалтын хугацааг хэмнэх зорилгоор урьдчилан сургагдсан параметруудийг ашигладаг. YOLOv5 нь PyTorch фреймворк дээр хөгжүүлэгдсэн бөгөөд Google Colab-ийн үнэгүй GPU ашиглан сургалтыг хурдан хийж болдог. MS-COCO зэрэг өгөгдлийн санг Google Drive-д байршуулан Colab-т mount хийж, сургалтын өгөгдөлд объектуудын координатыг агуулсан байх шаардлагатай.

YOLOv5-д сургалт хийхийн тулд дараах үндсэн тохиргооны файлууд шаардлагатай:

1. **.yaml файл** – сургалтын болон баталгаажуулах өгөгдлийн замуудыг багтаана.
2. **Data.yaml файл** – замын мэдээллийг тодорхойлно.
3. **Загварын тохиргоо** – YOLOv5-н загварын хэмжээнүүд (s, m, l, x) сонгох ба эдгээр нь тухайн моделийн нарийвчлалыг тодорхойлно.

Сургалтын явцад загвар нь batch size, сургалтын хурд зэрэг параметруудийг ашиглан суралцана. Сургалтын дараа, загварыг туршилтын зургууд дээр ажиллуулж, нарийвчлалыг хэмжихийн

тулд дундаж нарийвчлал mAP, FPS зэрэг үзүүлэлтээр үнэлнэ. Тиймээс дээрх 4-р хүснэгтээс харахад mAP болон FPS үзүүлэлтээс нь хамаараад YOLOv5 моделийг сонгон, сургасан. YOLO фреймворк хөгжихийн хэрээр хурд болон нарийвчлалын хоорондын тохиргоо улам нарийссан. YOLOv4 болон YOLOv5 зэрэг загваруудад сүлжээний шинэ арга, өгөгдлийн өргөтгөлийн сайжруулсан аргууд, сургалтын оновчтой стратеги зэрэг шинэлэг өөрчлөлтүүдийг нэвтрүүлсэн нь загварын бодит цагийн гүйцэтгэлийг огцом бууруулахгүйгээр нарийвчлалын өндөр ахиц гаргах боломжийг олгосон. YOLOv5-ээс эхлэн бүх албан ёсны YOLO загварууд нь хурд болон нарийвчлалын хоорондох тохиргоог нарийн тааруулж, тухайн хэрэглээний шаардлага, техник хангамжийн боломжид тохирсон загварын янз бүрийн хэмжээсүүдийг санал болгодог болсон. Тухайлбал, эдгээр хувилбарууд нь захын төхөөрөмжүүдэд зориулагдсан хөнгөн жинтэй загваруудыг санал болгодог бөгөөд эдгээр нь нарийвчлалыг бууруулахын зэрэгцээ тооцооллын нарийн төвөгтэй байдлыг багасгаж, боловсруулалтын хурдыг нэмэгдүүлдэг.

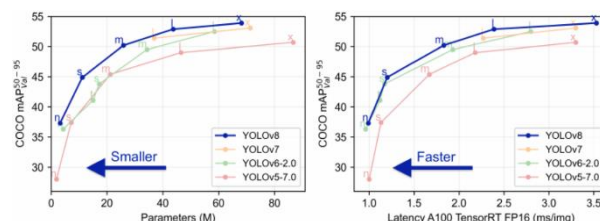


График 1. Гүйцэтгэлийн харьцуулалт

График 1 -т YOLOv5-аас YOLOv8 хүртэлх загваруудын хэмжээсүүдийг харьцуулсан. Энэ график нь нь янз бүрийн YOLO загваруудын нарийн төвөгтэй байдал болон гүйцэтгэлийг харьцуулсан шинжилгээг харуулдаг. Зүүн талын графикт параметрийн тоо (сая нэгжээр) болон COCO баталгаажуулалтын өгөгдлийн багц дээрх дундаж нарийвчлалын утгыг (mAP) IOU босго 50-95-ын хооронд харьцуулсан байна. Энэ нь параметрийн тоо нэмэгдэхийн хэрээр загварын нарийвчлал сайжирдаг чиг хандлагыг тодорхой харуулдаг. Загвар бүрийг nano (n), small (s), medium (m), large (l), extra-large (x) гэсэн хэмжээстүүдээр тэмдэглэсэн.

### ХЭРЭГЖҮҮЛЭЛТ

Ухаалаг хөтөч системийн туршилтыг явган хүний зам дээрх тодорхой объектуудыг таних болон объектуудын зайн мэдээллийг аудио хэлбэрээр гаргах зорилгоор туршиж үзсэн. Туршилт нь гурван үндсэн хэсгээс бүрдсэн бөгөөд үүнд объект таних,

объектын зайг тооцоолох, мэдээллийг аудио хэлбэрээр дамжуулах туршилтуудыг хийсэн.



8-р зураг. Системийн туршилтын хэсэг

### V. ҮР ДҮН

Туршилтын явцад хийгдсэн үйл явц, ажиллагааг нарийвчлан хянаж, алдааны хувиуд дээр үндэслэн харьцуулалтыг хийсэн. Энэ харьцуулалтаас цаашид анхаарах шаардлагатай зүйлс болон ирээдүйн хөгжүүлэлтэд хэрэгжүүлэх шаардлагатай шинэ санаанууд тодорхой болсон юм.

Туршилтын харьцуулалтыг хийхдээ хэд хэдэн үндсэн атрибутуудыг сонгон авч, тэдгээрийг хувиар тооцоолон гаргаж, үр дүнг график хэлбэрээр харуулсан болно. Туршилт нийт 20 бичлэг дээр хийгдэж, тэдгээрээс дараах үндсэн харьцуулалтуудыг гаргаж ирсэн.

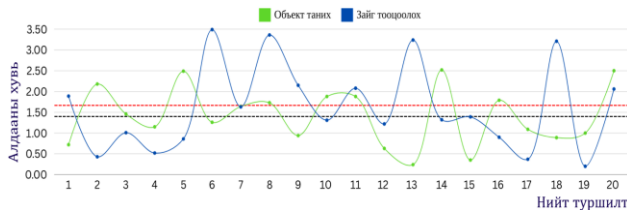


График 2. Харьцуулалт

#### A. Ногоон → Объект таних

Объект таних хурд нь туршилтын голлох үзүүлэлтүүдийн нэг бөгөөд энэхүү атрибутыг хугацаагаар хэмжин, үр дүнг хувиар илэрхийлсэн графикаар харуулсан болно.

Объект таних хурд нь системийн гүйцэтгэлийг тодорхойлж, үр дүнгийн бодит байдалд шууд нөлөөлдөг тул бидний судалгааны чухал хэмжигдэхүүн байлаа.

#### B. Улаан → Зайг тооцоолох

Зайг тооцоолох үзүүлэлт нь хэрэглэгчдэд зөв, бодитой мэдээлэл хүргэхэд нэн шаардлагатай нэгж

юм. Зайг зөв тооцоолох чадвар нь системийн найдвартай байдал болон бодит байдлыг баталгаажуулдаг бөгөөд энэ нь хэрэглэгчдийн ашиглах туршлага, үр дүнд шууд нөлөөлдөг. Туршилтын явцад гарсан алдааг илрүүлж, анализ хийснээр алдааны хэмжээг бууруулах, цаашдын хөгжүүлэлтийн суурь нөхцөлийг бий болгосон болно.

Эдгээр үзүүлэлтүүд дээр тулгуурлан хийсэн харьцуулалтууд нь судалгааны үр дүнгийн чанарыг дээшлүүлэх, үр ашигтай хөгжүүлэлтийн чиглэл тодорхойлоход онцгой ач холбогдолтой байлаа.

	Min (%)	Max (%)	Avg (%)	Accuracy (%)
Объект таних	0.24	2.52	1.41	98.58
Зайг тооцоолох	0.2	3.49	1.63	98.36

9-р зураг. Харьцуулалтын хүснэгт

#### B. Аудио мэдээлэл

Ашиглагдсан API : Бичвэрээс яриа руу хөрвүүлэх, бичвэрийг аудио файл болгон хөрвүүлэхдээ ашигласан. Хөрвөсөн аудио файлын төрөл нь audio/x-wav байна.

Авсан параметрээр хоолойгоо сонгож, speed болон pitch параметрээр ярианы хурд болон өнгийг тааруулсан.

Эдгээр туршилт болон харьцуулалтын үр дүнд манай систем эхний шаардлагын дагуу мэдээлэх чадвар нь 98% дүнтэй гэж үзэж байна.

### VI. ДҮГНЭЛТ

Гар утасны камерыг ашиглан, объектыг таньж, зайг тооцоолон хэрэглэгчид аудио хэлбэрээр мэдээлэл хүргэх ухаалаг хөтөч системийг нэвтрүүлэхээр зорьсон. Судалгааны явцад туршилтын алдаа болон гүйцэтгэлийн үзүүлэлтүүдийг нарийвчлан судалж, харьцуулалт хийснээр цаашдын хөгжүүлэлтэд хэрэгжүүлэх шаардлагатай шинэ санаанууд тодорхойлогдсон. Объект таних хурд болон зайг зөв тооцоолох чадвар нь системийн бодит үр дүн болон найдвартай байдалд чухал нөлөө үзүүлж байгааг туршилтаар баталлаа. Мөн аудио мэдээлэл дамжуулахад ашигласан API нь ярианы хурд, өнгийг тохируулах боломжийг олгож, мэдээлэл дамжуулах чадварыг 98%-д хүргэсэн нь батлагдсан. Мөн туршилтаар Монгол Улсын явган хүний зам дээрх гол объектуудыг илрүүлэх зорилгоор YOLOv5 загварт суурилсан объект таних алгоритмыг ашиглаж, 20 бодит замын бичлэг дээр туршилт хийсэн. Үүний үр дүнд объект илрүүлэх модуль 98.58%-ийн, зай тодорхойлох модуль 98.36%-ийн

нарийвчлалтай болохыг баталгаажуулсан. Эдгээр үр дүн нь судалгааны үр дүнгийн чанарыг дээшлүүлж, цаашдын хөгжүүлэлтийг бодитой болгоход чиглэсэн суурь нөхцөлийг бүрдүүлж өгч байна.

#### ТАЛАРХАЛ

Энэхүү төслийг хийж гүйцэтгэхэд туслалцаа үзүүлж, их зүйлийг зааж, чиглүүлж өгсөн удирдагч багш Доктор (Ph.D) С.Өлзийбаяр, зөвлөх багш нартаа баярлалаа.

#### НОМЗҮЙ

- [1] Kuriakose, B.; Shrestha, R.; Sandnes, F.E. DeepNAVI: A deep learning based smartphone navigation assistant for people with visual impairments. *Expert Syst. Appl.* 2023
- [2] <https://mpress.mn/p/2765> - Хараагүй иргэдэд тулгамддаг гол асуудал бол дэд бүтэц
- [3] Building\_A\_Voice\_Based\_Image\_Caption\_Generator\_with\_Deep\_Learning, 2021он
- [4] Indoor objects detection and recognition for an ict mobility assistance of visually impaired people, 2020.
- [5] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
- [6] Enhancing Object Detection for VIPs Using YOLOv4\_Resnet101 and Text-to-Speech Conversion Model  
Published online : 2 August 2023  
Authors : Academic Editors: Christos Troussas, Cleo Sgouropoulou, Akriivi Krouska, Ioannis Voyiatzis and Athanasios Voulodimos
- [7] OpenCV: How-to calculate distance between camera and object using image? - Stack Overflow
- [8] R. Nicole, "Title of paper with only first word capitalized," *J. Name Stand. Abbrev.*, in press.
- [9] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," *IEEE Transl. J. Magn. Japan*, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
- [10] Харааны бэрхшээлтэй иргэдэд зориулсан таяг Author : Б. Билгүүн 2019 он

## ДУУ ХООЛОЙГООР УДИРДАГ ЭЛЕКТРОН ЦООЖНЫ ХӨГЖҮҮЛЭЛТ

**Б.ӨСӨХБАЯР, А.ОДГЭРЭЛ**

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Электроникийн салбар  
*Холбоо барих зохиогчийн и-мэйл: odgerel55@must.edu.mn*

*Хураангуй*—Судалгааны ажлаар хүний дуу хоолойгоор удирддаг хаалганы электрон цоожны загварыг хөгжүүлж туршсан. Wi-Fi болон Bluetooth модул агуулсан 32 битийн ESP32 микроконтроллэрыг удирдлагаар нь ашигласан. MIT App inventor програмаар дуу хоолойг удирдах Андроид аппликэшнийг хөгжүүлж ухаалаг утсан дээрээ суулгасан. Ухаалаг утас, микроконтроллёр хоёр нь хоорондоо Bluetooth-р холбогдоно. Ухаалаг утаснаас хэрэглэгч цоожийг онгойлгох, түгжих түлхүүр үгийг хэлэхэд Андроид аппликэши боловсруулж интернетийн сүлжээгээр дамжин ESP32 микроконтроллэроор удирдах зарчмаар ажиллана. Одоогоор уг MIT-ийн хөгжүүлсэн аппликэши нь дэлхийн 50 орчим хэлийг танидаг бөгөөд бид Англиар хэлсэн үгийг боловсруулж байна. Уг судалгаа нь тусгай хэрэгцээт хүмүүст чухал ач холбогдолтой. Системийг цаашид үргэлжлүүлж Монгол инженерүүдийн бүтээсэн Чимэгэ дуу таних системтэй холбож Монголоор хэлийг танидаг болгож хөгжүүлэх бодит шаардлага байна.

*Түлхүүр үг* – Wi-Fi, солениод релей, ESP32, MIT App, Андроид

### I. УДИРТГАЛ

Өнөө үед технологи хурдтай хөгжиж гэр дундаа хүний дуу хоолойг таних технологиудыг дэлхийн томоохон мэдээллийн технологийн компаниуд эрчимтэй хөгжүүлж байна. Хүний хэлсэн үг, өгүүлбэрийг боловсруулан текст болгох, эсрэгээр нь бичсэн текстийг дуу хоолой болгон хөрвүүлдэг хиймэл оюун ухаан, машин сургалтын аргуудыг ашигласан функц, түүл, програм хангамжуудыг ихээр хөгжүүлж байна.

Уг судалгааны ажлаар зайнаас Bluetooth ашиглан хүний дуу хоолойгоор удирддаг хаалганы цоожны загварыг хөгжүүлж турших зорилго тавин ажилласан. Гараа ашиглах шаардлагагүй, зөвхөн дуу хоолойгоороо хаалгаа онгойлгож, түгжих боломжтой. Мөн нууцлал ба аюулгүй байдал талаасаа зөвхөн таны түлхүүр үгийг таниж нэвтрэх боломжтой тул хулгай болон зөвшөөрөлгүй нэвтрэлтээс хамгаалагдсан. Дуу хоолой таних технологийн тусламжтайгаар гэрийн автоматжуулалтыг хөгжүүлж, орчин үеийн амьдралыг хялбаршуулна. Электрон цоожийг гэр бүлийн гишүүд эсвэл итгэмжлэгдсэн хүмүүс л ашиглах боломжтой бөгөөд хүн бүрт тусгай түлхүүр шаардлагагүй зэрэг ач холбогдолтой. Хаалганы цоожийг дуу хоолойгоор удирдах нь тусгай хэрэгцээт хүмүүсийн тулгамдсан асуудлуудын нэг хэсгийг шийдэх ач холбогдолтой. Монгол Улсын хэмжээнд 2022 оны байдлаар 115.100 гаруй тусгай хэрэгцээт иргэн байна [1].

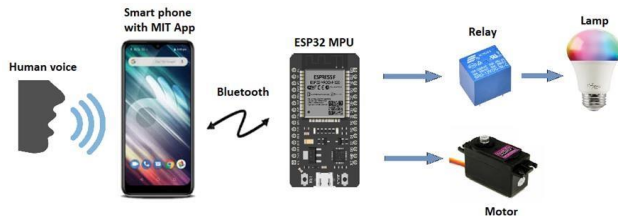


Зураг 1. Монгол улсын тусгай хэрэгцээт хүмүүсийн статистик

Энэ судалгаанд Гүүгл компаний хөгжүүлсэн машин сургалтын аргыг ашигласан дуу хоолой таних функцийг (Android RecognizerIntent Class) ашигласан [2]. Уг загварт одоохондоо Монгол хэл ороогүй учраас Англи хэлийг ашигласан. Электрон цоожийг MIT-с хөгжүүлсэн App Inventor блок програмчлалаар програмчилан Андроид аппликэши хөгжүүлж ухаалаг утсан дээр суулган удирдсан. Гүүглийн хүний дуу хоолой таних функцийг аппликэши дээр дуудаж ажиллуулсан.

Удирдах төхөөрөмж нь Андроид үйлдлийн системтэй ухаалаг гар утас эсвэл таблет байж болно. Андроид төхөөрөмж нь цоожийг нээх / хаах командуудыг илгээж, хүлээн авсны дараа микроконтроллёр цоожны гол төмөрийг солениод релейгээр нээж хааж ажиллуулна. Андроид төхөөрөмж болон хүлээн авагчийн хоорондох харилцаа холбоог утасгүй сүлжээгээр өгөгдөл хэлбэрээр илгээдэг. Микроконтроллерийн програм нь андроид төхөөрөмжөөс илгээсэн командын дагуу солениод релейгээр дамжуулан цоожны голыг

хөдөлгөнө. Arduino микроконтроллер Bluetooth утасгүй өгөгдөл дамжуулах модул ашиглан дуу хоолойгоор машин удирдах ажлыг [3, 4] дээр хийсэн. Програм хангамжийн хэсэг нь Embedded C-г ашиглан ESP32 микроконтроллер дээр хийгдсэн. ESP32 микроконтроллер ашиглан гэрийн автоматжуулалт системийг хөгжүүлж гэрэл, хөшиг, агааржуулалтын сэнс зэргийг удирдах ажил хийсэн [5].



Зураг 2. Судалгааны ажлын бүтцийн схем [5]

Дээрх зурагт [5]-р ажлын бүтцийн схемийг харуулав.

Энэтхэгийн “Viral Science” лабд ESP32 Cam модул ашиглан нүүр царай таниж онгойдог цоожийг хөгжүүлсэн [6].

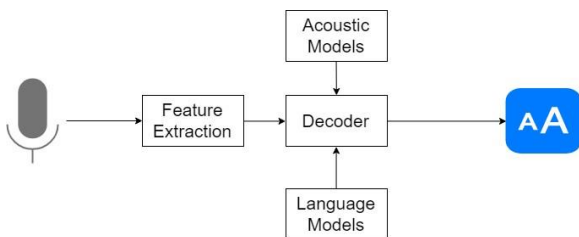
## II. ДУУ ХООЛОЙ ТАНИХ ЗАРЧИМ

### A. Дуу хоолойг хувиргах процесс

Хүний яриаг компьютерын команд болгон хувиргахын тулд компьютер хэд хэдэн нарийн төвөгтэй алхмуудыг гүйцэтгэдэг.

1. Аналогоос тоон хувиргагч нь дуут дохиог компьютерт тоон дохио болгон хувиргадаг. ADC нь тодорхой хэмжилтүүдийг хийснээр дууны долгионыг давтамжтайгаар тоон болгодог. Илүүц дуу чимээг арилгахын тулд дээж авсан эсвэл тоон болгосон дууг шүүнэ. Энэ нь мөн давтамжийн өөр өөр зурвас дахь дууг тусгаарлах, дуу чимээг хэвийн болгохын тулд хийдэг.

Хүмүүсийн ярих хурд өөр өөр байдаг тул дууг системийн санах ойд хадгалагдсан дууны загварын хурдтай тааруулахаар тохируулдаг [7].



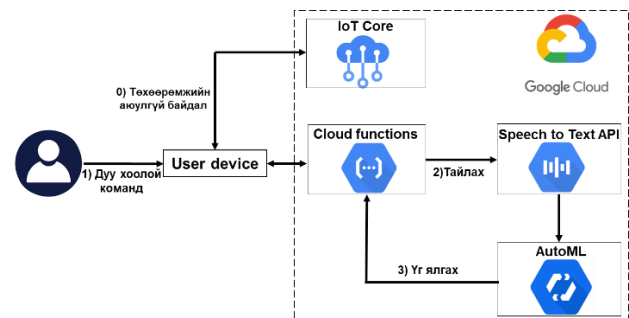
Зураг 3. Дуу хоолой таних процесс

2. Дараагийн алхам бол дохиог секундын хэдэн зуу эсвэл мянганы нэг болгон жижиг хэсгүүдэд хуваах явдал юм. Дараа нь эдгээр дохионууд нь

мэдэгдэж буй фонемуудтай таарч байгааг шалгана. Фонем гэдэг нь аливаа хэлний хамгийн жижиг элемент юм. Англи хэлэнд 40 орчим фонем байдаг. Бусад орны хэлүүд нь өөрсдийн онцлогоосоо хамааран өөр өөр тооны фонемтэй байдаг.

3. Дараагийн алхам нь яриа таних хамгийн хэцүү алхам юм. Дуу авиаг эргэн тойронд байгаа бусад фонемуудын хүрээнд авч үздэг. Дараа нь статистикийн нарийн төвөгтэй загвар нь контекст фонемийн схемийг судалж, үг, өгүүлбэр, хэллэгийн том архивын сантай харьцуулдаг. Үүний дараа програм нь хэрэглэгчийн хэлж буй үгсийг эцэст нь тодорхойлж, гаралтыг текст хэлбэрээр харуулдаг.

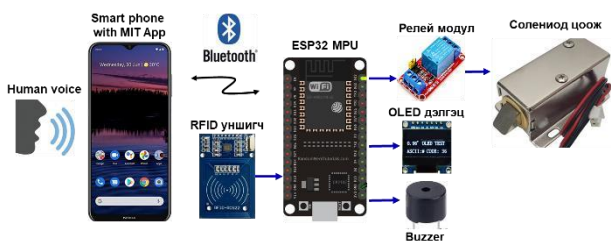
B. Дуу таних системийн загварууд Google IoT Core нь хэрэглэгчийн төхөөрөмжийг найдвартай, аюулгүй ажиллагаагаар хангадаг [8]. Хэрэглэгчийн төхөөрөмж нь Гүүглийн дуу хоолой таних функцийг агуулсан програм бүхий ухаалаг утас, таблет, компьютер байж болно. Cloud functions нь кодыг клауд дээр боловсруулдаг нэг төрлийн програмчлалын хэлний компайлор юм. Speech to Text нь дуу хоолойг текст болгох аппликэшн програм юм. AutoML (Automation machine learning) нь машин сургалтын аргаар текст болгосон үгнүүдийг ялган Cloud functions хэсэгт өгөх гэдрэг холбоотойгоор систем ажиллана. Гүүгл компаний машин сургалтанд суурилсан хүний дуу хоолойг текст болгох загварыг дараах зурагт харуулав.



Зураг 4. Гүүглийн хүний дуу хоолой таних загварын диаграм

## III. СИСТЕМ ИЙН ДИЗАЙН БА ШИЙДЭЛ

A. Системийн бүтэц Дараах зурагт системийн ерөнхий бүтцийг харуулав. ESP32 микроконтроллерын оролтонд RFID уншигчийг холбосон. Энэ нь нөөц систем буюу хэрэглэгч түлхүүр үгээ мартсан, утасны цэнэг дууссан эсвэл хоолой өвдсөн үед RFID картаа уншуулж цоожоо нээнэ. OLED дэлгэц дээр цоожны нээгдсэн, хаагдсан зэрэг одоогийн төлвүүдийг харуулна. Харааны бэрхшээлтэй иргэдэд зориулж хаалга нээгдэж хаагдсаныг баззер дуугаргаж мэдэгдэнэ.



Зураг 5. Системийн ерөнхий бүтэц

Энэ бүтцийн схем дээр харагдаж байгааг ханган байгааг хэрэглэгч “computer” гэсэн түлхүүр үг болох командыг ухаалаг утсанд байгаа MIT App inventor програмаар хөгжүүлсэн Андроид апп-д хэлнэ. Хэлсэн командыг Гүүглийн клауд сервер дээр боловсруулсан текстийг ESP32 микроконтроллер Bluetooth-р хүлээн авна. Хүлээн авсан дуу хоолойг текст болгосон командыг ESP32 микроконтроллер өөрийн програмын кодын функцтэй харьцуулан боловсруулж солениод цоожны голыг удирдах релей модулд мэдээлэл өгөх зарчмаар ажиллана.

**В. ESP32 микроконтроллер** Бүх ESP32 хувилбарууд нь ESP8266EX гэсэн үндсэн процессортой, Tensilica L106 32 битийн микро удирдлагатай. Энэ нь бага өртөгтэй, өндөр гүйцэтгэлтэй, бага эрчим хүч зарцуулдаг, програмчлахад хялбар, утасгүй SoC(System-On-Chip) юм. Мөн түүнчлэн:

- 2.4 GHz Wi-Fi (802.11 b/g/n, WPA/WPA2-г дэмждэг)
- Ерөнхий зориулалтын оролт/гаралт (13 GPIO), • Inter-integrated Circuit (I<sup>2</sup>C)
- Аналог-тоон хувиргалт (10-бит ADC), • Serial Peripheral Interface (SPI)
- DMA-тай I<sup>2</sup>S интерфэйсүүд (GPIO-гэй хуваалцах хөл)
- UART (GPIO2 дээр зөвхөн дамжуулах UART-г идэвхжүүлж болно)

Уг микроконтроллер нь өөрийн орчны бие даасан утасгүй сүлжээ үүсгэх (Access point-AP mode) болон өөрт ойрхон утасгүй сүлжээнд клиент болж оролцох гэсэн 2 горимд ажилладаг [9].

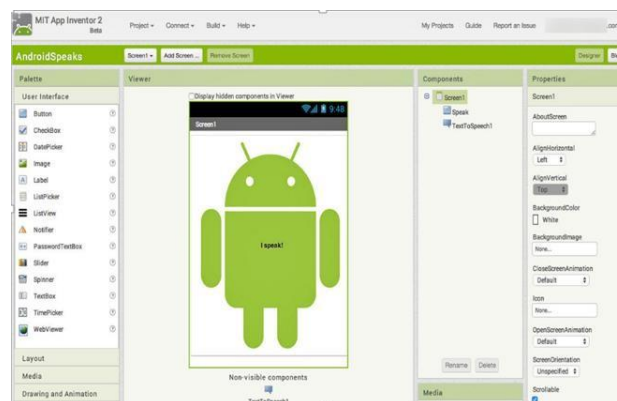
**С. MIT App Inventor програма**

MIT App Inventor нь Google-ээс вэб програмыг анх гаргаж өгсөн бөгөөд одоо Массачусетсийн Технологийн Институт (Massachusetts Institute of Technology) хариуцдаг. Энэхүү програм нь компьютерийн програмчлалд шинээр орж ирж буй хүмүүст зориулж Android болон iOS гэсэн хоёр үйлдлийн системд хэрэглээний программ хангамж (апп) хөгжүүлэх боломжийг олгодог. 2010 оноос олон нийтэд хүртээл болж, цааш хөгжүүлэгдэж эхэлсэн бөгөөд 2019 оны 7-р сарын 8-ны байдлаар

эцсийн бета шалгалтанд орж 11-р сарын 26-нд олон нийтэд хүртээл болсон [10].

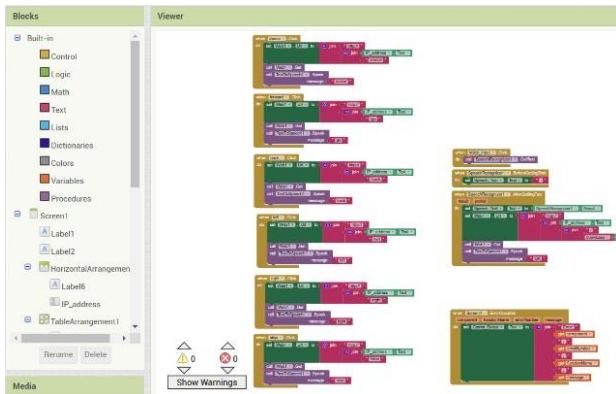
Энэ программ нь үнэгүй, нээлттэй эхийн програм хангамж бөгөөд 2 давхар лицензтэйгээр олон нийтэд гаргасан. Сүүлийн 10 жилд MIT App inventor програмаар хийсэн Андроид апп-уудыг автоматжуулалтын систем, агаарын бохирдлын хяналтын систем, гар утасны программ, боловсрол, эрүүл мэнд, машин хяналт, хяналт зэрэг хэрэглээнээс гадна робот системд ашиглаж ирсэн. Дэлхийн 195 орноос сар бүр нэг сая гаруй зочдыг нэгтгэн 60 сая гаруй аппликэшн бүтээдэг MIT App Inventor нь дэлхий дээрх програмуудыг бүтээх арга барил, хүүхдүүдийн компьютерын талаар суралцах арга барилыг өөрчилж байгаа юм.

MIT App Inventor нь бүрэн ажиллагаатайгаар Android программ болон дизайн хийх боломжтой. MIT App Inventor нь дизайнер ба блок загварлагч гэсэн хоёр хэсгээс бүрдэнэ. Доорх зурагт App Inventor програмын дизайнер хэсгийн интерфэйс, агуулгыг үүсгэдэг хэсгийг харуулав.

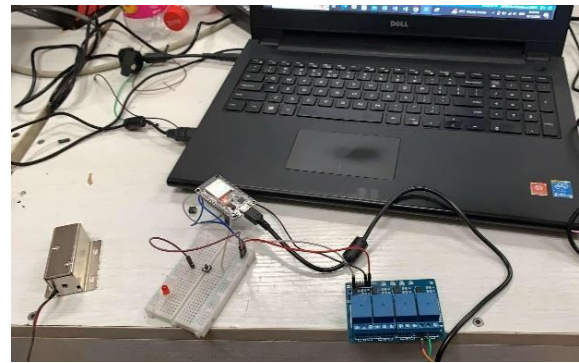


Зураг 6. MIT App Inventor-ийн дизайнерийн хэсэг

Анх блок хэл нь Google Blockly дээр бүтээгдсэн, StarLogo TNG, Scratch зэрэг хэлнүүдээс санаа авч блок суурилсан програмчлалын хэлийг ашигладаг. Блок програм нь эвлүүлдэг тоглоомын хэсгүүд шиг хоорондоо холбогдсон өнгөт кодлогдсон блокуудын тусламжтайгаар програмынхаа логикийг нүдээр засах боломжтой код юм.



Зураг 7. MIT App Inventor-ийн блок програмчлалын хэсэг

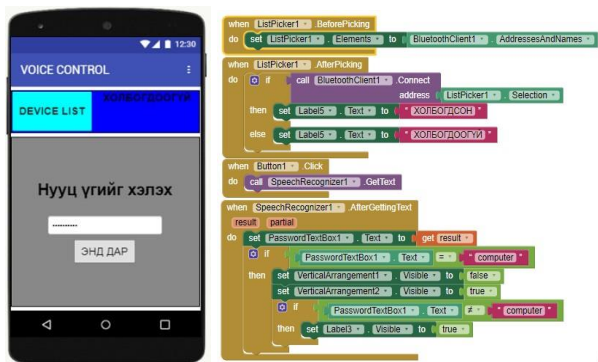


Зураг 9. Туршилтын электрон цоож

**IV. ТУРШИЛТ, ҮР ДҮН**

*A. Андроид апп-ын загвар, дизайн*

MIT App inventor-оор хийсэн андроид апп-ын загвар болон блок програмчлалын кодыг дараах зурагт харуулав. Энэ туршилтанд нь ESP32 микроконтроллэрын удирдлагатай электрон цоожийг ухаалаг утастай Bluetooth-р холбож туршилт хийсэн.

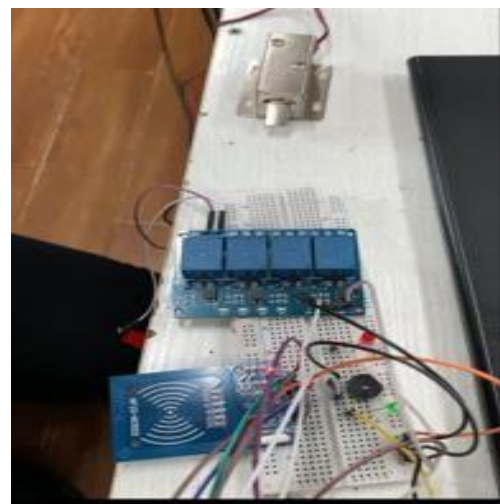


Зураг 8. MIT App inventor-оор хийсэн Андроид апп болон блок код

MIT App inventor програмын Designer-Загварын хэсэгт өөрийн хийсэн апп-ын үйлдэлүүд түлхүүр үг, speech-дуу хоолой таних товчлуур, Bluetooth-тэй холбогдох хэсэг болон бусад олон нэмэлт жижиг зүйлсийг хийж загварчилсан. Мөн Web1-сүлжээнд холбох, SpeechRecognizer1-дуу хоолойг таних, текст функцуудыг оруулсан.

*B. Туршилтын цоожны загвар* Угсарсан электрон цоожны зургийг харуулав. Эхний туршилтаар товчлуур дарахад релей модулаар дамжуулан солениод цоожны голыг нээж, хаах туршилтыг хийсэн.

Дараах зурагт нөөц системтэй туршилтын загварыг харуулав.



Зураг 10. Электрон цоожны туршилтын загвар

Хэрэглэгчийн утасны батерей дууссан, түлхүүр үгээ мартсан болон хоолой сөөсөн зэрэг асуудал гарсан үед RFID карт ашиглан онгойлгох нөөц системийг давхар хийж өгсөн.

MIT App inventor програмаар хөгжүүлж ухаалаг утсан дээр суулгасан Андроид апп-ны Google speech функцийг товчийг дарж түлхүүр үгээ (жишээн дээрх нууц үг: computer) хэлнэ. Хэлсэн үгийг Гүүгл клауд дээр боловсруулалт хийж текст болгон хувиргаж ESP32 микроконтроллер дээр харьцуулан зөв бол Bluetooth модулаар релейны гаралтанд холбогдсон солениод цоожны гол төмрийг нээж хаах зарчмаар систем ажиллана. Апп дээр хаалга нээгдэж хаагдсан үед хаалга амжилттай, нээгдэж хаагдлаа гэсэн мэдээллийг харуулна.

**V. ДҮГНЭЛТ**

Судалгааны ажлаар гэрийн автоматжуулалтын системүүдийн нэг болох хүний дуу хоолойгоор удирддаг хаалганы систем хөгжүүлж туршсан. Энэхүү электрон цоожны систем нь аюулгүй байдал, хялбар ашиглалт, зардал багатайгаараа онцлогтой.

Электрон цоожийг гэр, албан газар, зочид буудал зэрэг аюулгүй байдал шаарддаг газруудад ашиглах боломжтой. Мөн түлхүүр, карт зэрэг физик зүйлс шаардлагагүй тул хэрэглэгчдэд хялбар байна.

MIT App inventor програмаар хөгжүүлсэн дуу хоолойг удирдах Андроид аппликэшнийг өөрийн ажилдаа зориулан хөгжүүлж ухаалаг утсан дээрээ суулгасан. Ухаалаг утаснаас түлхүүр үг хэлж цоожийг нээж, хааж удирдана. Мөн хэрэглэгчийн утасны батерей дууссан, түлхүүр үгээ мартсан болон хоолой сөөсөн зэрэг асуудал үүссэх үед RFID карт ашиглан онгойлгох нөөц системийг давхар хийж өгсөнөөрөө онцлогтой. Уг электрон цоожийг тусгай хэрэгцээт хүмүүст зориулан цааш нь хөгжүүлэх зорилготой ажиллаж байна.

Одоогоор уг MIT-с гаргасан аппликэшн нь дэлхийн 50 орчим хэлээр (Англи, Хятад, Орос. . . ) хэлсэн үгийг боловсруулж байгаа боловч Монгол хэл байхгүй. Системийг цаашид үргэлжлүүлж Монгол инженерүүдийн бүтээсэн Чимэгэ дуу таних системтэй холбож Монголоор хэлийг танидаг болгож хөгжүүлэх боломжтой.

## НОМ ЗҮЙ

- [1] [https://www.1212.mn/tables.aspx?TBL\\_ID=DT\\_NSO\\_3300\\_014\\_V1](https://www.1212.mn/tables.aspx?TBL_ID=DT_NSO_3300_014_V1)
- [2] <https://cloud.google.com/speech-to-text>
- [3] Kantekar Sampath Kumar, Pinkesh Santhosh Reddy, Manchala Rajiv Vikram Revanth, Dr. Krishna Samalla “Voice Controlled Robot Vehicle Using Arduino” International Journal for Research in Applied Science & Engineering Technology Volume 10, Issue VI, June 2022
- [4] Suwarna Gothane “Development of IoT Enabled Voice Controlled Robot Using Arduino” International Journal of innovative research in Technology, Volume 7, Issue 11, April 2021 [5] Б.Очирсүрэн “Дуу хоолойгоор удирддаг гэр ахуйн төхөөрөмжийн загвар”, Бакалаврын дипломын ажил, 2022 хавар
- [6] [https://youtu.be/\\_VOmfJ4x-Fg?si=MdnRhoA-bM17Y0cr](https://youtu.be/_VOmfJ4x-Fg?si=MdnRhoA-bM17Y0cr)
- [7] Lawrence Rabiner, Biin-Hwang Juang “Fundamentals of Speech Recognition”, Prentice Hall, Signal Processing Series, 1993
- [8] <https://android-developers.googleblog.com/2018/06/androidthings-client-library-for.html>
- [9] <https://www.embedded-robotics.com/esp8266-wifi/>
- [10] <http://ai2.appinventor.mit.edu/reference/>

## ХУРЛЫН ТЭМДЭГЛЭЛ ХӨТЛӨГЧ УХААЛАГ СИСТЕМИЙН СУДАЛГАА, ХӨГЖҮҮЛЭЛТ

Г. МАГВАН-ЭРДЭНЭ<sup>1</sup>, Ү. МӨНХТУЯА<sup>2</sup>, Б. ДОЛГОРСҮРЭН<sup>3</sup>

<sup>1</sup>Монгол улс, Улаанбаатар хот, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Компьютерын ухааны салбар, Мэдээллийн технологийн салбар

*Зохиогчийн и-мэйл хаяг: b.dolgorsuren@must.edu.mn\**

**Хураангуй:** Өнөө үед хурал, чуулган, уулзалтын тэмдэглэлийг тухайн болж буй процессыг баримтжуулах үүднээс механик буюу гар аргаар хөгждөг. Энэ нь цаг хугацаа алдах, хурлын тэмдэглэлийн үнэн зөв байдал алдагдах, дутуу өгөгдөл хадгалах зэрэг дутагдалтай талуудыг үүсгэж байна. Энэ үйл явцыг хиймэл оюун ухаан, машин сургалт, гүн сургалтын аргуудыг ашиглан автоматжуулахаар зорьсон бөгөөд тодорхой загваруудыг монгол хэл дээр турших, оновчтой загварыг хэрэгжүүлсэн ухаалаг веб системийн шийдлийг боловсруулсан болно. Уг системийг бүх төрлийн байгууллага, гадаад харилцаа, олон улсын гэрээ хэлэлцээр, уулзалт, хурал, чуулганы аудио бичлэгийг оруулж, ямар оролцогч, ямар хугацаанд, юу ярьсан болохыг таньж илрүүлээд, тогтсон хурлын протоколын загвараар гаргах юм. Тус сэдвийн хүрээнд төрийн өмчийн болон хувийн өмчийн байгууллагууд дээр судалгаа хийж, түүнд чиглэсэн оновчтой үр дүнг боловсруулан гаргав.

*Түлхүүр үг:* Хурлын тэмдэглэл, гүн сургалт, яриа танилт, пианнот

### I. УДИРТГАЛ

Хиймэл оюун ухаан (AI) нь боловсрол, соёл, шинжлэх ухаан зэрэг олон салбарт инноваци, өөрчлөлтийн шинэ эрин үеийг бий болгож байна. AI технологи ашигласнаар уламжлалт байдлаар, механик буюу гар аргаар хийгддэг үйлдлүүдийг өөрчлөх боломжтой бөгөөд цаашид илүү ухаалаг шинэ хэрэгсэл, програмууд бүтээгдсээр байна. Ухаалаг танилтын технологи нь хиймэл оюун ухааны үндсэн ангилалуудын нэг юм. Ухаалаг таних технологийг үндсэндээ хоёр хэсэгт хуваадаг. Үүнд: нэгдүгээрт, дүрс таних технологи, хоёрдугаарт нь яриа таних технологи тус тус орно. Хиймэл оюун ухаан нь бүтээмжийг дээшлүүлэх, үйл явцыг хурдасгах, өгөгдлийн үнэн зөв, бүрэн бүтэн байдлыг хадгалах зэрэг бүх шатны байгууллагад өргөн хүрээний боломжит хэрэглээтэй. Монгол улсад үйл ажиллагаагаа явуулж буй хувийн өмчит болон төрийн өмчит олон шатны байгууллагууд гадаад болон дотоод үйл ажиллагааныхаа хурал, уулзалт, чуулган зэрэгтээ тусгай мэргэжилтнээр, механик аргаар протокол, тэмдэглэлийг хөглүүлж архивладаг үйл явцыг хиймэл оюун ухаан, машин сургалт, гүн сургалтын аргуудыг ашиглан веб системийн оновчтой шийдлийг хөгжүүлэхээр зорилоо. Энэ нь шаардлагатай өгөгдлийн үнэн зөв байдлыг хадгалах, бүрэн бүтэн байдлыг авч үлдэх, цаг хугацаа хэмнэх зэргээр чухал нөлөө үзүүлж байна [1].

**Судалгааны зорилго:** Энэхүү судалгааны ажлын зорилго нь хурал, уулзалт, чуулганы аудио бичлэгийг боловсруулж, тогтсон стандарт, загварын дагуу тухайн хурлын протоколыг боловсруулан гаргах

боломжтой хиймэл оюун ухааны яриа танилтын санд суурьлагдсан веб системийн оновчтой шийдэл боловсруулахад оршино.

### Судалгааны зорилт:

1. Яриаг бичвэрт хөрвүүлэхэд шаардлагатай онолын судалгааг хийнэ.
2. Өгөгдлөө цуглуулна, бэлтгэнэ.
3. Туршилт хийнэ.

### II. ОНОЛЫН ХЭСЭГ

Хиймэл оюун ухаан тэр дундаа машин сургалт болон гүн сургалтын фреймворк дээр ажилладаг олон төрлийн сан байдаг бөгөөд үүнээс яриа танилтийн технологид хамгийн өргөн ашиглагддаг Kaldi, Google Cloud Speech, LIUM, Sonix, Voice.NET, Ryannote гэх мэт сангуудыг тодорхой үзүүлэлтүүдээр харьцуулсны үндсэн дээр хамгийн оновчтойг нь сонгон бодит бүтээгдэхүүн болгохоор энэхүү судалгааны ажил тулгуурласан болно. Харьцуулсан судалгааны үр дүнг Хүснэгт 1-т орууллаа. Бидний сонгосон пианот сан нь сегментчлэл, эмбеддинг, кластеринг гэсэн хэд хэдэн давхаргаас бүрдэх ба яриа танилт болон ярианы хэлбэр таних (speaker diarization) зэрэг дууны дохио боловсруулах талбарт ашиглагддаг нээлттэй эхийн “toolkit” юм. Үүний давуу талуудыг дурьдвал:

1. **Нээлттэй эхийн код:** PyAnnote нь нээлттэй эхийн бөгөөд хэн ч кодыг ашиглах, засварлах боломжтой байдаг. Энэ нь судалгаа, хөгжүүлэлтийн ажлыг хурдасгадаг.
2. **Орчин үеийн алгоритмууд:** PyAnnote нь яриа танилт, ярианы сегментаци, илрүүлэлт зэрэгт

хамгийн сүүлийн үеийн deep learning загваруудыг ашигладаг.

- Туршлагатай хэрэглээ:** Энэ toolkit нь судалгааны болон үйлдвэрлэлийн орчинд ашиглагддаг туршлагатай. Ялангуяа академик орчинд ярианы танилт хийхэд өргөн хэрэглэгддэг.
- Pre-trained загварууд:** PyAnnote нь урьдчилан сургагдсан загваруудтай ирдэг бөгөөд үүнийг ашиглан шууд ярианы процессор дээр ажиллуулах боломжтой. Энэ нь загварыг сургах цаг хугацааг хэмнэдэг.
- Өргөтгөх боломжтой:** PyAnnote нь модуляр бүтэцтэй тул хэрэглэгчид өөрсдийн хэрэгцээнд нийцүүлэн өргөтгөл хийж, өөрчлөлт оруулах боломжтой.
- График интерфэйс болон тайлбарлагч:** PyAnnote нь үзүүлэн болон анализ хийхэд ашиглах боломжтой график интерфэйс болон хэрэгслийн дэмжлэгтэй.

Эдгээр давуу талууд нь PyAnnote-г яриа таних, яриа сегментацлах гэх мэт нарийн дууны дохио боловсруулах ажлуудад хүчирхэг хэрэгсэл болгодог.

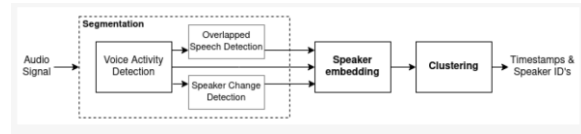
ПИАННОТ САНГ БУСАД ЯРИА ТАНИЛТЫН САНГУУДАЙ ХАРЬЦУУЛСАН ХҮСНЭГТ [2]

*I-P ХҮЧЭГТ*

Хүчин зүйлүүд	Пианнот аудио	Kaldi	Libim SphDiarization	SpeechBrain	Google Cloud Speech API	Sonix AI	Voice.net
Суурьлагдсан хэл	Python	C++	Java	Python	Python	Python	Python
Загварын төрөл	Гүн сургалт	GMM-HMM, x-vector	GMM-HMM	Гүн сургалт	Гүн сургалт	Гүн сургалт	Гүн сургалт
Урьдчилан боловсруулсан моделүүдтэй эсэх	Тийш	Үгүй	Тийш	Тийш	Тийш	Тийш	Тийш
Ашиглагдах байдал	Хялбар	Комплекс	Дулааж	Хялбар	Хялбар	Хялбар	Хялбар
Бодит цагийн боловсруулалт боломжтой эсэх	Тийш	Тийш	Үгүй	Тийш	Тийш	Тийш	Тийш
Үгүй зөв байдал, нарийвчлалын тооноовол	92%-95%	90%-93%	<80%	85%-88%	90%-95%	92%-94%	85%-90%
Алдааны хувь	5%-10%	5%-10%	15%-20%	10%-15%	5%-10%	5%-8%	10%-15%
Нэмэлтээр ажгуулагдах боломж	Өндөр	Дундаж	Бага	Өндөр	Бага	Дундаж	Бага
Ашиглагдах боломжтой салбарууд	Судалгаа, бүтээгдэхүүн хөгжүүлэлт	Өмнөх боловсруулалт шардана	Суурь хөгжүүлэлт	Өндөр түвшний аппликаци	Худалданы салбар	Шинжилгээ	Ярианы аппликаци

**2.1 Пианнот**

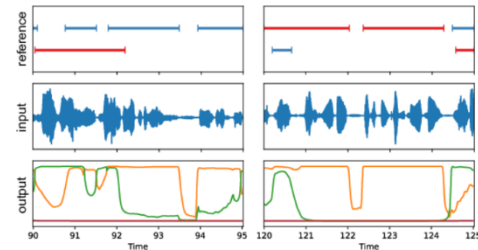
Пианнот бол Pytorch машин сургалтын фреймворк дээр ажилладаг Python хэл дээр бичигдсэн яриа танилтийн сан юм. Энэ нь модульчлагдсан, хурдан бөгөөд хэрэглэхэд хялбар байдлаар бүтээгдсэн. Үүнийг судлаач, инженер “Herve Bredin, Ruiqing Yin, Juan Manuel Coria, Gregory Gelly, Pavel Korshunov, Marvin Lavechin, Diego Fustes, Hadrien Titeux, Wassim Bouaziz, Marie-Philippe Gill” нар бүтээсэн [3].



Зураг 2.1.1 Пианнот сангийн ажиллагааны диаграм [4]

**2.1.1 Сегментчлэл**

Энэхүү шатанд аудио бичлэгийг хэд хэдэн хэсэг болгон хувааж, хүн ярьж байгаа эсэхийг шүүх, шуугианыг бууруулах зэргээр өгөгдлийн цэвэрлэгээ хийгддэг. Ингэснээр тухайн аудионоос ярьж буй



субъектуудыг ангилах боломжийг олгодог [5], зураг 2.1.1. Сегментчлэл нь Recurrent Neural Network (RNN) алгоритм дээр сууриглагдаж гүйцэтгэгддэг [зураг 2.1.2].

Зураг 2.1.1 Сегментчлэх процессын диаграм [4]

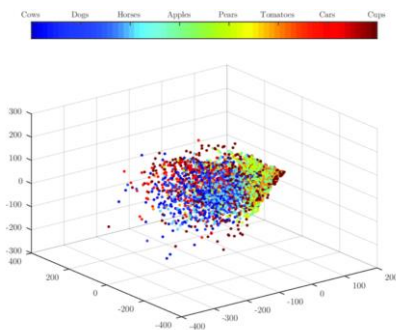
$$h_t = \sigma(W_x X_t + W_h h_t - 1 + b)$$

- $X_t$  : Аудио сигналын оролт
- $h_t - 1$  : Илэрүүлэх хувьсагчийн утга
- $W_x$  : Матрицын оролтын утгын жин
- $W_h$  : Матрицын хувьсагчийн утгын жин
- $b$  : Хазайлтын утга
- $\sigma$  : Идэвхжүүлэлтийн функц

Томьёо 2.1.2 Recurrent Neural Networks алгоритмын томьёо

**2.1.2 Эмбеддинг**

Энэхүү шатанд сегментүүдээс буюу ярьж буй субъектуудээс хоолойны өнгө, ярианы хурд, ярианы зангилаа(pitch) зэрэг шинж чанаруудыг илрүүлэх үйл явц хийгддэг [5], зураг 2.2.1. Эмбеддинг нь Deep Neural Network (DNN) алгоритм дээр сууриглагдаж гүйцэтгэгддэг [зураг 2.2.2].



Зураг 2.2.1 Эмбеддинг процессын диаграм [4]

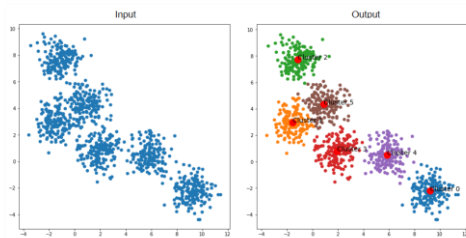
$$E(X) = f_{NN}(X)$$

- $X$  : Оролтын аудио сигнал
- $f_{NN}$  : Нейрон сүлжээ

Томьёо 2.2.2 Deep Neural Network алгоритмын томьёо

### 2.1.3 Кластеринг

Энэхүү шатанд эмбеддинг хийгдсэний үр дүнд илэрсэн шинж чанаруудыг ангилах үйл явц хийгддэг [5], [зураг 2.3.1]. Кластеринг нь Agglomerative Hierarchical Clustering (АНХ) алгоритм дээр суурьлагдаж гүйцэтгэгддэг [зураг 2.3.2].



Зураг 2.3.1 Кластеринг процессын диаграм [4]

$$D(E_i \cdot E_j) = 1 - (E_i \cdot E_j) / \|E_i\| \|E_j\|$$

- $E_i \cdot E_j$  = Эмбеддинг үе шатны үр дүн
- $\|E_i\| \|E_j\|$  = Эвклидийн зай

Томьёо 2.3.2 Agglomerative Hierarchical Clustering алгоритмын томьёо

## III. СУДАЛГААНЫ ХЭСЭГ

Монгол улсад үйл ажиллагаа явуулж буй төрийн болон хувийн өмчит байгууллагууд уулзалт, хурал чуулганахаа тэмдэглэлийг хэрхэн хөтөлдөг талаар судалгаа явуулсны үндсэн дээр тусгай ажилтан тухайн хурал, чуулган, уулзалтын тэмдэглэлийг гар аргаар хөтөлдөг болохыг илрүүлэв. Ингэхдээ хурлын тэмдэглэл хөтлөх загварын дагуу шаардлагатай мэдээлэл, тоо баримтийг багтаан, хурлаар хэлэлцэж

буй асуудалтай холбоотой санал, шүүмжийг мөн багтаадаг болохыг судалгааны үр дүнгээр олж тогтоов.

### 3.1 Хурлын тэмдэглэл хөтлөх стандарт

- Байгууллагын нэр
- Баримт бичгийн нэр
- Хурал болсон газар
- Хуралдсан он, сар, өдөр
- Дугаар
- Гарын үсэг, баталгаа
- Оролцогчдын нэр, албан тушаал
- Хэлэлцсэн нь
- Сонссон нь : Хуралдааны явцад хэлэлцсэн илтгэл, сонсгол болон холбогдож гарсан асуулт, хариулт, санал, шүүмжлэлийг дарааллаар үг хэлсэн хүн тус бүрээр бичнэ.
- Шийдвэрлэсэн нь

### 3.2 Төрийн өмчийн болон хувийн өмчийн байгууллага

ШУТИС МХТС салбар сургууль дээр сард дунджаар 40 орчим хурал болдог. Хурал бүр тухайн хурлын зорилго, түвшингээс хамааран 60-120 минут үргэлжилдэг. Хурал бүрийн тэмдэглэлийг захирлын туслах Жаргалмаа гар аргаар хөтөлдөг. Үүний тулд нэг хурлын тэмдэглэл дээр 3-4 цагийг үргэлжилсэн хугацаанаас хамааран зарцуулдаг болохыг судалгааны үндсэн дээр тогтоов.

Монгол улсад үйл ажиллагаагаа явуулдаг МОН-НАБ ХК сард дунджаар 50 орчим хурал болдог. Хурал бүрийн тэмдэглэлийг тухайн хурлын зорилгоос шалтгаалан ерөнхий менежер Г. Нарантуяа эсвэл ахлах менежер Г. Мөнхзул гар аргаар хөтөлж, хуралд оролцогчдоор батлуулдаг. Нэг хурал ойролцоогоор 90-120 минут үргэлжилдэг. Үүний тулд нэг хурлын тэмдэглэл дээр 3-4 цаг орчим хугацаа зарцуулдаг байгууллага зарцуулдгийг тогтоов.

## IV. ТУРШИЛТ, ХЭРЭГЖҮҮЛЭЛТ

### 4.1 Өгөгдөл оруулах.

Бид хэрэгжүүлэлтэндээ УИХ-ын ээлжит чуулганы 10 минутын аудио бичлэгийг ашигласан болно.

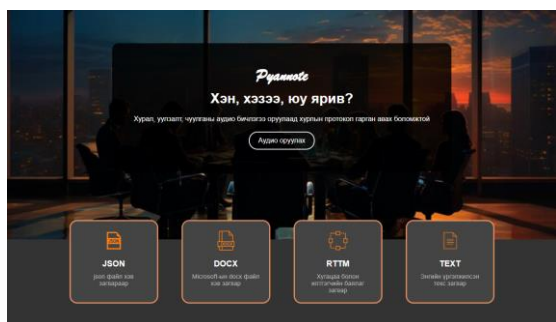
### 4.2 ТУРШИЛТ

Хурлын аудио бичлэгийг дуу бичлэг оруулах хэсэгт оруулах бөгөөд, хурлын протоколын тогтсон загварын дагуу хурлын гарчиг, огноо, дугаар, газар, баталсан хүн, тэмдэглэл хөтөлсөн хүн, оролцогчдын мэдээлэл зэрэг зайлшгүй өгөгдлүүдийг оруулж өгснөөр боловсруулалт хийгдэж гарна.

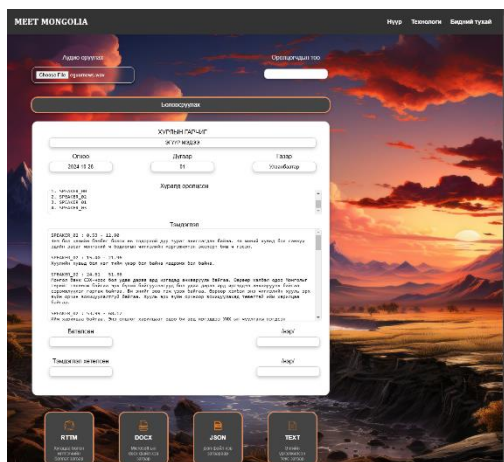
Боловсруулагдсан хурлын тэмдэглэлийг “docs, txt, json, rttm” гэсэн дөрвөн форматаар татаж авах боломжтой юм.

Боловсруулагдсан хурлын тэмдэглэлийн давуу тал:

- Тоон төрлийн текстүүдийг таньж цифрээр бичнэ.
- Нийтлэг албан газруудын нэрийг таньж товчилж бичнэ.
- Тусгай тэмдэгтүүдийг таньж хөрвүүлж бичнэ.



Зураг 4.2.1 Вэб сайтын нүүр хэсэг



Зураг 4.2.2 Аудио бичлэг боловсруулах хэсэг

### 4.3 АЛДААНЫ ТООЦООЛОЛ

Бид туршилтандаа ашигласан 10 минутын урттай аудио бичлэгний алдааны тооцооллыг Diarization Error Rate(DER) метрикээр хэмжиж гаргав. Энэ нь алдааны тоог нийт бодит ярианы хугацааны харьцаагаар тодорхойлогддог метрик юм. Үүний үр дүнд нийт алдаа хувь = 0.01424063260 гарлаа.

$$\text{Алдааны хувь} = \frac{\text{алдааны тоо}}{\text{нийт бодит ярианы хугацаа}}$$

Зураг 4.3.1 DER метрикийн томъёо

### ДҮГНЭЛТ

Энэхүү судалгааны ажлаар бүх шатны байгууллага, гадаад харилцаа, олон улсын харилцааны хурал, чуулган, уулзалтын аудио бичлэгнээс хиймэл оюун ухааны гүн сургалтын яриа танилтын санд суурьлан, веб интерфэйсийг хөгжүүлж, үр дүнг хурлын протоколын загварт боловсруулж, боловсруулагдсан хурлын тэмдэглэлийг дөрвөн форматаар татаж авах зэрэг өргөн хэрэглээтэй веб системийн оновчтой шийдэл боловсруулан хурлын тэмдэглэлийг механикаар хөтлөх үйл явцыг автоматжуулах системийн судалгааг хийж, хөгжүүлэхээр зорьлоо.

### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Sayama, H., Pestov, I., Schmidt, J., Bush, B. J., Wong, C., Yamanoi, J., & Gross, T. (2023). Modeling complex systems with adaptive networks. *Computers & Mathematics with Applications*, 65(10), 1645-1664. Available [online]: <https://ieeexplore.ieee.org/abstract/document/7078608>
- [2] Bredin, H. (2017, August). pyannote. metrics: A Toolkit for Reproducible Evaluation, Diagnostic, and Error Analysis of Speaker Diarization Systems. In *INTERSPEECH* (pp. 3587-3591). Available [online]: [https://www.isca-archive.org/interspeech\\_2017/bredin17\\_interspeech.pdf](https://www.isca-archive.org/interspeech_2017/bredin17_interspeech.pdf)
- [3] Bredin, H. pyannote. audio speaker diarization pipeline at VoxSRC 2022. Available [online]: [https://www.robots.ox.ac.uk/~vgg/data/voxceleb/data\\_workshop\\_2022/reports/pyannote\\_report.pdf](https://www.robots.ox.ac.uk/~vgg/data/voxceleb/data_workshop_2022/reports/pyannote_report.pdf)
- [4] Bredin, H. (2023, August). pyannote. audio 2.1 speaker diarization pipeline: principle, benchmark, and recipe. In *24th INTERSPEECH Conference (INTERSPEECH 2023)* (pp. 1983-1987). ISCA. Available [online]: <https://hal.science/hal-04247212/>
- [5] Khoma, V.; Khoma, Y.; Brydinskyi, V.; Kononov, A. Development of Supervised Speaker Diarization System Based on the PyAnnote Audio Processing Library. *Sensors* 2023, 23, 2082. Available [online]: <https://doi.org/10.3390/s23042082> <https://www.mdpi.com/1424-8220/23/4/2082>
- [6] <https://www.monlab.mn/> /хурлын-тэмдэглэл/

## DEEPFAKE AUDIO АШИГЛАСАН САНХҮҮГИЙН ЗАЛИЛАНГ АИ АШИГЛАН ИЛРҮҮЛЭХ НЬ

Болд ТУНГАЛАГТУУЛ<sup>1</sup>, Гансүх ӨЛЗИЙТӨГС<sup>1</sup> Бат-Эрдэнэ МӨНХБАЯР<sup>2</sup>

<sup>1,2</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбооны технологийн сургууль, Мэдээллийн сүлжээ, Аюулгүй байдлын салбар

*Холбоо барих и-мэйл хаяг: munkhbayar.b@must.edu.mn<sup>2</sup>*

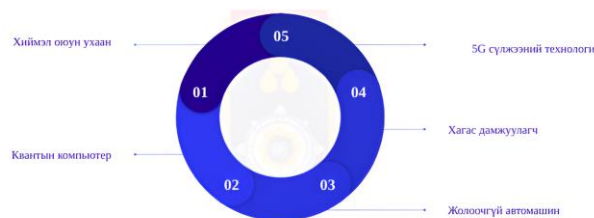
**Хураангуй:** Сүүлийн жилүүдэд Audio Deepfakes (ADs) гэж нэрлэгддэг хиймэл оюун ухаан дээр суурилсан хүний дуу хоолой, видео, зураг, текстийг нэгтгэж хиймэлээр дуурайлган үүсгэх технологийн тусламжтай гэмт хэргийн зорилгоор хиймэл контент үүсгэж худал хуурмаг мэдээлэл нийгэмд түгээх, хувь хүн рүү чиглэсэн халдлага зохион байгуулах зэрэгт ашиглах болсон. Хүний амьдралыг сайжруулах зорилгоор анх аудио ном болгон нэвтрүүлсэн ч сүүлийн жилүүдэд нийгэм, хувь хүнийг дан ганц санхүүгийн хувьд гэлтгүй бие ээтгэл, эрүүл мэндийн хувьд ч мөн хохироох болсон билээ. Ийнхүү сүүлийн үед AD нь судлаачдын анхаарлыг татах болсон бөгөөд тэдгээрийг илрүүлэхийн тулд Machine Learning (ML) болон Deep Learning (DL) аргуудыг боловсруулж байна. Мэдээж дүрс бичлэгийн хуурамч дүрсийг тодорхойлоход ихээхэн ахиц дэвшил гарсан. Гэсэн хэдий ч монгол хэл дээр энэ төрлийн судлагдсан ажил байхгүй. Энэхүү судалгаан ажлын хүрээнд бид дуу хоолойны онцлог болон хэлсэн үгнүүд дээр дүн шинжилгээ хийн залилан байх боломжтой эсэхийг тодорхойлох хиймэл оюун хөгжүүлсэн.

**Түлхүүр үг:** хуурамч дуудлага илрүүлэх, машин сургалт, хиймэл оюун

### I. УДИРТГАЛ

Сүүлийн үед ихээр үйлдэгдэж байгаа хэргүүдийн нэг нь санхүүгийн залилан юм. Богино хугацаанд их мөнгөтэй болох гэсэн эсвэл мөнгөө өсгөх үүднээс сайтар нягтлалгүйгээр санхүүгийн харилцаанд орсноос хохирогч болсон иргэд, аж ахуйн нэгжийн тоо сүүлийн үед эрс нэмэгдэж байна. Монгол Улсын үндэсний эрсдэлийн үнэлгээгээр “залилах” гэмт хэргийн улмаас олсон орлогоос үүдэлтэй аюул занал “өндөр” хэмжээнд үнэлэгджээ (Үндэсний эрсдэлийн үнэлгээ, 2021). Залилах гэмт хэргийн ангиллаар эрүүгийн хэргийн үндсэн яллагдагчаар татсан хэргийн тоо 2020 оны байдлаар 3,238 буюу нийт хэргийн 34.9 хувийг эзэлж байгаа бөгөөд хулгайлах гэмт хэргийн дараа орж байна[1]. Монгол улсын хувьд хүн ам нийгмийн байдлаас шалтгаалан залилах хэмээх гэмт хэрэг улам газар авсаар байгаа бөгөөд сүүлийн жилүүдэд гадаадаас хөгжиж буй орнууд руу чиглэсэн халдлага эрс ихэссэн. Үүний хамгийн том жишээ нь хуурамч дуудлага[2].

Энэхүү судалгаагаар Deepfake audio ашигласан санхүүгийн залиланг илрүүлэх хамгийн үр дүнтэй аргыг эрэлхийлсэн.

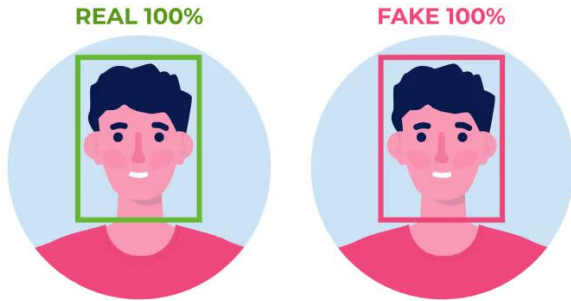


1-р Диаграм. 2020 оноос хойшхи инновацийн хамгийн чухал 5 салбар[3]

### II. ОНОЛЫН ХЭСЭГ

*Deepfake гэж юу вэ?*

DeepFake гэдэг нь хүний дүрс болон дуу хоолойг хиймэл байдлаар дуурайж, хуурамч контент үүсгэх боломжийг олгодог технологи юм[4]. Deepfake анх 2017 онд "deep-fakes" нэртэй хэрэглэгч өөр жүжигчний царайтай хуурамч бичлэгийг энэ веб сайтад байршуулснаар Reddit дээр гарч ирсэн. Энэ нь шинэ технологийн хувьд хөрөг зураг зурах эрх, нэр хүнд, зохиогчийн эрх зэрэг хувийн ашиг сонирхлыг зөрчиж, бизнес эрхлэгчдэд эдийн засаг, нэр хүндэд хохирол учруулдаг хууль эрх зүйн олон бэрхшээлийг зайлшгүй дагуулдаг[1][4].



1-р Зураг. DeepFake Видео Тархалт

Интернэт сүлжээн дэх DeepFake аргаар бүтээгдсэн хуурамч бичлэг контентын тоо 2020 онд 85,000, 2023 он гэхэд энэ тоо 145,000 хүрч нэмэгдсэн ба тэдгээрийн 70%-аас илүү хувь нь YouTube, TikTok, Reddit зэрэг социал сувгууд дээр тархсан байлаг[2]. DeepFake технологийг улс төрийн компани ажил, суртал ухуулгад ашиглаж байгаа тохиолдол улам бүр нэмэгдэж байна. 2021 оны тооцоогоор DeepFake технологийн улмаас дэлхийн эдийн засагт учруулах хохирол ойролцоогоор 250 сая ам.доллар-т хүрсэн гэж тооцоологдсон. Компаниудын 47% нь DeepFake-ийн улмаас бизнесийн нэр хүнд, санхүүгийн эрсдэлд орох магадлалтай гэж үздэг.[3][6].

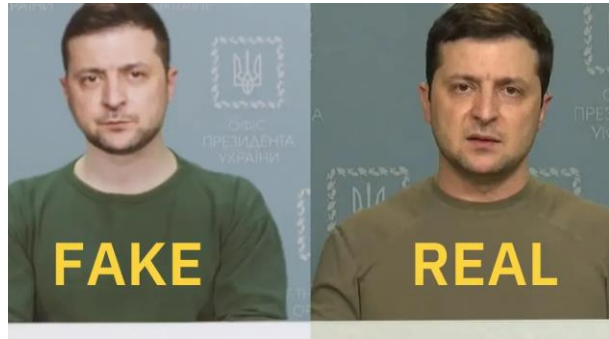


2-р Зураг. Deepfake-д хамгийн их өртсөн алдартан болоод улс төрч[5]

**Deepfake audio гэж юу вэ?**

Deepfake audio нь хиймэл оюун ухаанаар үүсгэгдсэн эсвэл өөрчилсөн хуурамч аудио бөгөөд бодит мэт сонсогддог. Сүүлийн жилүүдэд хуурамч аудио хэд хэдэн гэмт хэрэгт ашиглагдаж байгаа тул тэдгээрийг илрүүлэх чадвар нь маш чухал болоод байна. 2018-2019 оны хооронд Deepfake аудио-ийн тухай нийтлэлийн тоо мэдэгдэхүйц нэмэгдсэн (60-аас 309 хүртэл)[5]. 2020 онд DeepFake ашиглан

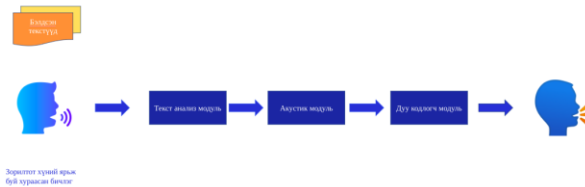
санхүүгийн залилан хийсэн тохиолдлуудыг нийтэлсэн бөгөөд CEO-гийн дуу хоолойг ашиглан 243,000 ам.доллар залилсан байна.[1]



3-р Зураг. Украин Орос хоёрын дайны үеэр Украины ерөнхийлөгч Volodymyr Zelensky хуурамч бичлэг олон нийтийн сүлжээнд тархсан[7]

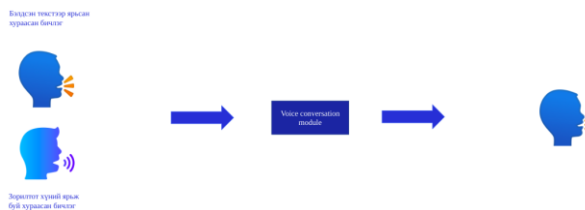
**Deepfake audio төрлүүд:**

1. Synthetic-based - Зорилтот хүний ярьж буй бичлэг болон бэлдсэн текстүүд дээр үндэслэн тухайн хүнийг бэлдсэн текстийн хэлж буй мэтээр хуурамч дуу хоолой үүсгэх



4-р Зураг. Synthetic-based [8]

2. Imitation-based - Зорилтот хүний ярьж буй бичлэг болон бэлдсэн текстийг ярьсан хураасан бичлэг дээр үндэслэн тухайн хүнийг бэлдсэн текстийн хэлж буй мэтээр хуурамч дуу хоолой үүсгэх



5-р Зураг. Imitation-based [8]

**Хуурамч аудио илрүүлэх үндсэн 3 төрөл**

1. Статик хуурамч аудио илрүүлэгч - өгөгдсөн бичлэгийг жинхэнэ эсэхийг шалгах;

2. Real-time хуурамч аудио илрүүлэгч - шууд яриан дундаас хуурамч аудио илрүүлэх;
3. Real-time communication platform хуурамч аудио илрүүлэгч - хуурамч аудио илрүүлэгэх програм хангамж ашиглаж илрүүлэх;



6-р Зураг. Хуурамч аудио илрүүлэх үндсэн 3 төрөл

Машин сургалт /Machine learning/

Хиймэл оюун ухааны дэд хэсэг болох Machine Learning нь тодорхой алгоритм ашиглан машиныг сургадаг буюу даалгавар тус бүрийг тодорхой програмчлалгүйгээр урьдчилан таамаглах эсвэл шийдвэр гаргахад сургадаг[9]. ML нь өгөгдлийн хэв маягийг олох, шийдвэр гаргах, таамаглал гаргахад алгоритм ашигладаг илүү өргөн хүрээний салбар юм. Machine Learning нь шугаман регресс, шийдвэрийн мод, дэмжлэгийн вектор машин зэрэг олон төрлийн загваруудыг агуулдаг тэдгээрийг үндсэн дөрвөн төрөлд авч үзэж болно.

МАШИН СУРГАЛТЫН ҮНДСЭН 4 ТӨРӨЛ

1-р ХҮСНЭГТ

Сурах төрөл	Шошго /мэддэг өгөгдөл/	Зорилго	Жишээ
Supervised	тийм	өмнөх дээр үндэслэн гаралтыг таамаглах	Зургийн ангилал, спам илрүүлэх
Unsupervised	үгүй	хэв маяг, бүтцийг олж мэдэх	Хэрэглэгчийн сегментчилэл, гажиг илрүүлэх
Semi-Supervised	хэсэгчилэн	шошгогүй өгөгдөл ашиглан сайжруулах	бүхий текстийн ангилал үүсгэх
Reinforcement	Шууд бусаар	Үйлдлээр дамжуулан урамшуулах	Тоглоом тоглох, бие даасан робот

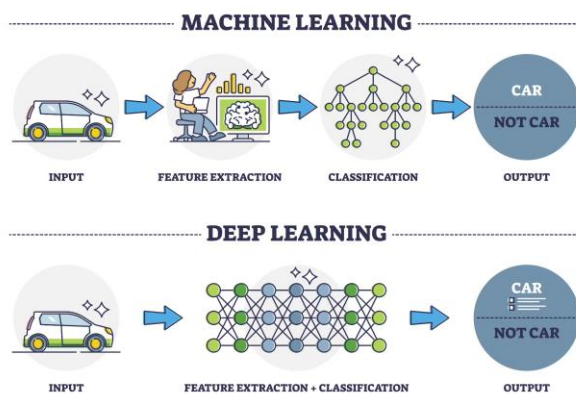
1. Supervised - сургах өгөгдлүүд бүгд мэддэг буюу 1000 өгөгдөл байлаа гэж бодвол 700 нь

жинхэнэ хүний хоолой, 300 нь хуурамчаар үүсгэсэн байна гэдгийг нь мэдэх өгөгдлийн багцтай гэж ойлгож болно

2. Unsupervised - сургах өгөгдлүүдийг огт мэдэхгүй буюу 1000 өгөгдөл байлаа гэж бодвол 1000 нь жинхэнэ эсэхийг нь мэдэхгүй өгөгдлийн багцтай гэж ойлгож болно.
3. Semi-Supervised - сургах өгөгдлүүдийн зарим хэсгийг мэддэг буюу 1000 өгөгдөл байлаа гэж бодвол 500 нь жинхэнэ хүний хоолой, 300 нь хуурамчаар үүсгэсэн байна гэдгийг нь мэднэ, үлдсэн 200 нь жинхэнэ эсэхийг нь мэдэхгүй өгөгдлийн багцтай гэж ойлгож болно.
4. Reinforcement - алдаагаар дамжуулан оновчтой үйлдлүүдийг сурч, нийт шагналыг цаг хугацааны явцад нэмэгдүүлэх бодлого, стратегитай буюу хүрээлэн буй орчинтой харилцаж, санал хүсэлтийг шагнал эсвэл шийтгэл болгон хүлээн авдаг гэж ойлгож болно.

Гүн сургалт /Deep learning/

Deep learning нь түүхий өгөгдлөөс өндөр түвшний функцуудыг автоматаар гаргаж авахын тулд олон давхаргатай мэдрэлийн сүлжээг ашигладаг ML-ийн дэд хэсэг юм[9]. DL-ийг дүрс таних, яриа боловсруулах, байгалийн хэлийг ойлгох гэх мэт илүү төвөгтэй өгөгдөл, даалгавруудыг хүний оролцоогүйгээр хийх боломжийг олгож байна.



7-р Зураг. Машин сургалт болон Гүн сургалт хоёрын ялгаа

III. СУДАЛГААНЫХЭСЭГ

**ӨМНӨ СУДЛАГДСАН АЖИЛУУДААС ХАМГИЙН ИХ ХУВЬ НЭМЭО ОРУУЛСАН СУДАЛГААНЫ АЖИЛУУД**

2-Р ХҮСНЭГТ

№	Судалгааны ажил	Хураангуй	Дэвшүүлсэн санаа	Үр дүн	Хувь нэмэр
1	El-Gayar, M. M., Abouhawwash, M., Askar, S. S., & Sweidan, S. (2024). A novel approach for detecting deep fake videos using graph neural network.	Энэ судалгааны ажлаар GNN ашиглан нүүрний хүрээ гаргах, зургаас дүрслэл рүү буулгах, Graph neural network ашиглах зэргээр хуурамч бичлэгийг илүү нарийвчлалтай илрүүлэх талаар дүрсэлсэн.	Face-to-Face, Face-Swap, Deepfakes, NeuralTextures, FaceShifter зэрэг хуурамч бичлэг илрүүлэх арга техникүүд байдаг ч GNN ашигласан нь хамгийн үр дүнтэй хуурамч бичлэгийг илрүүлэх арга юм.	Face2Face нь 92.49%, NeuralTexture нь 95.09% байсан. Харин GNN ашигласан илрүүлэлт нь 99.3% хүрсэн.	Хуурамч зураг, видео илрүүлэх техник нь байнгын сайжралттай байгаа ч адил хор уршигтай хуурамч аудио илрүүлэх судалгаа бага байсаар байна.
2	Helmus, T. C. (2022). Artificial intelligence, deepfakes, and disinformation. RAND Corporation, 1-24.	Deepfake нь AI, GAN зэргийг ашиглан хуурамч контент үүсгэдэг бөгөөд энэ технологийг ашигласан хуурамч зураг, бичлэг, дуу хоолой, текстүүд ихсэж байгаа нь нийгмийн хуваагдал, нэр төрд халдах, сэтгэл зүйн хямрал зэрэг үр дагавруудыг авчирч байна.	Deepfake нийгэмд маш олон сөрөг үр дагавар авчирч байгаа мөн бүр илүүг авчрах төлөвтэй байгаа тул энэ талаарх судалгаа илүү ихсэх хэрэгтэй.	Хуурамч зураг, видео нь нийгмийн тархи угаалт, сэтгэл зүйн дарамтыг авчирч байна.	Захирлын хуурамч дуу хоолойг ашиглан компаний ажилчин руу залгаж 243,000\$ доллар залилсан хэрэг гарсан.
3	Shaaban, O.A., Yildirim, R., & Alguttar, A. A. (2023). Audio Deepfake Approaches	Эхний хэсэгт Deepfake илрүүлэх үндсэн аргуудын талаарх мэдээллийг багтаасан. Хоёрдахь хэсэгт хуурамч аудио үүсгэх болон илрүүлэх үндсэн аргуудыг тоймлон авч үзсэн.	Хуурамч аудио илрүүлэх аргуудыг туршин хооронд нь харьцуулах. Үүнд: Support Vector Machines (SVMs), Decision Trees (DTs), Convolutional Neural Networks (CNNs), Siamese CNNs, Deep Neural Networks (DNNs), combination of CNNs and Recurrent Neural Networks (RNNs).	Эдгээр аргуудын нарийвчлал нь харилцан адилгүй байсан бөгөөд хамгийн өндөр нарийвчлал нь SVM-д 99%, хамгийн бага нь DT-д 73.33% байв.	Нэгэнт хуурамч аудио илрүүлэх аргуудыг харьцуулсан судалгаа байгаа тул SVMs арга дээр үндэслэн өөрсдийн шинэ хуурамч аудио илрүүлэх системийг хөгжүүлэхэд их хувь нэмэр оруулсан.
4	Mathew, J. J., Ahsan, R., Furukawa, S., Kumar, J. G. K., Pallan, H., Padda, A. S., ... & Pankajakshan, A. (2024).	Бодит цаг хугацаанд статик хуурамч дуу хоолойг ASVspoof ашиглан илрүүлэх байсан. Тэр teams, zoom, google meet зэрэг дээрх дата өгөгдлүүдийг ашиглан туршилт хийсэн. Энэ судалгааны ажилд хуурамч аудио илрүүлэх гол 2 арга нь ResNet based, LCNN based 2 байсан.	Өмнө нь ASVspoof ашигласан бодит цаг хугацаанд дахь хуурамч дуу хоолойг илрүүлдэг технологи байгаагүй ба энэ нь шинээр дэвшүүлсэн санаа байсан.	Нийт 4 модел загвар ашигласан ба үр дүнгийн хувьд 7.39 байснаар хамгийн сайн гүйцэтгэлтэй байсан. Гэвч эдгээр моделууд нь бодит цагийн илрүүлэлт дээр хамаагүй муу байна.	Одоогоор real-time хуурамч аудио илрүүлдэг алгоритмууд тийм ч их хөгжөөгүй байгаа ч хуурамч аудио ашигласан утасны түгжээ гаргах, онлайн аюулгүй мэдээлэлд хандах, утсаар залилан хийх зэрэг нэмэгдсээр байгаа нь илүү нарийвчлалтай судлагдсан synthetic based real-time дуу хоолой илрүүлэгч алгоритм хэрэгтэй юм байна гэх бодлыг өгсөн.

5	Khochare, J., Joshi, C., Yenarkar, B., Suratkar, S., & Kazi, F. (2021). A deep learning framework for audio deepfake detection.	FoR өгөгдлийн багц болон хэд хэдэн машин сургалтын алгоритмыг сонгон авч онцлог шинж чанарт суурилсан арга, дүрс дээр суурилсан арга гэсэн хоёр хэсэгт хуваан туршилт хийсэн.	Энэхүү шийдэл нь VGG16, XceptionNet гэх мэт уламжлалт CNN загваруудтай дүйцэхүйц нарийвчлалтай загварыг танилцуулсан.	Үр дүн TCN алгоритм хялбар бүтэцтэй ч гэсэн 92% нарийвчлалтай үр дүн гаргасан.	Энэхүү аргыг бэлэн өгөгдлийн сан дээр туршин амжилттай ажиллаж байгааг нь харсан тул Real-Time хуурамч аудио илрүүлэхэд ашиглаж болох эсэхийг турших хэрэгтэй санагдсан.
---	---------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Хуурамч дуу хоолой илрүүлэх нь тийм шинэ сэдэв биш боловч жил ирэх тусам хиймэл оюун хөгжихийн хэрээр энэ сэдвийн хүрээнд судлагдсан ажлууд олширч байгаа билээ.

**IV. СЭДЭВ СОНГОСОН ШАЛТГААН**

Хүний амьдралд тус болох зорилгоор анх аудио ном болгон нэвтрүүлсэн хиймэл оюун ашиглан хуурамч хоолой үүсгэх /deepfake audio/ технологи нь сүүлийн жилүүдэд санхүүгийн залилангийн гол хэрэгсэл болсон. Мэдээж хуурамч хоолойг илрүүлэх хэрэгсэл олон байгаа ч одоогоор real-time хуурамч аудио илрүүлдэг алгоритмууд тийм ч их хөгжөөгүй мөн монгол хэл дээр илрүүлэх төхөөрөмж байхгүй байгаа тул өөрсдийн зүгээс хэлсэн үг болон дуу хоолой дээр үндэслэн залиланг илрүүлэх арга боловсруулахыг зорисон.

1. AI-д суурилсан бичвэр болон дүрс засварлах програмуудын хэрэглээ 80%-аар өссөн
2. Захирлын хуурамч дуу хоолойг ашиглан компаний ажилчин руу залгаж 243,000\$ доллар залилан хэрэг гарсан
3. Хуурамч зураг видео илрүүлэх техник нь одоогийн байдлаар багадаа 91.5%, хуурамч аудио илрүүлэх техник нь ихдээ 95.2% ч илүү нарийвчлал нарийн техник хэрэгтэй байгаа[11].
4. 2 жилийн дараа гэхэд хуурамч дуу хоолой ашигласан залилан нь дэлхийн хэмжээнд 82% хүрэх төлөвтэй байгаа нь deepfake чиглэлийг илүү чухалчилж судлах нь хэрэгцээтэй юм байна гэх мотиваци өгсөн

**V. ЗОРИЛГО, ЗОРИЛТ**

Сүүлийн жилүүдэд Audio Deepfakes (ADs) гэж нэрлэгддэг хиймэл оюун ухаан дээр суурилсан хүний дуу хоолой, видео, зураг, текстийг нэгтгэж хиймлээр дуурайлган үүсгэх технологийн тусламжтай гэмт хэргийн зорилгоор хиймэл контент үүсгэж худал хуурмаг мэдээлэл нийгэмд түгээх, хувь хүн рүү

чиглэсэн халдлага зохион байгуулах зэрэгт ашиглах болсон. Ийнхүү сүүлийн үед AD нь судлаачдын анхаарлыг татах болсон бөгөөд тэдгээрийг илрүүлэхийн тулд Machine Learning (ML) болон Deep Learning (DL) аргуудыг боловсруулж байна. Мэдээж дүрс бичлэгийн хуурамч дүрсийг тодорхойлоход ихээхэн ахиц дэвшил гарсан. Гэсэн хэдий ч монгол хэл дээр энэ төрлийн судлагдсан ажил байхгүй. Энэхүү судалгаан ажлын хүрээнд бид дуу хоолойны онцлог болон хэлсэн үгнүүд дээр дүн шинжилгээ хийн залилан байх боломжтой эсэхийг тодорхойлох хиймэл оюун хөгжүүлэхийг зорьсон.

Зорилт:

1. Төстэй системийн судалгаа хийх
2. Хурдан алгоритм шалгаж олох
3. Өөрсдийн бүтцийн схемийг зохиох
4. Туршилт хийж үр дүнг тайлагнах

**VI. ТУРШИЛТ**

- *Бүтцийн схем*



8-р Зураг. Бүтцийн схем

**Deepfake audio илрүүлэх техникүүд:**

Feature Analysis and Signal Processing Techniques [12]

Mel-frequency Cepstral Coefficients (MFCC) - MFCC нь аудио боловсруулахад өргөн хэрэглэгддэг богино хугацааны цахилгааны спектрийн шинж

чанарыг олж авдаг. Эдгээр коэффициентүүд нь байгалийн сонсогддог боловч хүний ярианы нарийн спектрийн шинж чанаргүй синтетик хоолойн гажигуудыг илрүүлж чаддаг.

Linear Predictive Coding (LPC) - Энэ техник нь дууны замыг төлөөлөх шүүлтүүрийг тооцоолохын тулд ярианы дохиог шинжилдэг. Байгалийн болон синтетик дууны замын шинж чанаруудын ялгааг LPC шинжилгээг ашиглан тодорхойлж болно.

#### Machine Learning-Based Classifiers [12]

Support Vector Machines (SVMs) - SVM ангилагчийг MFCC болон бусад аудио функцуудтай хослуулснаар бодит болон хуурамч аудио ангилалд тусалдаг. SVM нь том хэмжээний функцтэй ажиллахад онцгой ач холбогдолтой бөгөөд сургалтын хязгаарлагдмал өгөгдөлтэй үр дүнтэй ажиллах боломжтой.

Random Forest and Gradient Boosting Classifiers - Эдгээр сургалтын аргууд нь аудио файлуудаас гаргаж авсан функцүүдийн хослолд дүн шинжилгээ хийх замаар ангиллын нарийвчлалыг сайжруулж чадна.

#### Deep Learning Models [12]

Convolutional Neural Networks (CNNs) - CNN нь спектрограммд (дууны давтамжийн дүрслэл) шинжилгээ хийхэд өргөн хэрэглэгддэг. Аудио спектрограмм болгон хувиргаснаар CNN нь синтетик заль мэхийг илтгэж болох харааны хэв маягийг тодорхойлж чадна.

Recurrent Neural Networks (RNNs) and Long Short-Term Memory Networks (LSTMs) - Эдгээр загварууд нь дараалсан өгөгдлийн хэв маягийг авахдаа маш

сайн бөгөөд аудио файлуудын цаг хугацааны тогтвортой байдалд дүн шинжилгээ хийхэд үр дүнтэй байдаг. Гүн хуурамч аудионы хувьд RNN болон LSTM нь дууны давтамж, хэмнэл болон бусад дараалсан шинж чанаруудын байгалийн бус хэв маягийг илрүүлж чаддаг.

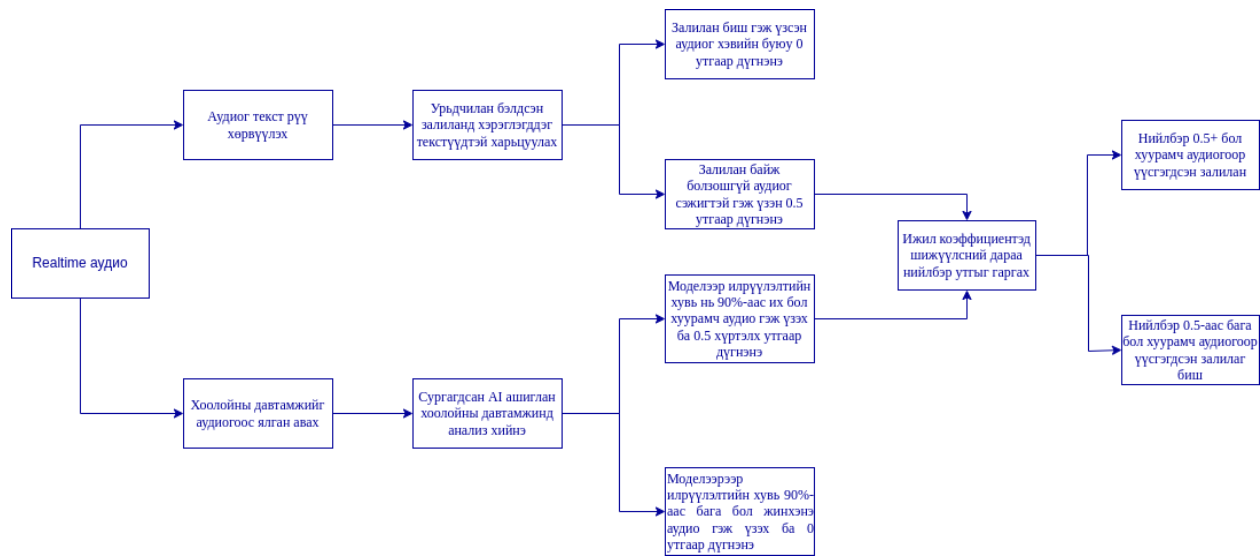
#### Voice Biometric Analysis [12]

Speaker Verification and Voice Biometrics - Чанга яригчийг баталгаажуулах технологийг ашигладаг дуут биометрийн систем нь дуу хоолойг мэдэгдэж буй чанга яригчийн профайлтай тааруулж, синтетик дуу хоолой эсвэл хувилсан дуу хоолойны загварыг илтгэх зөрчилтэй байдлыг тэмдэглэж чаддаг.

Cross-Modal Techniques - Видеон дээрх уруулын хөдөлгөөнтэй дуу хоолойг (боломжтой бол) харьцуулах замаар кросс-модаль гүн хуурамч илрүүлэлт нь гүн хуурамч хэвлэл мэдээллийн хэрэгсэлд түгээмэл тохиолддог аудио болон визуал дохионы хооронд үл нийцэх байдлыг тодорхойлох боломжтой.

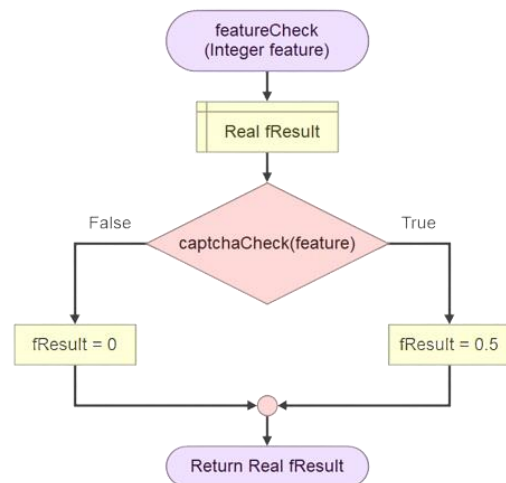
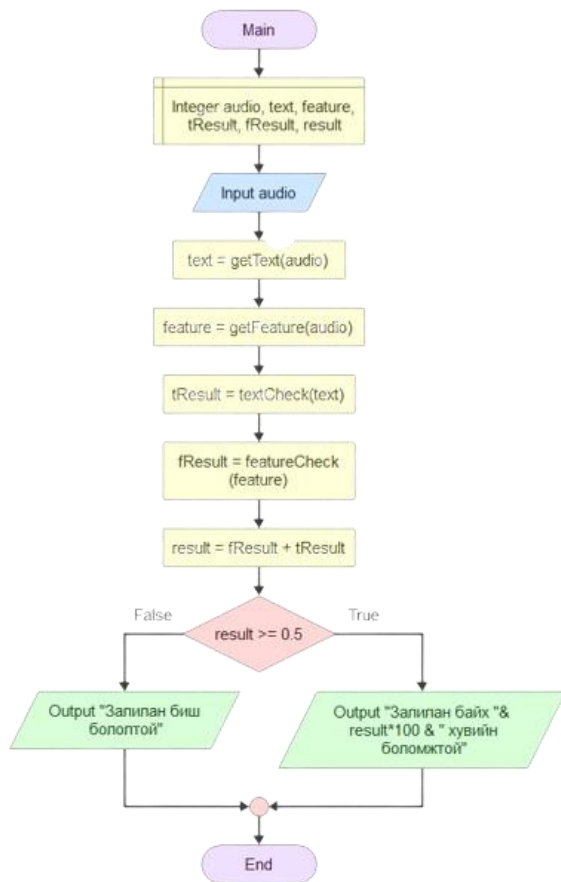
#### Spectrogram-Based Detection [12]

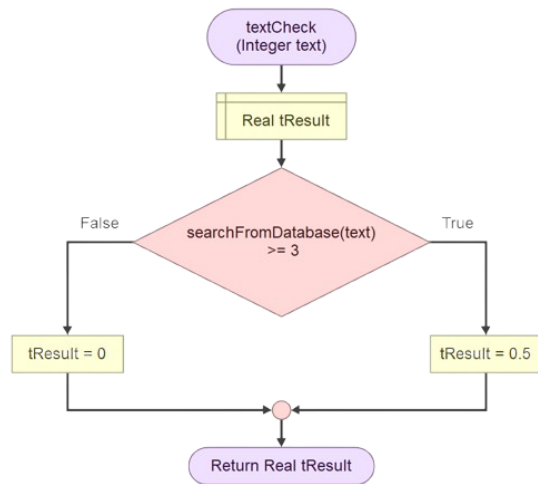
Wavelet Transform and Fourier Transform Analysis - Эдгээр аргууд нь аудио дохиог бүрэлдэхүүн хэсгүүдэд задалж, синтетик дуу хоолой нь ихэвчлэн нэвтрүүлдэг олдворуудыг илрүүлэх боломжийг олгодог. Спектрограммууд нь цаг хугацааны давтамжийн дүрслэлийг өгч, дууны өнгө, бүтэц дэх ялгааг илрүүлдэг тул гүн хуурамч загваруудад жинхэнэ хуулбарлахад хэцүү байдаг.



9-р Зураг. Туршилтын бүтцийн схем

Алгоритм





10-р Зураг. Судалгааны ажил дээрхи хуурамч аудио илрүүлэх алгоритм  
Сургах үйл явц

Өмнө судлагдсан ажлууд дунд энгийн өгөгдлийн багц дээр хийсэн туршилтууд дунд хамгийн өндөр буюу 99% -ийн чанартай зөв хариу гаргаж байсан SVMs гэх машин сургалтын арга нь real-time буюу шууд орж ирсэн өгөгдөл дээрх туршилтад ч мөн чанартай үзүүлэлт гаргах боломжтой тул SVMs аргыг ашиглаж туршилтаа хийсэн.

Машин сургалтанд ашигласан өгөгдлийн багцууд:

False-or-Real (FoR) нь бодит хүмүүс болон хиймэл оюун ухаанаар үүсгэсэн дуу хоолойн 195,000 гаруй бичлэгтэй өгөгдлийн багц

- For-original
- For-norm
- For-2sec
- For-rerec

ASVspoof 2021 нь бодит болон синтетик хуурамч дуу хоолойн бичлэгийг агуулсан 181566 өгөгдлийн багц

- Logical Access (LA)
- Physical Access (PA)
- DeepFake (DF)

Function load\_labels(metadata\_file):

```

file_to_label ← Empty dictionary
Open metadata_file for reading:
For each line in metadata_file:
  Split line into parts
  If parts has at least 5 items:
    file_id ← parts[1]
  
```

```
label ← parts[5]
```

```
file_to_label[file_id] ← 1 if label is 'spoof' else
```

```
0
```

```
Print "Loaded {length of file_to_label} labels"
```

```
Return file_to_label
```

Function count\_label\_types(file\_to\_label):

```
spoof_count ← Count values in file_to_label that are
```

```
1
```

```
genuine_count ← Count values in file_to_label that
```

```
are 0
```

```
Print "Spoof samples:", spoof_count, "Genuine
```

```
samples:", genuine_count
```

```
Return spoof_count, genuine_count
```

Function load\_data\_from\_folder(folder, file\_to\_label, max\_files):

```
features ← Empty list
```

```
labels ← Empty list
```

```
files_found ← List of all '.flac' files in folder
```

```
Print "Found {length of files_found} audio files"
```

```
For i, file_path in files_found:
```

```
  file_name ← Remove '.flac' extension from
```

```
file_path
```

```
  If file_name in file_to_label:
```

```
    label ← file_to_label[file_name]
```

```
    Try:
```

```
      audio, sr ← Load audio from file_path
```

```
      mfcc ← Compute MFCC from audio
```

```
      mfcc_mean ← Mean of mfcc across time axis
```

```
      Add mfcc_mean to features
```

```
      Add label to labels
```

```
      Print "Running on {i}th file"
```

```
    Catch exception as e:
```

```
      Print "Error loading file:", file_name, e
```

```
  If i + 1 ≥ max_files:
```

```
    Print "Reached max files for testing"
```

```
    Break
```

```
Print "Loaded {length of features} audio features and
```

```
{length of labels} labels"
```

```
Return features, labels
```

Function prepare\_data\_for\_training(audio\_folder, metadata\_file, max\_files):

```
file_to_label ← load_labels(metadata_file)
```

```

    count_label_types(file_to_label)
    features, labels ←
load_data_from_folder(audio_folder, file_to_label,
max_files)
    Print "Label distribution:", unique(labels), "Counts:",
counts(labels)
    Return features, labels

Function train_and_evaluate_model(X, y):
    X_train, X_test, y_train, y_test ← Split X and y into
train and test sets
    model ← LogisticRegression()
    Train model on X_train and y_train
    y_pred ← Predict labels for X_test using model
    accuracy ← Calculate accuracy between y_test and
y_pred
    Print "Model accuracy:", accuracy * 100
    Save model as 'spooof_detection_model.pkl'
    Print "Model saved as 'spooof_detection_model.pkl'"
    Return model

// Main program
audio_folder ← 'ASVspooof2021_LA_eval/flac'
metadata_file ← 'keys/LA/CM/trial_metadata.txt'
features, labels ←
prepare_data_for_training(audio_folder,
metadata_file, max_files=181566)
model ← train_and_evaluate_model(features, labels)

```

1-р Код. ASV spooof LA өгөгдлийн багц ашиглан машинаа сургасан

### Туришлын үйл явц

```

Function load_model(model_file):
    model ← Load model from model_file
    Print "Loaded model for real-time prediction"
    Return model

Function capture_and_predict(model, duration=3,
sample_rate=16000):
    Print "Recording..."

    audio ← Record audio with duration * sample_rate
samples, sample_rate, and 1 channel
    Wait for recording to complete
    Flatten audio array to a 1-dimensional array

```

```

mfcc ← Calculate MFCC from audio with sample_rate
and 13 coefficients
mfcc_mean ← Calculate mean of mfcc across time
axis

prediction ← Use model to predict label based on
mfcc_mean
If prediction is 1:
    Print "Prediction: Spooof"
Else:
    Print "Prediction: Genuine"

model_file ← 'spooof_detection_model.pkl'
model ← load_model(model_file)
capture_and_predict(model)

```

2-р Код. Сургасан машинаа ашиглан туришиж үзсэн

```

Function find_common_words(words_file,
result_file):
    // Read the first file (words_file)
words_set ← New set()
    Open words_file for reading:
    For each line in words_file:
        Trim whitespace and convert to lowercase
        Add the line to words_set

    // Read the second file (result_file)
result_words ← New set()
    Open result_file for reading:
    For each line in result_file:
        Trim whitespace and convert to lowercase
        Split the line into words and add them to
result_words

common_words ← words_set ∩ result_words
common_count ← Count(common_words) // Count
of common words

    Return common_words, common_count

Function real_time_audio_recognition(result_file,
words_file):

```

Open microphone:

Print "Ready to receive audio..."

Adjust ambient noise level

Repeat indefinitely:

Open result\_file for writing:

Print "Listening for audio..."

audio ← Receive audio (timeout = 10 seconds)

text ← Convert audio to text

Print "Transcribed text: " + text

Write text to result\_file

// Check for common words after 5 seconds of no audio

common\_words, common\_count ← find\_common\_words(words\_file, result\_file)

If common\_words is not empty:

Print "Common words: " + common\_words

Print "Count of common words: " + common\_count

Else:

Print "No common words found."

// Handle exceptions:

If unable to recognize audio:

Print "Could not recognize audio."

If request error occurs:

Print "Request error; {error}"

If KeyboardInterrupt:

Print "Stopped."

Break

// Run the audio recognition function

result\_file ← "result.txt"

words\_file ← "words.txt"

real\_time\_audio\_recognition(result\_file, words\_file)

3-р Код. Ярианаас текст болгох

### Үр дүн

```
(pws@1em) - [~/Desktop/F.NS354/code]
$ python3 diff.py
Давхцсан үгс: {'яаралтай', 'данс'}
```

1-р Үр дүн. Давхардсан үг тоолсон байдал

```
Model accuracy: 89.58%
Model saved as 'spoof_detection_model.pkl'
```

2-р Үр дүн. Машин сургаж дууссан байдал

```
(v10d@tool) - [~/Downloads/papers/test_detection]
$ python3 real_time.py
Loaded model for real-time prediction
Recording...
Prediction: Spoof

(v10d@tool) - [~/Downloads/papers/test_detection]
$ python3 real_time.py
Loaded model for real-time prediction
Recording...
Prediction: Genuine
```

3-р Үр дүн. Машин сургаж дууссан байдал

## VII. ДҮГНЭЛТ

Энэхүү судалгаан ажлын хүрээнд бид дуу хоолойны онцлог болон хэлсэн үгнүүд дээр дүн шинжилгээ хийн залилан байх боломжтой эсэхийг тодорхойлох хиймэл оюун хөгжүүлсэн. Бидний зүгээс дуу хоолойг текст рүү хөрвүүлээд тэр текст дундаас залилан хийхэд ашиглагдаж болох үгнүүд буюу мөнгө, дансны дугаар, шилжүүлэх, нууц үг зэрэг үгсийг харилцан яриандаа ашиглаж байвал 0.5 оноо үгүй бол 0 оноо өгөхөөр сургасан ба дараагаар нь мөн адил хоолойн онцлогийг ялган авч энгийн хүн болон машин хуурамчаар үүсгэсэн эсэхийг ялгахар тохируулан машин хуурамчаар үүсгэсэн гэж үзвэл 0.5, хүний хоолой мөн гэж үзвэл 0 оноо өгөх ба өмнөх текстээс авсан оноо болон хоолойноос авсан онооны нийлбэр дүнгээс эцсийн хариу гарна. Чанарын үзүүлэлт нь 89.58% буюу real-time илрүүлэхэд хангалттай сайн эхлэл гэж бодож байгаа. Энэ ажлыг үргэлжлүүлэн дуудлага хийх боломжтой байдаг программ хангамжуудтай хамтарч ажилладаг болгохыг зорьж байгаа.

## VIII. АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] <https://fiu.mongolbank.mn/mn/r/543>

- 
- [2] Bateman, J. (2022). Deepfakes and synthetic media in the financial system: Assessing threat scenarios. Carnegie Endowment for International Peace.
- [3] Khanjani, Zahra, Gabrielle Watson, and Vandana P. Janeja. "How deep are the fakes? focusing on audio deepfake: A survey." arXiv preprint arXiv:2111.14203 (2021).
- [4] Almutairi, Z., & Elgibreen, H. (2022). A review of modern audio deepfake detection methods: challenges and future directions. *Algorithms*, 15(5), 155.
- [5] Yi, J., Wang, C., Tao, J., Zhang, X., Zhang, C. Y., & Zhao, Y. (2023). Audio deepfake detection: A survey. arXiv preprint arXiv:2308.14970.
- [6] Patel, Yogesh, et al. "Deepfake generation and detection: Case study and challenges." *IEEE Access* (2023).
- [7] Zhang, Tao. "Deepfake generation and detection, a survey." *Multimedia Tools and Applications* 81.5 (2022): 6259-6276.
- [8] C. Stupp, "Fraudsters used ai to mimic ceo's voice in unusual cybercrime case," *The Wall Street Journal*, vol. 30, no. 08, 2019.
- [9] Kufel, J., Bargiel-Łączek, K., Kocot, S., Koźlik, M., Bartnikowska, W., Janik, M., ... & Gruszczyńska, K. (2023). What is machine learning, artificial neural networks and deep learning?—Examples of practical applications in medicine. *Diagnostics*, 13(15), 2582.
- [10] Rabhi, M., Bakiras, S., & Di Pietro, R. (2024). Audio-deepfake detection: Adversarial attacks and countermeasures. *Expert Systems with Applications*, 250, 123941.
- [11] Khochare, J., Joshi, C., Yenarkar, B., Suratkar, S., & Kazi, F. (2021). A deep learning framework for audio deepfake detection. *Arabian Journal for Science and Engineering*, 1-12.
- [12] Hamza, A., Javed, A. R. R., Iqbal, F., Kryvinska, N., Almadhor, A. S., Jalil, Z., & Borghol, R. (2022). Deepfake audio detection via MFCC features using machine learning. *IEEE Access*, 10, 134018-134028.

## ГУРВАН ХЭМЖЭЭСТ ХИЙСВЭР БИЕТ ЗАГВАР БҮТЭЭХ

Батбилэгийн ТЭМҮҮЛЭН<sup>1</sup>, Ариунзолын БАЯРЖАВХЛАН<sup>1</sup>, Цэвээнлхаазалийн ТӨГӨЛДӨР<sup>1</sup>,  
Цогбаярын БЭЛГҮТЭЙ<sup>1</sup>, Бадарчийн ТУЯАЦЭЦЭГ<sup>1</sup>

<sup>1</sup> Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Компьютерын ухааны салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: tuyatsetseg.b@must.edu.mn<sup>1\*</sup>*

**Хураангуй:** Энэхүү төсөл нь бодит объектын гурван хэмжээст дүрсийг үүсгэх зориулалттай 3D багажийн хөгжүүлэлт ба хэрэгжүүлэлтийг танилцуулж байна. Энэ төслийн ерөнхий шинжлэх ухааны нэршил нь фотограмметри буюу энэ нь зургаас 3D биет үүсгэх явдал юм. Систем нь объектын бичлэгийг олон өнцгөөс авч, дараа нь бичлэгийг зураг хэлбэрт өндөр нарийвчлалтай фрэймүүдээр хувиргаж зургуудаас чанар сайтайг нь ялгаж аваад OpenCV санг ашиглаж 25% ба түүнээс бага алдагдалтай зургуудыг хадгална. Нээлттэй эх сурвалжийн хэрэгсэл болох Meshroom ба AliceVision-ний санг ашиглан задалсан зургуудыг боловсруулж, объектын геометр болон гадаргуугийн бүтцийг үнэн зөв илэрхийлнэ. Мөн төслийн загварыг бүтээх үйл явцад AliceVision санг ашигласнаар олон өнцгөөс авсан зургуудыг нарийвчлалтай болон чанартай боловсруулах чадвартай. AliceVision нь фотограмметрийн алгоритмуудыг багтаасан бөгөөд энэ нь 2D зургийг илүү бодитой 3D загвар болгон хувиргахад чухал үүрэгтэй юм. Фотограмметрийн техник нь объектын гадаргууг янз бүрийн өнцгөөс боловсруулахын тулд олон тооны зураг ашиглах шаардлагатай бөгөөд үүнийг бүтээхийн тулд зургийг ерөнхий хэрэглэгддэг төрлийн нэгээр нь хүлээн авч түгээмэл хэрэглэгддэг 3D төрөлд хувиргах юм. Объектын хэмжээсийг нарийвчлалтай авснаар техник нь дизайн, үйлдвэрлэл, хийсвэр дүрслэл зэрэгт хэрэглэхэд тохиромжтой өндөр нарийвчлалтай загваруудыг гаргаж чадна. Үүссэн 3D загвар нь холбогдсон нүүрэн дээр гарч, хэрэглэгчдийн гаргасан объекттой янз бүрийн өнцгөөс харьцах боломж олгодог. 3D загварыг эргүүлж, томруулж болох бөгөөд энэ нь дижитал орчинд объекттой нарийн дүн шинжилгээ хийх, харилцан үйлчлэх боломжийг олгодог. Энэхүү төсөл нь дижитал хуулбарыг бүтээхэд 3D фотограмметри технологийн үр нөлөөг харуулж, чанарын хяналт, дижитал график салбарт хувь нэмрээ оруулдаг.

*Түлхүүр үг:* Фотограмметри, 3D загварчлал, OpenCV, Meshroom, AliceVision

### I. УДИРТГАЛ

Сүүлийн жилүүдэд 3D загварчлал нь бүтээгдэхүүний дизайн, виртуал орчин зэрэг салбаруудын салшгүй хэсэг нь болж, салбарууд хэрэглэгчдэд 3D биет объектын хуулбарыг бүтээх боломжийг олгож байна. Фотограмметри нь объектын бичлэгийг зураг болгон авч 3D биет болгон гаргаж авах замаар ажилладаг. Энэхүү төсөл нь видео бичлэг болон фотограмметрийн программ хангамжийг ашиглан нарийвчилсан 3D загвар бүтээх замаар илүү хүртээмжтэй, зардал багатай хувилбарыг хөгжүүлэх зорилготой юм. Тус судалгааны ажлаар 3D загвар гаргахад тохиолдож байгаа сүүлийн үеийн технологийн асуудлууд дээр тулгуурлан тодорхой шийдлүүдийг авч үзэхийг зорьсон. Энэ чиглэлд тухайлбал, ойрын зайн фотограмметр нь 3D загварчлалын нарийвчлалыг гар аргаар эсвэл автоматаар хэмжиж олон жилийн турш ажиллаж ирсэн. Өнөө үед 3D сканнерууд нь хэрэглээний олон талбарт өгөгдөл оруулах стандарт эх үүсвэр болж байгаа боловч загварчлал нь зөөврийн, уян хатан, өргөн хэрэглэгддэг байаар хөгжигдсээр байгаа.

### II. АРГА ЗҮЙ

Видеоноос 3D загвар бүтээх бидний үйл явц нь гурван үндсэн үе шатыг агуулдаг: видео бичлэг хийх, зураг задлах, хөрвүүлэх, AliceVision ашиглан 3D загварыг дахин бүтээх.<sup>[2]</sup> Фотограмметр бол гэрэл зургаас хэмжилт хийх шинжлэх ухаан юм. Энэ нь ямар нэг дараалалгүй гэрэл зураг эсвэл видео бичлэгээс геометрийг дүрслэлийг үүсгэдэг. Гэрэл зураг гэдэг нь 3 хэмжээст үзэгдлийг 2 хэмжээст

хавтгайд тусгах процессоор тодорхойлогдох бөгөөд фотограмметрийн зорилго нь энэ үйл явцад ашиглагддаг үндсэн шийдэл юм.

#### 1. Видео бичлэг хийх

Объектын дүрсийг янз бүрийн өнцгөөс авахын тулд эхлээд бүх талаас нь видео бичлэг хийнэ. Объектыг тогтвортой гадаргуу дээр байрлуулсан бөгөөд камерыг тойруулан хөдөлгөж, тодорхой зайтай байлгадаг. Бид тодорхой мэдээлэл авахын тулд өндөр нарийвчлалтайгаар (1080p ба түүнээс дээш) бичлэг хийх шаардлагатай бөгөөд загварт саад болох сүүдэр, тусгалаас зайлсхийхийн тулд жигд гэрэлтүүлгийн орчин бүрдүүлэх хэрэгтэй.

#### 2. Зургийг задлах, хөрвүүлэх

Бичлэг хийсний дараа янз бүрийн өнцгөөс авсан зургийн цуглуулгыг авахын тулд тодорхой давтамжтайгаар видеоноос фреймүүд гаргаж авдаг. Дараа нь эдгээр фреймүүдийг PNG формат руу хөрвүүлдэг бөгөөд энэ нь боловсруулахад зориулсан зургийн тод байдал, чанарыг сайжруулдаг. Энэхүү зургийн хөрвүүлэлт нь фрейм тус бүрийн нарийн мэдээллийг авч илүү нарийвчлалтай 3D загвар бүтээхэд AliceVision-д тусалдаг.

#### 3. AliceVision ашиглан 3D загвар бүтээх

Хөрвүүлсэн PNG зургуудыг AliceVision сангийн функцуудад ачаалах бөгөөд AliceVision 3D загвар бүтээхийн тулд тэдгээрийг олон үе шат дамжуулан боловсруулдаг.<sup>[3][4]</sup> AliceVision нь объектын хэлбэр, гадаргууг сэргээхийн тулд зурган дээрх давхацсан

нарийн өгөгдлийг шинжилдэг. Үндсэн загвар бүтээгдсэний дараа анхны зургуудын бүтцийг хэрэглэж, загварт бодит дүр төрхийг өгдөг. Эцсийн 3D загварыг дараа нь экспортолж, өөр өөр өнцгөөс харж, нарийвчлан судлах боломжтой.

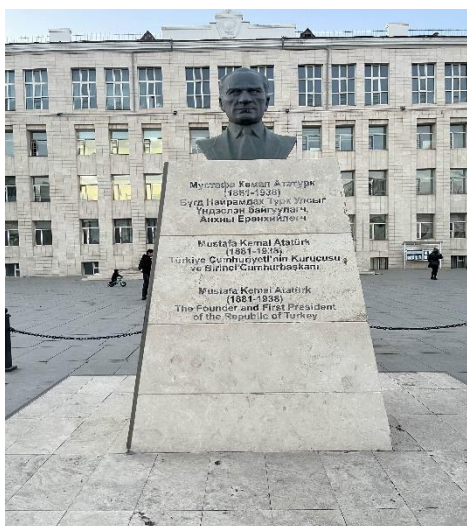
### III. ҮР ДҮН

Манай видео бичлэгээс 3D загвар бүтээх үйл явц нь дүрсийг PNG формат руу хөрвүүлж, AliceVision ашиглан боловсруулснаар дараах үр дүнг үзүүлээ.

#### 1. Загварын нарийвчлал ба чанар:

Манай аргаар бүтээсэн загварууд нь сканнердсан объектуудын хэлбэр болон гадаргуугийн бүтэцийг өндөр нарийвчлалтайгаар буулгаж чадаж байна. Гадаргуугийн нумарсан хэлбэрүүд, жижиг хотгор, бүтэцийн ялгаа зэрэг нарийн ширийн зүйлс өндөр нягтаршилтай хэсгүүдэд илүү тод харагддаг. Стандарт дүрсний форматуудтай харьцуулахад PNG форматтай зураг ашигласнаар загварын нарийн деталиудыг хадгалж чадсан нь зурагт харагдаж байна.

Авсан зураг:



1-р зураг



2-р зураг

#### 2. Гадаргуугийн бүтцийн дэлгэрэнгүй байдал:

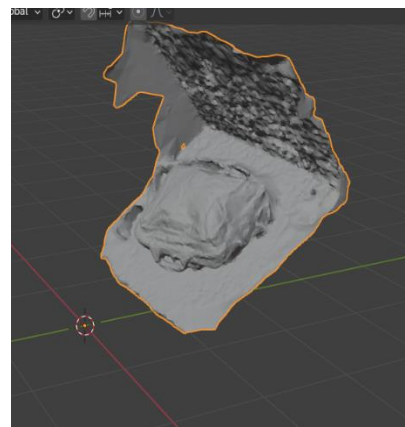
Олон өндөр нарийвчлалтай зураг ашигласнаар гадаргуугийн бүтэц нь бодит объектын дүртэй илүү дөхөм болж байна.

Манай арга хэвийн нөхцөлд үр дүнтэй байсан ч гэрэлтүүлгийн жигд бус байдал, сүүдэр үүссэнээр зарим загваруудад нөлөөлсөн бөгөөд энэ нь доорх зургуудад харагдаж байна. Гялалзсан болон маш бараан гадаргуутай объектуудыг тодорхой буулгахад хэцүү байсан бөгөөд энэ нь фотограмметрийн ердийн асуудал бөгөөд гэрлийн нэмэлт эх үүсвэрийг ашигласнаар төвөгтэй гадаргууг буулгахад тус болно.

Авсан зураг:



3-р зураг



4-р зураг

## ДҮГНЭЛТ

Энэхүү төсөлд бид 3D загвар бүтээх өндөр чанартай аргачлалыг амжилттай боловсрууллаа. Бид видео бичлэгийн аргаар динамик дүрсүүдийг статик зургуудад хувиргаж, эдгээрийг илүү нарийвчлалтай, бодитой болгохын тулд боловсруулалт хийсэн. Мөн зургийн файлуудыг PNG формат руу хөрвүүлснээр зургийн чанарыг алдахаас сэргийлж, 3D загвар бүтээхэд илүү тохиромжтой болсон.

AliceVision програмыг ашиглан бид камерын анхны тохиргоо, онцлог шинж чанарын танилт, гүний зураг гаргах үе шатуудыг агуулсан хүчирхэг үйл явцыг хэрэгжүүлсэн. Хөдөлгөөнт бүтэц үүсгэх үе шатанд зарим файлын асуудал болон хосолсон зураг илрүүлэхэд бэрхшээл гарсан ч бид тохиргоог өөрчилж, амжилттай загвар бүтээх нөхцөлийг бүрдүүлж чадсан юм.

Энэхүү ажлын үр дүн нь манай аргачлалын боломжийг тод харуулж байна. Энэ аргыг соёлын өвийг дижиталаар архивлах<sup>[1]</sup>, виртуал бодит байдал болон симуляцийн нарийвчилсан загвар бүтээх зэрэг

олон төрлийн хэрэглээнд ашиглах боломжтой юм. Ирээдүйд бид үйл явцыг нарийвчлах, онцлог шинжийг илүү сайн таних алгоритмуудыг боловсруулах боломжтой. Энэ төсөл нь 3D дүрслэлийн технологиор бодит эд зүйлсийг дижитал хөрөнгө болгох үр дүнтэй арга болохыг харуулж, олон салбарт шинэлэг хэрэглээг бий болгох боломжийг нээж байна.

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] W. R. Bascom, "Possible Applications of Kite Photography to Archaeology and Ethnology," Illinois State Academy of Science, Transactions, vol. 34, pp. 62–63, 1941.
- [2] AliceVision Meshroom, [Online]. [Accessed: Nov. 1, 2024]. <https://github.com/alicevision/Meshroom>
- [3] A. Yurasov, "3D Modeling with Python," Medium, Oct. 2018. [Online]. [Accessed: Nov. 1, 2024]. <https://medium.com/@alexeyyurasov/3d-modeling-with-python-c21296756db2>
- [4] GeeksforGeeks, "3D Modeling & Animation App using Python – Part 1," [Online]. [Accessed: Nov. 1, 2024]. <https://www.geeksforgeeks.org/3d-modeling-animation-app-using-python-1/>

## ДҮРСИЙН БОЛОВСРУУЛАЛТАД СУУРИЛСАН УХААЛАГ ХОГ АНГИЛАГЧ

Ариунболдын ЦОЛМОНБАЯР<sup>1</sup>, Батбаатарын БОЛОРЖИН<sup>2</sup>, Бямбасүрэнгийн ЭНХЗУЛ<sup>3</sup>, Бямбадоржийн ЗОЛЗАЯА<sup>4</sup>

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: [b.zolzaya@must.edu.mn](mailto:b.zolzaya@must.edu.mn)<sup>1\*</sup>

**Хураангуй:** Бидний эргэн тойронд өдөр тутам их хэмжээний хог хаягдал үүсэж, хуримтлагддаг ч хүмүүс ихэвчлэн хог хаягдлаа хаана очиж, хэрхэн боловсруулагддаг талаар тэр бүр боддоггүй. Хог хаягдлын талаарх ойлголтыг нэмэгдүүлэх, түүнд зориулсан үр дүнтэй бүтээгдэхүүн хөгжүүлснээр бидний хэрэглээний хэв маягт эерэг өөрчлөлт оруулж, хүрээлэн буй орчныг хамгаалахад үнэтэй хувь нэмэр оруулах боломжтой юм. Энэхүү судалгаанд бид дахин боловсруулах хог хаягдлыг төрөлжүүлэн ангилах зорилгоор MobileNetV2, YOLOv11n-cls, MobileNetV2+SVM гэсэн гурван ангиллын загварыг сургаж, тестийн өгөгдөл дээр гүйцэтгэлийг нь харьцуулан үнэллээ. Туршилтын үр дүнгээс үзэхэд өгөгдлийн хязгаарлагдмал нөхцөлд MobileNetV2 загвар нь бусад загваруудаас илүү өндөр нарийвчлал (90%), гүйцэтгэлтэй гарч, хог хаягдлыг илүү үр дүнтэй таних чадварыг харуулсан байна. Уг судалгаа нь хог хаягдлыг хүний оролцоог багасган, автоматаар таньж ангилах шийдлийг боловсруулснаар дахин боловсруулах үйл явцыг хялбарчлах, хүрээлэн буй орчны бохирдлыг бууруулахад дэмжлэг үзүүлэх боломжтой.

**Түлхүүр үг:** Convolutional Neural Networks, MobileNetV2, yolo, MobileNetV2+SVM

### I. УДИРТГАЛ

Өдрөөс өдөрт өсөн нэмэгдэж буй хог хаягдалтай холбоотой асуудлыг шийдвэрлэх нь нийгэм, байгаль орчинд тулгарч буй хамгийн чухал сорилтуудын нэг юм. Харамсалтай нь ихэнх тохиолдолд хог хаягдлыг зөв менежментгүйгээр шууд хаяснаар байгаль орчинд аюул учруулах төдийгүй эдгээр хаягдлыг дахин ашиглах боломж алдаж байдаг. Жишээлбэл, пластик, шил, металл зэрэг хатуу хог хаягдал нь урт удаан хугацааны туршид задардаг тул байгаль орчныг бохирдуулж, нөөц баялгийг багасгадаг. Энэ нөхцөл байдал нь хог хаягдлыг ангилан дахин боловсруулах ажлыг зохистойгоор гүйцэтгэх шаардлагатайг улам тодотгож байна. Гэвч хог хаягдлыг зөвхөн гараар ялган боловсруулах нь ихээхэн цаг хугацаа, хөдөлмөр шаарддаг тул технологийн дэвшлийг ашиглан хог хаягдлыг автоматжуулан ангилах боломжийг эрэлхийлэх нь үр дүнтэй шийдэл юм.

Хүн амын тоо нэмэгдэхийн хэрээр хог хаягдлын хэмжээ өсөж, үүнээс үүдэн байгаль орчны бохирдол, уур амьсгалын өөрчлөлтөд сөрөг нөлөө үзүүлж байна. Дэлхийн банкны тайланд дэлхий даяар жил бүр 4 тэрбум тонн хог хаягдал хаягддаг бөгөөд 2025 онд 70 орчим хувиар өсөх төлөвтэй байна [1]. 25 жилийн дараа гэхэд буурай хөгжилтэй орнуудын хог хаягдлын хуримтлал эрс нэмэгдэнэ гэж үзэж байна. Хог хаягдлыг удирдахад өргөн хэрэглэгддэг арга нь булаах бөгөөд энэ нь үр ашиггүй, өртөг өндөртэй, байгаль орчныг бохирдуулдаг. Жишээлбэл, хогийн цэг түүний эргэн тойронд байгаа хүмүүсийн эрүүл мэндэд сөргөөр нөлөөлдөг. Хог хаягдлыг боловсруулах бас нэг өөр арга нь хог хаягдлыг шатаах явдал бөгөөд энэ арга нь хог хаягдлаас зарим аюултай хорт хий, хүнд металлуудыг ялгаруулснаар агаар, хөрс, усыг бохирдуулж, экологид болон хүний эрүүл мэндэд маш аюултай нөхцөл байдлыг бий болгодог [2]. Тиймээс байгаль орчин, хүн төрөлхтнийг

хамгаалахын тулд хог хаягдлыг дахин боловсруулах шаардлагатай байна.

Хог хаягдлын нийтлэг ангилалд хатуу хог хаягдал, аюултай хог хаягдал, электрон хог хаягдал, био эмнэлгийн хог хаягдал гэсэн төрлүүд багтдаг ба материалыг үндсэн шинж чанар, найрлага дээр тулгуурлан ангилах олон аргууд байдаг. Үүнд:

- Харааны хяналт
- Химийн шинжилгээ зэрэг аргачлалууд багтана.

Хог хаягдлын зохистой менежмент нь хүн төрөлхтөн болон байгаль орчинд эрүүл амьдрал, цэвэр орчин бүрдүүлэх үндсэн нөхцөл бөгөөд үүний нэг чухал алхам бол хог хаягдлыг төрлөөр нь ангилан ялгах явдал юм. Энэ асуудлыг шийдвэрлэхийн тулд хиймэл оюун ухаан, дүрс боловсруулах технологийг ашиглан хог хаягдлыг ангилах, түүнийг дахин боловсруулах боломжтой.

Хог хаягдлыг ангилахад дүрс боловсруулах технологиудыг ашиглах нь бодит цагийн объект илрүүлэлт болон дүрсний онцлогийг ялгах процессыг илүү хялбарчилж өгдөг. Үүнд бага нөөц шаарддаг MobileNetV2, YOLOv11n-cls, MobileNetV2+SVM зэрэг загваруудыг ашиглах боломжтой. YOLOv11n-cls нь бодит цагийн илрүүлэлтэд оновчтой бол MobileNetV2 нь хөнгөн, бага нөөц шаарддаг тул эмбэддэд төхөөрөмжид тохиромжтой. Эдгээр аргууд нь ангилсан хог хаягдлыг дахин боловсруулах үйлдвэрүүдэд түүхий эд болгон нийлүүлэхэд дэмжлэг үзүүлэх боломжтой шийдлүүдийг санал болгодог.

### II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Сүүлийн үеийн судалгаанаас харахад хог хаягдлыг ангилах машин сургалтын загваруудад CNN архитектурууд болон тэдгээрийн хослолуудыг ашиглах нь үр дүнтэй болох нь батлагдаж байна.

Тухайлбал, CNN + SVM хослуулан хог хаягдлыг 4 ангилалд хуваахад 87%-ийн нарийвчлалтайгаар ангилсан судалгаа байдаг [7]. Түүнчлэн, CNN архитектур болох EfficientNet-B0 нь хог хаягдлын ангилалд зориулсан өргөн хүрээтэй өгөгдөл дээр 224×224 хэмжээтэй оролтод 67%-ийн нарийвчлалтай ажиллаж байсныг оролтын хэмжээг 240×240 болгон сайжруулж, EfficientNet-B3 загвар руу шилжүүлснээр 85%-д хүргэж чадсан байна. EfficientNet-B3 загвар нь илүү гүн давхаргатай бөгөөд хог хаягдлыг илүү тодорхой ангилах чадвартайг харуулсан [3]. Мөн өөр өөр CNN архитектуруудаас InceptionV3, InceptionResNetV2, Xception, VGG19, MobileNetv2, ResNet50, DenseNet201 загваруудыг туршиж үзэхэд MobileNetv2 болон ResNet50 нь өндөр нарийвчлалтай байсан бөгөөд MobileNetv2 нь 95.05%-ийн гүйцэтгэлээр хамгийн үр дүнг үзүүлсэн байна [2].

Иймд бид судалгаандаа MobileNetv2, MobileNetv2+SVM хосолсон загваруудыг, түүнчлэн бодит цагийн хэрэглээнд тохиромжтой, хог хаягдлын төрөл ангиллыг хурдан хийхэд тохиромжтой Yolov11n-cls ашиглан өөрсдийн өгөгдөл дээр туршиж, эдгээр загваруудын гүйцэтгэлийг харьцуулан, оновчтой загварыг тодорхойлохыг зорьж байна.

### III. АШИГЛАСАН АРГА

#### I. Өгөгдлийн багц

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

- Gary Thung TrashNet Dataset

TrashNet өгөгдлийн багц нь шил, цаас, картон, хуванцар, металл, хатуу хог хаягдал гэсэн нийтдээ 6 ангиллаас бүрдэх, шошгологдоогүй нийтдээ 2527 зургаас бүрдэх өгөгдлийн багц юм. Харин бид судалгааны ажилдаа манай улсад дахин боловсруулагдах үйлдвэр баригдахаар төсөл нь хэрэгжиж байгаатай холбоотойгоор, нийтлэг ашиглагддаг 4 төрлийн хог хаягдал болох шил, металл, хуванцар, цаас зэрэг зурган өгөгдлийн тоог тэнцвэртэйгээр сонгон нийтдээ 1989 зурган өгөгдлийг ялган авсан. Мөн интернетээс дээрх 4 ангиллаар зургуудыг цуглуулж, өгөгдлөө нэмж өгснөөр нийтдээ 3230 зураг бүхий өгөгдлийн багцыг бэлдсэн. Түүнчлэн энэхүү өгөгдлийн багцын ангилал бүр дэх зургийн шошгололтыг гараар үүсгэж өгсөн.



1-р зураг. TrashNet өгөгдлийн багц

Өгөгдлийн хэмжээ болон олон талт байдлыг нэмэгдүүлэх зорилгоор анхны өгөгдлийн багц дахь зураг бүрээс шинж чанаруудыг өөрчлөн, синтетик өгөгдлүүдийг үүсгэсэн. Ангилал бүр дэх өгөгдлийн хэмжээ синтетик өгөгдлийг үүсгэсний дараа хэрхэн өөрчлөгдсөнийг 1-р хүснэгтэд харуулав. Бид өгөгдлийн багцын хэмжээг ихэсгэх нь загварын гүйцэтгэлд хэрхэн нөлөөлөхийг шалгахын тулд загваруудыг анхны болон нэмэгдүүлсэн өгөгдлийн багцууд дээр тус тусад нь сургасан.

1-Р ХҮСНЭГТ

Ангилал	Анхны өгөгдөл	Синтетик өгөгдөл	Нийт өгөгдөл
Шил	846	2538	3384
Металл	824	2472	3296
Хуванцар	770	2440	3200
Цаас	760	2280	3040
	3230	9730	12920

- Тестийн өгөгдлийн багц

Ангиллын загваруудын гүйцэтгэлийг үнэлэхийн тулд тестийн өгөгдлийн багц үүсгэсэн. 4 төрөл бүхий хогны ангилалд тус бүрд 30 зураг нийтдээ 120 зургийг өөрсдөө бий болгон шошголон бэлтгэсэн.



2-р зураг. Тестийн өгөгдлийн багц

2-Р ХҮСНЭГТ

Ангилал	Үүсгэсэн өгөгдлийн тоо хэмжээ
Шил	30
Металл	30
Хуванцар	30
Цаас	30
Нийт	120

II. Өгөгдлийн урьдчилсан боловсруулалт

Судалгааны ажлыг эхлэхээс өмнө сургалтын болон тестийн өгөгдлөө цэвэрлэх хэрэгтэй. Энэ нь анхны түүхий өгөгдлийг ашиглах боломжтой, тохиромжтой хэлбэрт оруулах үйл явц ба дүрсийн боловсруулалтад шаардлагатай тодорхой зургийн чанарыг сайжруулах боломжийг олгодог.

Үүнд өгөгдлийг дахин хэмжээсжүүлэх (resize) буюу зургийн хэмжээг нэг ижил төрлийн болгож өөрчлөх нь машин сургалтын алгоритмуудыг зөв ажиллуулахад чухал ач холбогдолтой, PyTorch матриц руу ToTensor() ашиглан хөрвүүлэх, дундаж стандарт хазайлтыг ашиглан пикселүүдийг нормалчлах (Normalize), пикселийн эрчимжилтийн утгыг хүссэн мужид (ихэвчлэн 0-ээс 1-ийн хооронд) тохируулдаг. Энэ нь машин сургалтын загваруудын гүйцэтгэлийг сайжруулж чадна.

III. Машин сургалтын алгоритм

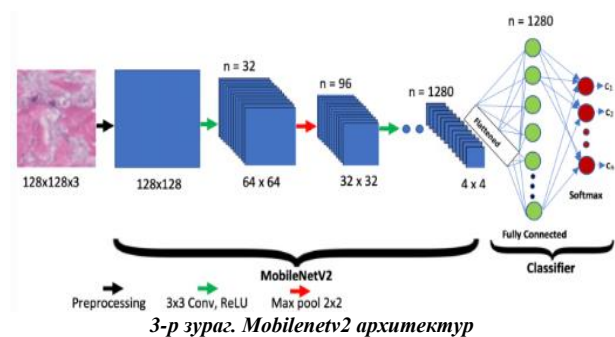
- CNN (Convolutional Neural Networks)

CNN нь конволюцийн давхарга, пүүл (pooling) давхарга, бүрэн холбоост давхарга зэрэг олон давхаргуудаас бүрддэг бөгөөд эдгээр нь хамтдаа ажиллаж загварыг сургах явцад чухал шинж чанаруудыг автоматаар сурах боломжийг олгодог. Хог хаягдлын ангиллын хувьд CNN нь дахин боловсруулах боломжтой материалыг дахин боловсруулах боломжгүй материалаас ялгаж салгахад шаардлагатай гол шинж чанаруудыг автоматаар илрүүлэх боломжтой. Конволюцийн давхаргууд нь зургийн локал хэсгүүд дээр анхаарлаа төвлөрүүлж, ирмэг, текстур зэрэг шинж чанаруудыг илрүүлдэг бол пүүл давхаргууд нь хэмжээсийг бууруулж, хамгийн чухал шинж чанаруудыг онцлон авч үлддэг. Ингэснээр загвар нь нарийвчлал сайтай, үр ашигтай ажилладаг.

- MobileNetV2

MobileNetV2 нь тооцоолох нөөц хязгаарлагдмал байдаг гар утасны болон эмбэдэд програмуудад зориулагдсан үр ашигтай мэдрэлийн сүлжээний архитектур юм. Энэ нь хурд, өндөр нарийвчлалыг хослуулсан тул бодит цагийн объект илрүүлэх,

ангилах ажилд өргөн хэрэглэгддэг. Ихэвчлэн зургийн ангилал, видео дээрх объектыг таних, нүүр царай, дүр зураг илрүүлэх зэрэг програмуудад хязгаарлагдмал хүчээр хурдан боловсруулалт шаарддаг орчинд ашиглагддаг.



1. Depthwise Separable Convolutions нь стандарт конволюцийн үйлдэл бөгөөд оролтын зургийг бүх сувгуудад нэгэн зэрэг хэрэглэдэг конволюцийн шүүлтүүрээр боловсруулдаг. Энэ нь тооцоолох хүчин чадлын хувьд үнэтэй байж болно. Харин MobileNetV2 нь гүний мэдрэмтгий конволюцийг ашигладаг бөгөөд энэ нь үүнийг хоёр үе шатанд задалдаг. Үүнд: Depthwise ба Pointwise конволюци Depthwise конволюци нь оролтын суваг бүрд тусдаа нэг ширхэг шүүлтүүрийг хэрэглэдэг:

$$Y_i = X_i * K_i$$

Энд:

- $X_i$  нь  $i$ -тэй холбоотой оролтын суваг,
- $K_i$  нь гүний мэдрэмтгий конволюцийн цөм буюу шүүлтүүр,
- $Y_i$  нь гүний мэдрэмтгий конволюцийн гаралт юм.

Pointwise конволюци нь гүний мэдрэмтгий конволюцийн гаралтуудыг нэгтгэдэг:

$$Z = \sum_{i=1}^C (Y_i \cdot W_i)$$

Энд:

- $Z$  нь эцсийн гаралт,
- $W_i$  нь pointwise шүүлтүүр,
- $C$  нь оролтын сувгийн тоо юм. Ийнхүү гүний мэдрэмтгий конволюцийг ашигласнаар параметруудийн тоо болон тооцооллын хүчин чадлыг ихээхэн бууруулж чаддаг.

MobileNetV2 нь bottleneck residual блокуудыг ашигладаг бөгөөд эдгээр нь оролтын хэмжээсийг багасгаж, дараа нь convolution үйлдлүүдийг хийдэг.

$$Z = W_{pw,1} \cdot X$$

Энд:

- $W_{pw,1}$  нь хэмжээсийг багасгадаг pointwise convolution юм. Дараа нь convolution үйлдлүүдийг хийсний дараа өгөгдлийг дахин өргөжүүлдэг:

$$Y = W_{pw,2} \cdot f(W_{dwe} \cdot Z)$$

Энд:

- $W_{pw,2}$  нь хэмжээсийг буцаан өргөжүүлдэг pointwise convolution,  $W_{dwe}$  нь depthwise convolution,  $f(\cdot)$  нь ReLU6 идэвхжүүлэгч функц юм. MobilenetV2 сүлжээнд bottleneck residual блокууд нь оролтын хэмжээсийг багасгаж, тооцооллын зардлыг бууруулдаг.

Инвертэд резидуал бүтэц нь bottleneck блокын оролт ба гаралтыг shortcut холболтоор холбодог. Хэрэв оролт ба гаралтын хэмжээс таарч байвал:

$$Y = X + Z$$

Харин хэрэв оролт ба гаралтын хэмжээс таарахгүй бол:

$$Y = Z$$

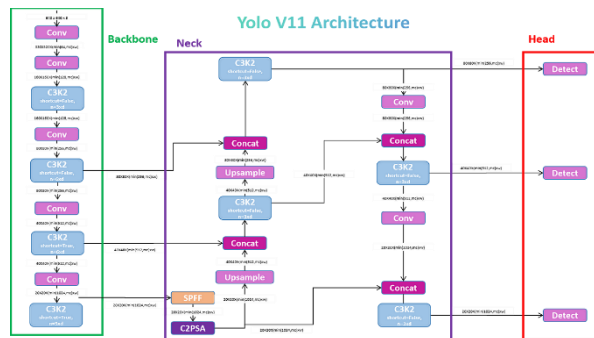
Энэ бүтэц нь анхны оролтын мэдээллийг хадгалж үлдэхэд тусалдаг бөгөөд сургалтын явцад градиентын урсгалыг сайжруулдаг. Ингэснээр сүлжээ илүү гүн болж, илүү нарийн төвөгтэй хамаарлуудыг сурах боломжтой болдог.

- Нарийн тохируулах (Fine-Tuning)

Загварыг ImageNet өгөгдлийн багц дээр урьдчилан сургасан учраас шилжүүлэн сургах замаар сүлжээний эхний 100 давхаргыг эцсийн сургалтад ашигласан. Эхний 100 давхаргыг эцсийн сургалтад оруулснаар загвар нь хог хаягдлын ангилалд зориулсан голлох шинж чанаруудыг олж авахдаа урьдчилан сургасан загвараас өвлөсөн тогтвортой байдлыг хадгалах юм. Энэ нь загварыг хог хаягдлын зургуудын онцлогт тохируулахын зэрэгцээ урьдчилан сургасан загварын найдвартай байдлыг алдахгүй байх боломжийг олгодог. Ийнхүү загвар нь хэлбэр, өнгөний ялгаа зэрэг ангиллаас хамааралгүй онцлогуудыг үр дүнтэй барьж авахын зэрэгцээ хуванцар, мятал, шил зэрэг хаягдлыг ялгахад чухал шинж чанаруудыг олж чадна.

#### IV. Yolov11n-cls

Энэ нь зураг эсвэл видео дээрх объектуудыг бодит цаг хугацаанд илрүүлж, олон объект болон тэдгээрийн байршлыг нэгэн зэрэг тодорхойлох зорилготой, ялангуяа жижиг объектуудыг илүү нарийвчлалтай илрүүлэх боломжийг олгодог. Энэ нь хөдөлгөөнт төхөөрөмжүүдийн хөнгөн загвараас өндөр хүчин чадалтай GPU-д зориулсан том загвар хүртэл уян хатан байдлыг санал болгож, янз бүрийн техник хангамжийн орчинд дасан зохицох боломжтой болгодог.



4-р зураг. Yolov11n-cls архитектур

#### 1. Grid-based Detection:

Оролтын зураг нь  $S \times S$  эсүүдэд хуваадаг. Хүснэгтийн эс бүр хэд хэдэн хязгаарлагдмал хайрцаг болон итгэлцлийн оноог урьдчилан таамагладаг. Хэрвээ биетийн төв нь тодорхой сүлжээний эсэд унавал тэр эс тухайн биетийг илрүүлэх үүрэгтэй.

$$\text{Зургийн хэмжээ} = W \times H$$

Сүлжээний эс бүр дараах зүйлсийг урьдчилан таамагладаг:

$$\text{Bounding box} : (x, y, w, h)$$

Энд:

- $x, y$  : bounding box-ын төвийн координат
- $w, h$  : хязгаарлагдмал хайрцгийн өргөн, өндөр.

Итгэлцлийн оноо  $P_o$  нь bounding box дотор объект агуулагдах магадлалыг илэрхийлдэг бөгөөд үүнийг дараах байдлаар тодорхойлно:

$$P_o = \text{IoU}(\text{pred box}, \text{truth box})$$

Энд:

- IoU: Intersection over Union буюу давхцал ба нийлбэрийн харьцаа юм. Энэ нь таамагласан хайрцаг болон үнэн зөв хайрцгийн хоорондын давхцлыг хэмждэг.

Түүнчлэн, загвар нь тухайн хайрцаг дахь объектын ангиллын магадлалыг мөн тооцоолдог:

$$P(c|o) = \text{softmax}(Wc \cdot f)$$

Энд:

- $P(c|o)$  :объектын ангиллын нөхцөлт магадлал,  $Wc$  нь ангиллын жингүүд,  $f$  нь онцлог вектор юм. Softmax функц нь эдгээр магадлалуудыг нормчилдог.

#### 2. Bounding box Regression:

Yolov11n-cls нь grid cell-ийн харьцангуй координатуудыг таамагладаг:

$$x^{\wedge} = \sigma(t_x) + c_x, y^{\wedge} = \sigma(t_y) + c_y$$

$$x = \sigma(t_x) + c_x, y = \sigma(t_y) + c_y$$

Энд:

- $t_x$  ба  $t_y$ : grid доторх таамагласан шилжилтүүд

- $c_x$  ба  $c_y$  : grid cell-ийн төвийн координатууд
- $\sigma(\cdot)$  : sigmoid функц бөгөөд энэ нь таамагласан координатуудыг 0-1 хооронд хязгаарлана.

Баундинг боксын өргөн болон өндрийг дараах томъёогоор таамаглана:

$$w^{\wedge} = p\_w e^{\wedge}(t\_w), h^{\wedge} = p\_h e^{\wedge}(t\_h)$$

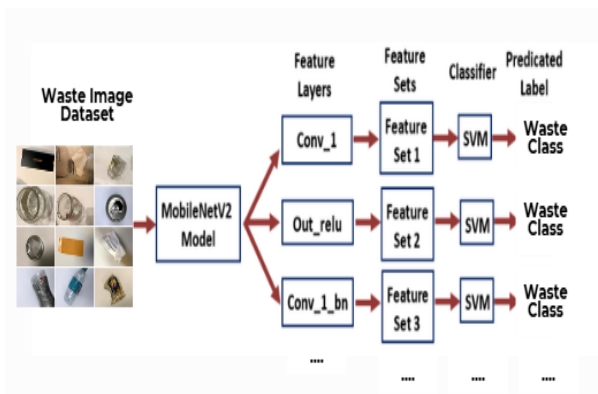
$$w = p\_w * e^{\wedge}(t\_w), h = p\_h * e^{\wedge}(t\_h)$$

Энд:

- $p_w$  ба  $p_h$  : урьдчилан тодорхойлсон анкор боксын хэмжээсүүд
- $t_w$  ба  $t_h$  : таамагласан тохируулгууд

### 3. Mobilenetv2 + SVM

Mobilenetv2 + SVM ангилагчдыг хослуулах нь зураг ангилах ажилд, ялангуяа хөдөлгөөнт болон эмбэдэд систем дээр ажиллахад маш үр дүнтэй арга юм. Энэхүү хослол нь MobileNetV2-ийн зургийн онцлогоос бий болох үр ашгийг, SVM нь зургийн давуу талыг ангилахдаа хэт тохируулгыг багасгаж, ялангуяа хөдөлгөөнт болон эмбэдэд системийн програмуудад үр дүнтэй байдаг.



5-р зураг. MobileNetv2+SVM архитектур

SVM:

SVM Decision Function:

SVM-ийн шийдвэрлэх функц нь хоёр ангиллын хооронд хамгийн их зайтай гипер хавтгайг олоход чиглэгддэг. Шийдвэрлэх функцийг дараах байдлаар тодорхойлно:

$$f(x) = w^T x + b$$

Энд:

- $w$ : жин вектор
- $x$ : шинж чанарын вектор (MobileNetV2-ын гаралтыг хавтгай болгосон)
- $b$ : нэмэгдэл гишүүн

SVM-ийн зорилго нь дараах зорилгот функцийг минимизаци хийх замаар ангилуудын хоорондох зайг максимум болгох явдал юм:

$$\min(1/2 \|w\|^2) y_i(w^T x_i + b) \geq 1$$

Энд:

- $y_i$ :  $i$  дахь дээжийн шошго юм. Хязгаарлалтууд нь бүх дээжүүд зөв ангилагдаж байхаар гипер хавтгайг сонгох ёстойг илэрхийлнэ.

2.Kerne trick:

Хэрэв шинж чанарын зай нь шугаман бус бол Kernel Trick (Optional): ашиглаж болно. Энэ тохиолдолд, нийтлэг хэрэглэгддэг кернел функц бол радиаль суурь функц (RBF) юм. RBF нь шинж чанарын зайг илүү өндөр хэмжээтэд хувиргаж, ангилууд энэхүү өндөр хэмжээт орон зайд шугаман салах боломжтой болдог.

RBF кернел функцийг дараах томъёогоор тодорхойлно:

$$K(x_i, x_j) = \exp(-\gamma \|x_i - x_j\|^2)$$

Энд:

- $x_i, x_j$ : шинж чанарын векторууд
- $\gamma$  : кернелийн параметр (ихэвчлэн сургалтын явцад тохируулагдана)
- $\|\cdot\|$ : Евклидийн норм

Оролт: Хаягдал зургийг (хуванцар, металл, цаас гэх мэт) MobileNetV2 загвар луу оруулна.

Шинж чанар гарган авах: MobileNetV2 нь гүнзгий ялгавартай конволюцийг ашиглан өндөр түвшний шинж чанаруудыг гарган авна.

Тэгшитгэх: Гарган авсан шинж чанарын зургуудыг 1D вектор болгон тэгшитгэнэ. Энэ нь зургийг төлөөлөх болно.

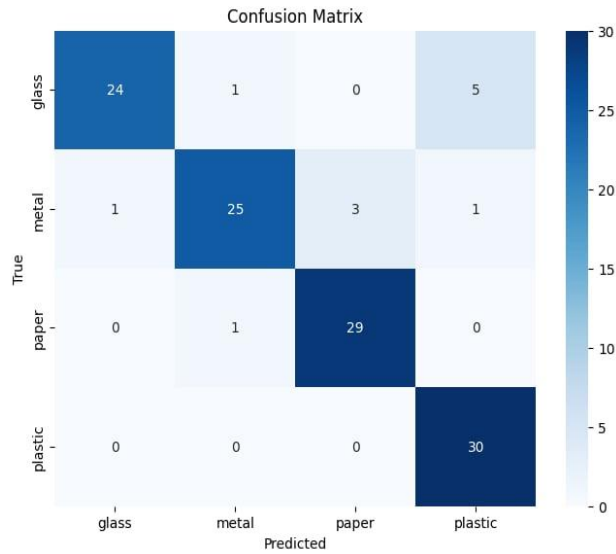
SVM ангилал: Тэгшитгэсэн шинж чанаруудыг SVM руу оруулж, сурсан шийдвэрийн хилээр хаягдлыг ангилна.

## IV.ҮР ДҮН

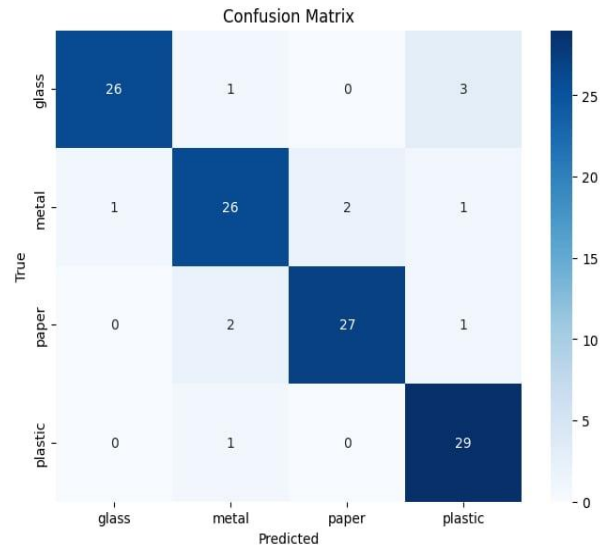
Бид судалгааны ажилдаа MobileNetv2, Yolov1 Incls, MobileNet2 + SVM ангиллын моделиудыг ашиглан өөрсдийн сонгож авсан өгөгдлийн багц дээр туршиж дараах үр дүнг гаргалаа.

### A. MobileNetv2

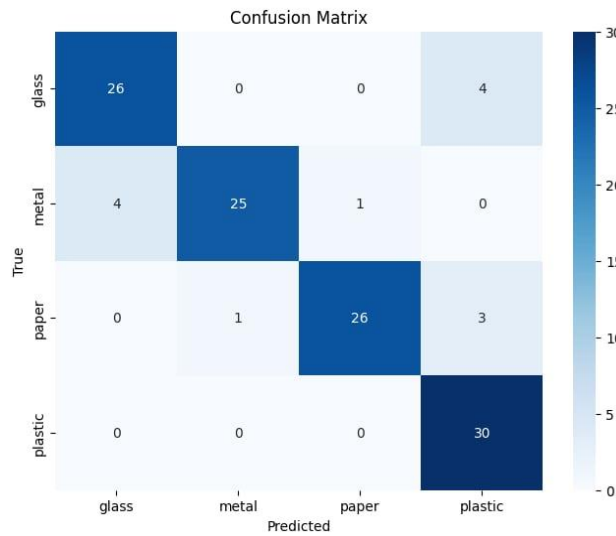
Сургалтын өгөгдлийн хэмжээг нэмэгдүүлэхээс өмнө загварын гүйцэтгэл төстийн өгөгдөл дээр 90% нарийвчлалтай байсан бол өгөгдлийн хэмжээ нэмэгдсэний дараа 89% болж буурсан. Энэхүү бууралт нь өгөгдлийг синтетик өгөгдлөөр өсгөх нь зарим үед анхны нарийвчлалд сөргөөр нөлөөлж болохыг харуулж байна.



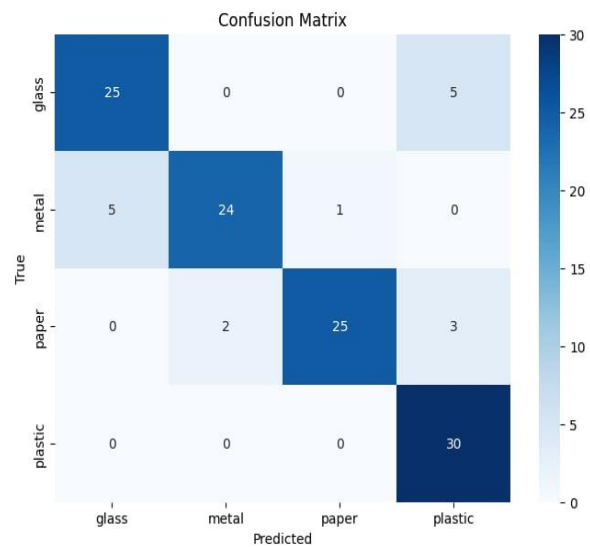
6-р зураг. MobileNetv2 төөрөгдлийн матриц (өгөгдлийн хэмжээг нэмэгдүүлэхийн өмнөх)



8-р зураг. MobileNetv2 + SVM төөрөгдлийн матриц (өгөгдлийн хэмжээг нэмэгдүүлэхийн өмнөх)



7-р зураг. MobileNetv2 төөрөгдлийн матриц (өгөгдлийн хэмжээг нэмэгдүүлсний дараах)



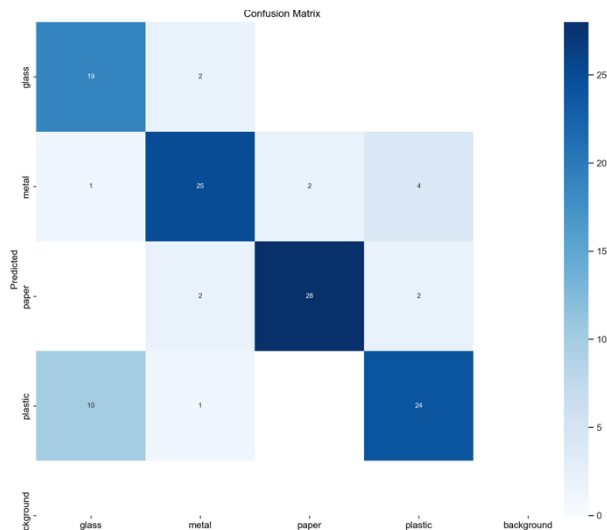
9-р зураг. MobileNetv2 + SVM төөрөгдлийн матриц (өгөгдлийн хэмжээг нэмэгдүүлсний дараах)

**B. MobileNetv2 + SVM**

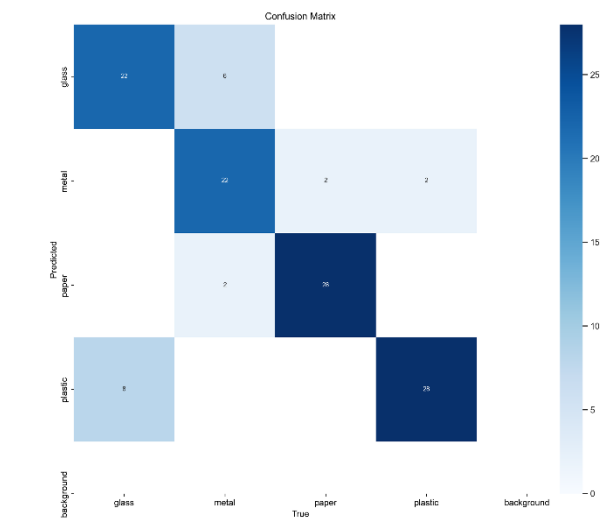
Энэ тохиолдолд бид MobileNetv2 + SVM хослол нь MobileNetv2 загварын гүйцэтгэлтэй ойролцоо дүнг авсан буюу сургалтын өгөгдлийн хэмжээг нэмэгдүүлэхээс өмнө загварын гүйцэтгэл тестийн өгөгдөл дээр 90% нарийвчлалтай байсан ба өгөгдлийн хэмжээ нэмэгдсэний дараа 86% болж буурсан.

**C. YOLOv1n-cls**

Өгөгдлийн хэмжээг нэмэгдүүлэхээс өмнө загварын гүйцэтгэл тестийн өгөгдөл дээр 81% нарийвчлалтай байсан бол өгөгдлийн хэмжээ нэмэгдсэний дараа бага зэрэг сайжирч 83% болсон. Энэхүү загвар нь архитектурын хувьд илүү их өгөгдөлд тохирсон тул өгөгдлийн хэмжээг өсгөх нь гүйцэтгэлд эерэг нөлөө үзүүлсэн байна.



10-р зураг. Yolov11n-cls төөрөгдлийг матриц (өгөгдлийн хэмжээг нэмэгдүүлэхийн өмнөх)



11-р зураг. Yolov11n-cls төөрөгдлийн матриц (өгөгдлийн хэмжээг нэмэгдүүлсний дараах)

D. Ангиллын загваруудын нэгтгэсэн үр дүн

Ангиллын загвар тус бүрийн хувьд өгөгдлийн хэмжээг нэмэгдүүлэхээс өмнө болон нэмэгдүүлсний дараах тестийн өгөгдлийн багц дээрх нарийвчлалын үзүүлэлтийг хүснэгтэд нэгтгэн харууллаа. Үүнд:

MobileNetv2

- M1: Анхны өгөгдөл
- M2: Augmentation хийсний дараах өгөгдөл

MobileNetv2 + SVM

- M3: Анхны өгөгдөл
- M4: Augmentation хийсний дараах өгөгдөл

Yolov11n-cls

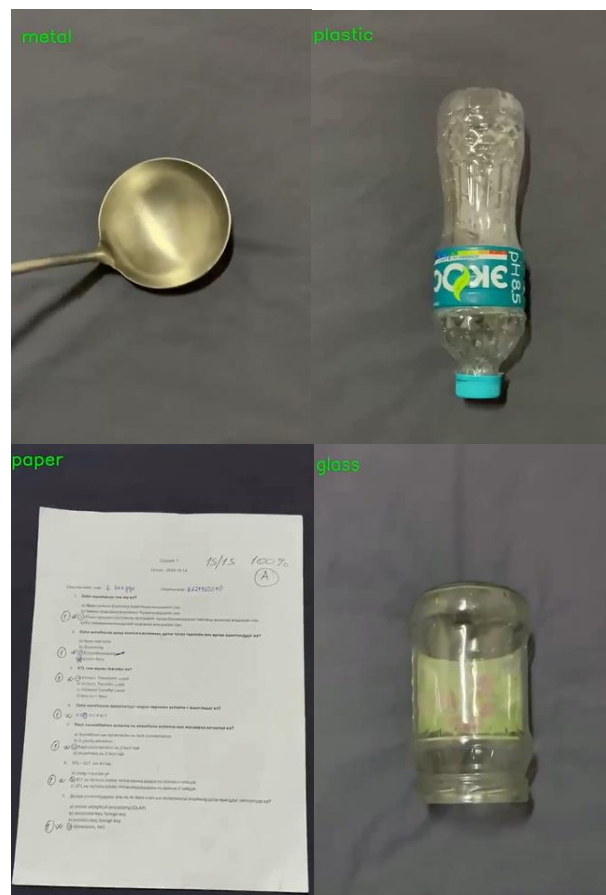
- M5: Анхны өгөгдөл
- M6: Augmentation хийсний дараах өгөгдөл

*3-Р ХҮСНЭГТ*

Моделууд (М)	M1	M2	M3	M4	M5	M6
Тестийн нарийвчлал	90 %	89 %	90 %	86 %	81 %	83 %

E. Бодит цагийн туршилт

Судалгааны ажлын хүрээнд үр дүнг бодит орчинд баталгаажуулах зорилгоор бодит цагийн туршилт гүйцэтгэсэн. Туршилтын явцад 4 төрлийн хог хаягдлыг амжилттай таньж, ангилах боломжтойг баталлаа. Гэсэн хэдий ч зарим тохиолдолд шил болон хуванцар хог хаягдлыг андуурч таних тохиолдол гарсан.



9-р зураг. Бодит цагийн туршилт

V. ДҮГНЭЛТ

Энэхүү судалгааны ажилд хиймэл оюун ухаан болон дүрс боловсруулах технологийг ашиглан хог хаягдлын ангиллын системийг хөгжүүлж, хог

хаягдлыг дахин боловсруулахад дэмжлэг үзүүлэх технологийн шийдэл санал болголоо.

Судалгаанд шил, металл, хуванцар, цаас гэсэн дөрвөн төрлийн хог хаягдлаас бүрдсэн 12,920 зурган өгөгдлийн багцыг ашиглаж, MobileNetV2, MobileNetV2 + SVM, болон Yolov11n-clс гэсэн гурван төрлийн ангиллын загварыг сурган туршив.

**Анхны өгөгдлийн туршилтын үр дүн:** Анхны сургалтын өгөгдөлд MobileNetV2 болон MobileNetV2 + SVM загварууд 90%-ийн нарийвчлалтай ажиллаж, хог хаягдлын ангиллын даалгаварт үр дүнтэй байгааг харууллаа.

**Өгөгдлийн хэмжээг нэмэгдүүлсэн туршилт:** Өгөгдөл өсгөх аргыг хэрэглэсний дараа MobileNetV2 болон MobileNetV2 + SVM загваруудын гүйцэтгэл 89%-с 86% болж бага зэрэг буурсан бол Yolov11n-clс загварын нарийвчлал 80%-с 83% болж сайжрав. Энэ нь Yolov11n-clс загвар нь архитектураасаа хамааран илүү том хэмжээний өгөгдөлд илүү сайн гүйцэтгэл үзүүлэх боломжтойг харуулсан бөгөөд уг загварыг цаашид илүү өргөн цар хүрээтэй өгөгдлийн багц дээр гүнзгийрүүлэн сургаж, сайжруулах боломжтой юм.

Судалгааны дүнгээс харахад, MobileNetV2 загвар нь тооцооллын нөөц бага шаардаж, харьцангуй бага хэмжээний өгөгдлөөр ч үр дүнтэй ажиллах чадвартай нь батлагдлаа. Энэ загвар нь хог хаягдлыг бодит нөхцөлд ангилан дахин боловсруулахад өндөр нарийвчлалтай ажиллах боломжтойг харуулсан бөгөөд 90%-ийн нарийвчлал үзүүлсэн нь энэхүү судалгааны ажлын хүрээнд хамгийн өндөр гүйцэтгэлтэй загвар болж байна.

Бид энэхүү судалгааны ажлаараа өсөн нэмэгдэж буй хог хаягдлын хэмжээг шийдвэрлэх, байгаль орчныг

хамгаалах зорилгоор хог хаягдлыг ангилан дахин боловсруулах ажлыг хялбарчлах шийдлийг санал болголоо. Энэхүү систем нь хог хаягдлын менежментэд тулгамдаж буй асуудлыг шийдвэрлэхэд дэмжлэг үзүүлж, байгаль орчныг хамгаалахад хувь нэмэр оруулах чухал технологийн шийдэл болох боломжтой юм.

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Daniil Filipenco “World waste: statistics by country and brief facts”, 2024.
- [2] Sujan Poudel, Prakash Poudyal “Classification of Waste Materials using CNN Based on Transfer Learning”, 2022.
- [3] Meena Malik, Mueen Uddin “Waste Classification for Sustainable Development Using Image Recognition with Deep Learning Neural Network Models”, 2022.
- [4] Gantulga.D, Munkhchuluun.B, “SOLID WASTE MANAGEMENT IN MONGOLIA”, 2024
- [5] Deep Learning Image Classification with CIFAR-10 Dataset Using CNN (with Transfer learning using MobileNetV2 architecture, pre-trained on the ImageNet dataset, for object detection on CIFAR-10 )
- [6] Andrey Germanov “How to Detect Objects in Images Using the Yolov11n-clс Neural Network”, 2023.
- [7] Olugboja Adedeji, Zenghui Wang, “Intelligent Waste Classification System Using Deep Learning Convolutional Neural Network”, 2019.
- [8] Shidqie Taufiqurrahman, Astri Handayani “Diabetic Retinopathy Classification Using A Hybrid and Efficient MobileNetV2-SVM Mode”, 2020.
- [9] Shivendu Mishra, Ritika Yaduvanshi, “An Integrated Deep-Learning Model for Smart Waste Classification”, 2024.

# МАШИН СУРГАЛТ АШИГЛАН DNS QUERY ӨГӨГДЛӨӨС БОТНЕТИЙГ ИЛРҮҮЛЭХ НЬ

Цогтсарангийн БИЛГҮҮН<sup>1</sup>, Лхагваагийн ОДОНЧИМЭГ<sup>2</sup>

<sup>1,2</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургуулийн

Компьютерийн Сүлжээ Аюулгүй Байдлын Салбар

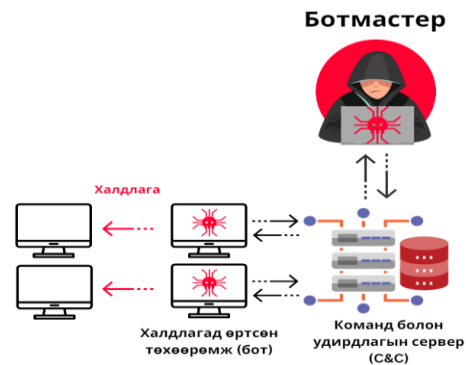
Холбоо барих зохиогчийн э-мэйл хаяг: [odno@must.edu.mn](mailto:odno@must.edu.mn)\*

Хураангуй: Сүүлийн жилүүдэд ботнетууд нь МАБ-ын нэгэн том аюул болж, түүнийг илрүүлэх нь нарийн төвөгтэй болсоор байна. Ботнетууд нь кибер гэмт хэрэгтнүүдэд кибер халдлага хийхэд зориулсан хүчирхэг хэрэгсэл болж (DDoS), фишинг, мэдээлэл хулгайлах зэрэг халдлагуудад ашиглагдаж байна. Иймээс ботнетийн асуудалд Domain Name System (DNS)-д суурилсан илрүүлэх аргачлалуудыг нэвтрүүлэх нь судалгааны чухал чиглэл болж байна. Учир нь DNS нь домэйн нэрийг IP хаягаар хөрвүүлж, сүлжээний урсгалыг тасралтгүй зохицуулахад чухал үүрэг гүйцэтгэдэг. Ботнетууд энэхүү системийг ашиглан өөрсдийн ажиллагааг нуух, динамик DNS (DDNS), домэйн үүсгэх алгоритмууд (DGA), мөн fast-flux зэрэг техникийг ашиглан домэйн мэдээллийг тасралтгүй өөрчлөх замаар өөрсдийн мөрийг далдалдаг байна. Энэхүү судалгаа нь DNS-ын ажиллагаа, түүнийг ашигласан ботнетийг илрүүлэх арга барилуудыг гүнзгий судалж, халдлагаас хамгаалах, машин сургалт ашиглан DNS query өгөгдлөөс ботнетийг илрүүлэх болон холбоотой кибер аюул заналыг эрт шатанд олж илрүүлэх боломжийг нэмэгдүүлж байгаа юм. Энэ нь кибер хамгаалалтын салбарт шинэ шийдэл болж байгаа бөгөөд үүний тусламжтайгаар кибер гэмт хэрэгтнүүдийн халдлагаас урьдчилан сэргийлэх боломжийг нэмэгдүүлнэ. Бид судалгааны хүрээнд Random Forest машин сургалтын аргыг ашиглан ботнетийг илрүүлсэн нь нарийвчлал 97%-иас дээш байж, уламжлалт аргуудаас илүү сайн үзүүлэлттэй гарсан. Гэвч зарим ботнетууд нь хууль ёсны домэйн нэртэй төстэй бүтэцтэй байсан нь илрүүлэх түвшинд сөргөөр нөлөөлж байсан. Энэ судалгааны ажлаар DGA-ийг ашиглан үүсгэсэн домэйннуудыг илүү сайн танихын тулд гийгүүлэгч болон эгшгийн харьцааг илэрхийлэх шинэ Гийгүүлэгч-Эгшгийн Харьцаа (CVR) гэсэн үзүүлэлтийг 25 дахь шинж чанар болгон нэмж ашигласан. Уг үзүүлэлт нь DGA-аар үүсгэгдсэн домэйн нэрүүдийн хувьд түгээмэл ажиглагдадаг фонетик болон бүтцийн онцлоггүй байдлыг илэрхийлдэг хэл зүйн үзүүлэлт юм. Судалгаагаар хууль ёсны домэйн нэрүүдийг уншигдахуйц байлгах үүднээс гийгүүлэгч-эгшгийн зохицолтой байдлыг хадгалдаг бол DGA-аар үүсгэсэн домэйн нэрүүд нь таних загвараас зайлсхийж, хар жагсаалтад орохоос хамгаалах зорилгоор ихэвчлэн гийгүүлэгчийг хэт их агуулсан бүтэцтэй байдаг болохыг тогтоосон үр дүнгээ танилцуулж байна.

Түлхүүр үг: Ботнет, машин сургалт, DNS, Random Forest, CVR.

## I. ОРШИЛ

Хувь хүн болон байгууллагыг чиглэсэн кибер халдлагууд нь интернэтийн дэд бүтэц болон хэрэглэгчдэд ихээхэн аюул учруулж байгаа бөгөөд дэлхий даяар янз бүрийн халдлага ажиглагдаж байна. Кибер халдлага хурдтай хувьсан өөрчлөгдөж байгаа нь ботнетуудийг кибер гэмт хэрэгтнүүдийн хамгийн аюултай зэвсэг болгож байна. Ботнет нь алсаас удирдагддаг, халдлагад өртсөн төхөөрөмжүүдийн сүлжээ бөгөөд "ботмастер" гэж нэрлэгдэх этгээдийн хяналтад ажиллаж, өргөн цар хүрээтэй халдлагууд, тухайлбал DDoS, фишинг, спам тараалт, мэдээлэл хулгайлах зэрэг халдлагуудыг зохион байгуулах боломжийг олгодог (1-р зураг)[1]. Эдгээр хортой сүлжээнүүд нь ихэвчлэн төвлөрсөн команд болон удирдлагын (C&C) дэд бүтцийг ашигладаг бөгөөд ингэснээр ботмастер нь сая сая халдвар авсан төхөөрөмжүүдийг хооронд нь уялдуулан ажиллуулах боломжтой болдог. Ботнетийг илрүүлэх нь тэдний тархсан шинж чанар, дасан зохицох чадвартай техникийг ашигладаг тул уламжлалт сүлжээний аюулгүй байдлын арга хэмжээг тойрон гарах нөхцөлийг бүрдүүлдэг. Иймээс ботнетийн удирдлага, холбоог нууцлахад ашиглагддаг Domain Name System (DNS)-д суурилсан ботнет илрүүлэх судалгаа маш чухал чиглэл болоод байна [1][2][3].



1-р зураг. Ботнетийн зарчим.

DNS нь дэлхий даяар тархсан систем бөгөөд домэйн нэрийг IP хаягаар хөрвүүлж, сүлжээний урсгалыг тасралтгүй зохицуулахад чухал үүрэг гүйцэтгэдэг. Ботнетууд энэхүү системийг ашиглан өөрсдийн ажиллагааг нуух, тогтвортой байлгах зорилгоор динамик DNS (DDNS), домэйн үүсгэх алгоритмууд (DGA), мөн fast-flux зэрэг техникийг ашиглан домэйн мэдээллийг тасралтгүй өөрчлөх замаар хар жагсаалтаас зайлсхийдэг [1][2]. Эдгээр арга нь ботмастеруудыг хортой домэинтэй холбоотой IP хаягийг тогтмол өөрчилж, тодорхой домэйн эсвэл IP хаяг илрүүлэгдсэн ч халдвар авсан төхөөрөмжүүдтэй харилцааг тасралтгүй хадгалах

боломжтой болгож байна. DGA төрлийн ботнет нь баримт бичигт харуулсан алгоритмыг ашиглан олон домэйн нэр үүсгэж, заримыг нь DNS серверт бүртгүүлж, C&C серверийн домэйн нэр болгон ашигладаг. Ботууд ч мөн адил алгоритмыг ашиглан домэйн нэрийг дараалан үүсгэж, тэдгээрийг DNS серверээс лавладаг. Лавласан домэйн нэр нь C&C серверийн домэйн нэртэй таарч, зөв нэр шийдвэрлэлт хийгдвэл C&C серверийн IP хаяг буцаж ирдэг тул тэр IP хаяг руу пакет илгээж, C&C сервертэй харилцдаг. DGA нь одоогийн цагт эсвэл интернэтэд хэрэглэгдэж буй үг зэрэг санамсаргүй утгыг оролтын утга болгон ашигладаг тул гүйцэтгэл бүрт үүсгэгдэх домэйн нэрүүд нь өөр өөр байдаг. C&C серверийн домэйн нэрийг байнга шинэчилж байдаг тул хар жагсаалтаар илрүүлэхээс зайлсхийж чаддаг. DGA төрлийн ботнетийн жишээнд Zeus, Conficker, Kraken, Gozi, Torpig, Bedep зэрэг багтана (2-р зураг).

<b>ZEUS</b> ..... vtyhb.com  iuwbc.xyz	<b>GOZI</b> ..... bankupdate-secure.com  onlineaccount-verification.net	<b>KRAKEN</b> ..... abcdfghjkl123.com  mnrqsuvyz.xyz
----------------------------------------------------	-------------------------------------------------------------------------------------	------------------------------------------------------------------

2-р зураг. DGA ботнетийн домэйн нэрсийн жишээ.

DNS-д суурилсан ботнет илрүүлэх ажил нь хууль ёсны DNS хүсэлтүүдээс хортой DNS урсгалыг ялгахад төвөгтэй байдаг. Интернэт сүлжээнүүдээс үүссэн DNS хүсэлтүүдийн асар их хэмжээ нь ботнетийн урсгалын нарийн бөгөөд далд хэв маягуудыг тодорхойлоход хүндрэл учруулдаг. Гарын үсэгт суурилсан болон босгод суурилсан уламжлалт илрүүлэх аргууд нь хурдтай хувьсан өөрчлөгдөж буй ботнетийн арга техникийг илрүүлэхэд дутмаг хэвээр байна. Иймээс сүүлийн үеийн судалгаанууд их хэмжээний DNS өгөгдлийг шинжлэх, хортой үйл ажиллагааг илтгэх хэв маягийг илрүүлэхийн тулд машин сургалт, гүн сургалт зэрэг дэвшилтэт аргуудыг ашиглахад анхаарлаа хандуулж байна. Эдгээр аргууд нь DNS урсгалын давтамж, домэйн нэрний нас, хүсэлтийн давтамж зэрэг шинж чанаруудыг ашиглан ботнетийн зан үйлийг таньж илрүүлэх замаар илүү нарийвчилсан ботнет илрүүлэх боломжийг олгодог [2][3]. Гэсэн хэдий ч, эдгээр илрүүлэлтээс зайлсхийхийн тулд халдлагын чиг хандлага болон аргууд өдөр бүр өөрчлөгдөж байгаа бөгөөд Zero-day attack зэрэг хэв маягийн тохирлыг илрүүлэхээс зайлсхийх жишээнүүд олон тохиолдож байна.

DNS-д суурилсан ботнет илрүүлэх аргууд сайжирч байгаа хэдий ч зарим асуудлууд хэвээр байна. Жишээлбэл, дүрэмд суурилсан аргууд нь гажууд хэв маягтай хууль ёсны урсгалтай тулгарах үед их хэмжээний хуурамч-эерэг илэрцтэй байх хандлагатай байдаг бол загварт суурилсан аргууд нь бодит цагийн ажиллагаанд их хэмжээний, зөв тэмдэглэгээтэй өгөгдөл, өндөр тооцооллын нөөц шаарддаг. Олон төрлийн илрүүлэх стратегийг хослуулсан холимог аргууд нь янз бүрийн халдлагыг

хамрах чадвар сайтай тул илүүд үзэгдэх болсон [3]. Гэсэн хэдий ч ботнетийн хувьсан өөрчлөгдөх чадвар нь илүү боловсронгуй, тогтвортой, өндөр нарийвчлалтай, бага хугацаанд илрүүлэх чадвартай DNS-д суурилсан илрүүлэх техникийг шаардсаар байна.



3-р зураг. DNS query болон домэйн нэр.

Бидний судалгаа нь DNS query-д (3-р зураг) суурилсан ботнет илрүүлэх аргуудыг судалж, машин сургалтаар сайжруулсан загваруудын илрүүлэх нарийвчлал, тогтвортой байдлыг хэрхэн сайжруулах боломжтойг судлах замаар энэ чиглэлд хувь нэмэр оруулах зорилготой юм.

## II. БОТНЕТИЙН ТАНИЛЦУУЛГА

Ботнетийн тархалт хурдтай өсөх нь кибер аюулгүй байдалд томоохон сорилтуудыг бий болгож, ботнет илрүүлэх судалгааны ажлуудыг урагшлуулж байна. Энэ хэсэгт ботнетийн талаар дэлгэрэнгүй мэдээлэл өгөх бөгөөд тэдний амьдралын мөчлөг, DNS-д суурилсан машин сургалтын илрүүлэх аргуудын ач холбогдлыг тодорхойлоход чиглэгдсэн болно.

### I. Ботнетийн мөчлөг

Ботнетийн мөчлөг нь халдлагад өртсөн төхөөрөмжүүдийг элсүүлэх, удирдах, дайралтанд ашиглахад чиглэсэн тодорхой үе шатуудтай (4-р зураг) байдаг. Эдгээр үе шатуудыг ойлгох нь DNS дээр суурилсан машин сургалтыг ашиглан ботнетийн үйл ажиллагааг илрүүлэхэд чухал үүрэгтэй. Ботнетийн амьдралын мөчлөг нь дараах үндсэн үе шатуудтай [1][4][5]:

#### I. Ашиглах үе шат

Ботнетийн амьдралын мөчлөг нь интернэтэд холбогдсон төхөөрөмжүүдийн эмзэг байдлыг илрүүлэхээс эхэлдэг. Энэ эмзэг байдлыг фишингийн халдлага, хортой программ татаж авах, эсвэл сул хамгаалалт бүхий системүүдийг ашиглах замаар программ суулгаж, төхөөрөмжийг ботнетийн сүлжээнд холбодог [2][6].

#### II. Уриалах үе шат буюу команд болон удирдлагын сүлжээ (C&C) бий болгох

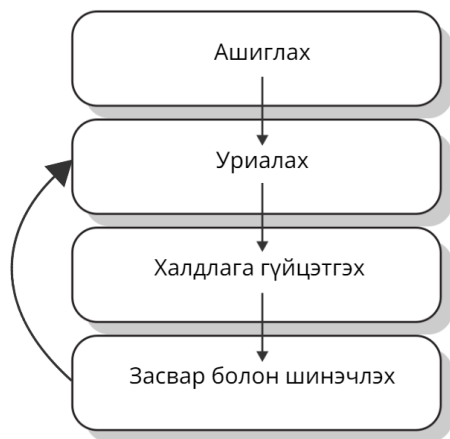
Төхөөрөмжүүд халдвар авсны дараа ботнетийн C&C системд холбогддог. C&C сүлжээ нь ботнетийн ажиллагааг хянан удирдах чухал суурь юм. Хуучин цагийн ботнетүүд төвлөрсөн C&C серверүүдэд найдаж байсан бол орчин үеийн ботнетүүд төвлөрсөн бус архитектур (жишээ нь, DNS дээр суурилсан харилцаа холбоо) ашиглан илрэх эрсдэлээс зайлсхийдэг [7]. Төвлөрсөн бус C&C загвар нь ганц цэгийн алдаанаас сэргийлж, ботнетийн ажиллагааг тасалдуулахад илүү хэцүү болгодог [3].

#### III. Халдлага гүйцэтгэх үе шат

Ботнет нь ажиллагаанд орох үедээ DDoS халдлага, мэдээлэл хулгайлах, спам тараах, болон "click fraud" зэрэг төрөл бүрийн хортой үйл ажиллагааг явуулдаг. Жишээ нь, Mirai зэрэг өндөр түвшний ботнетүүд нь IoT төхөөрөмжүүдийн сул хамгаалалтыг ашиглан асар их DDoS халдлагыг зохион байгуулж байна [9][10]. Зарим ботнетүүд банк санхүүгийн байгууллагуудыг чиглүүлэн халдлага үйлддэг ба зарим нь спам эмэйл тарааж, цаашид халдвар тараахад хувь нэмэр оруулдаг [2][5].

**IV. Шинэчлэл болон засварын үе шат**

Ботнетийн амьдралын мөчлөгийн сүүлийн үе шат нь ботуудыг шинэчлэх, арчлах явдал юм. Ботмастер нь ботуудын хэрэгжилтын байдлыг сайжруулах, цэгцлэх зорилгоор ботуудыг үе үе шинэчлэх шаардлагатай. Хуулийн байгууллага, аюулгүй байдлын судлаачид ботнетүүдийг илрүүлж устгах үед ботмастерууд хаягдсан төхөөрөмжүүдийг орхих эсвэл ботнетүүдийг илрэхгүй байх зорилгоор түр зогсоож, аюулгүй нөхцөл бүрдсэний дараа дахин ажиллагаанд оруулдаг. Зарим ботнетүүд нь устгах арга хэмжээ эсвэл өрсөлдөгч ботнет илрэх үед автоматаар устгах боломжтой байдаг [11]. Ингээд шинэчлэлтийн үе шат дууссаны дараа ботнет нь уриалах үе шат руу шилжиж, ботууд C&C сервертэй дахин холбогдон шинэ зааварчилгаа авч, сүлжээний бэлэн байдлаа шалгадаг. Ийнхүү тасралтгүй үргэлжлэх энэ цикл нь ботнетийг дасан зохицох чадвартай болгож хамгаалалтын арга хэмжээнээс зайлсхийхэд хялбар болгодог.



4-р зураг. Ботнетийн мөчлөг ба давтамж.

**III. БОТНЕТИЙН ТӨРӨЛ БА DNS ДЭЭР СУУРИЛСАН ИЛРҮҮЛГИЙН АРГУУД**

Ботнетууд нь мэдээлэл хулгайлах, спам тараах, DDoS халдлага хийх зэрэг хортой зорилгоор ашиглагддаг бөгөөд тэдгээрийн бүтэц болон холбооны загвараас хамааран ангилагддаг. Үндсэн төрлүүдийг дараах байдлаар авч үзье.

**I. Төвлөрсөн ботнет:**

Төвлөрсөн ботнет нь ганц C&C серверийг ашиглан ботуудыг удирддаг. Ихэвчлэн HTTP болон IRC протоколуудыг харилцаанд ашигладаг бөгөөд команд дамжуулахад энгийн, үр дүнтэй байдаг. Гэхдээ энэ загвар нь нэг цэгийн доголдолд өртөмтгий байдаг тул

C&C серверийг хааснаар ботнетийг саармагжуулах боломжтой болдог [1].

**2. Peer-to-Peer (P2P) ботнет:**

P2P ботнет нь төвлөрсөн C&C серверээс хамааралгүй ажилладаг. Bot бүр хоорондоо харилцан холбогдож, сүлжээний төвлөрлийг сааруулж өгдөг. Энэ нь ботнетийг задлахад хэцүү болгож, бүрэлдэхүүн хэсгүүдийг устгасан ч ботнетийн ажиллах чадварыг хадгалах боломжтой болгодог. Гэсэн хэдий ч P2P ботнет нь илүү удаан, команд түгээхэд төвөгтэй байдаг [3][2].

P2P ботнетийн нэг жишээ бол GameOver Zeus юм. Zeus нь халдлагын маш нарийн төвөгтэй хувилбар бөгөөд 2011 онд гарч ирж, 2014 он хүртэл идэвхтэй байсан. Эхний Zeus-с ялгаатай нь GameOver Zeus нь C&C дэд бүтцийн хувьд P2P загварыг ашиглаж байсан бөгөөд энэ нь цаашдын устгалд илүү тэсвэртэй, хууль сахиулагчдын ажиллагааг таслан зогсооход амархан болгосон. Эх загварынхаа адил GameOver Zeus нь голчлон банкны хулгай, болон хувийн мэдээлэл хулгайлах зорилготой байсан бөгөөд нэвтрэх мэдээлэл, кредит картын мэдээлэл, болон бусад мэдээллийг хулгайлахад зориулагдсан. 2014 оны 6 сард Холбооны Мөрдөх Товчоо (FBI), EuroPol болон бусад хууль сахиулах байгууллагуудын хамтарсан Operation Tovar ажиллагаа нь GameOver Zeus ботнетийг амжилттай устгасан. Энэ ажиллагаа нь P2P сүлжээнд байрлах гол зангилаануудыг зорилгот байдлаар устгаж, ботнетийг түр хугацаагаар саатуулсан бөгөөд түүний зохиогч болон ботмастеруудыг мөрдөн шалгах үйл ажиллагаа явуулсан.

**3. Холимог ботнет:**

Холимог ботнет нь төвлөрсөн ба P2P ботнетийн давуу талыг хослуулдаг. Тэд гол C&C серверийг команд түгээхэд ашигладаг ч P2P зангилааг тогтвортой байдлыг сайжруулахад нэмэлт давхарга болгон хэрэглэдэг. Энэ төрлийн загвар нь ботнет илрүүлэх болон саармагжуулахад илүү хэцүү болгож өгдөг [4][8].

**I. DNS дээр суурилсан ботнет илрүүлгийн аргууд**

DNS нь ихэвчлэн ботнетуудын команд дамжуулах сувгаар ашиглагддаг. DNS дээр суурилсан ботнет илрүүлгийн аргууд нь DNS урсгалыг шинжлэн сэжигтэй хандлагыг илрүүлэх зорилготой бөгөөд эдгээрийг дараах байдлаар ангилдаг:

**I. Урсгалын шинжилгээ (Flow-Based Analysis):**

Энэ арга нь DNS урсгалын хэв маягийг ажиглаж, ботнеттай холбоотой хачирхалтай давтамж эсвэл Time to Live (TTL) утгуудыг илрүүлдэг. DNS урсгалын өгөгдлийг шинжилснээр зохиомол DGA ашигладаг ботнетуудыг илрүүлэх боломжтой [1]. Урсгалын шинжилгээний арга нь бодит цагт ботнет илрүүлэлтэд тохиромжтой ч их хэмжээний өгөгдлийг боловруулах чадвар шаарддаг [5].

**II. Гарын үсгийн шинжилгээ (Signature-Based Detection):**

Энэ арга нь DNS хүсэлтийн гарын үсэг эсвэл хорлонтой домэйнүүдийг харьцуулан илрүүлдэг. Гарын үсгийн шинжилгээ нь тодорхой ботнетийг тодорхойлохдоо үр дүнтэй ч шинэ эсвэл дөнгөж үүссэн ботнетийг илрүүлэхэд сул талтай байдаг [7].

### III. Аномали буюу гэжүүдал дээр суурилсан илрүүлэлт (Anomaly-Based Detection):

Аномали дээр суурилсан илрүүлэлтийн аргууд нь DNS хүсэлтийн хэвийн бус зан төлвийг ажиглан илрүүлдэг. Жишээлбэл, DNS хүсэлтийн давтамж огцом өсөх, ер бусын бүтэцтэй домэйнуудыг олох зэрэгт үр дүнтэй байдаг. Энэ арга нь шинээр үүссэн эсвэл мэдэгдээгүй ботнетийг илрүүлэхэд сайн ч их хэмжээний худал дохио гаргаж болох тул оновчтой тохируулалт шаардлагатай байдаг [6].

### IV. Машин сургалт дээр суурилсан илрүүлэлт (Machine Learning-Based Detection):

Машин сургалтын аргууд нь ботнеттэй холбоотой шинж чанаруудыг ашиглан DNS урсгалыг ангилах боломжийг олгодог. Жишээ нь, домэйн нэрийн энтропи, хүсэлтийн давтамж, хариу өгөх хугацаа зэрэг үзүүлэлтүүдийг ашиглан ботнетийн урсгалыг тодорхойлдог. Машин сургалтын аргууд нь ботнетуудын хувьсамтгай шинж чанарт дасан зохицох чадвартай [9][10].

### V. Холимог илрүүлэлт (Hybrid Detection):

Холимог илрүүлэлтийн арга нь олон илрүүлэлтийн аргыг хослуулан ботнет илрүүлэлтийн нарийвчлалыг сайжруулах зорилготой. Энэ арга нь мэдэгдэж буй ботнетүүдийг хурдан илрүүлэхээс гадна аномали болон зан төлвийн шинжилгээгээр шинэ ботнет урсгалыг илрүүлэх боломжийг олгодог [8].

## IV. СУДЛАГДСАН БАЙДЛЫН ТОЙМ

Орчин үеийн сүлжээнүүдийн DNS урсгалын хэмжээ асар их бөгөөд үүнийг хурдан хугацаанд боловсруулах систем шаардлагатай. Ялангуяа гүн сургалтын загварууд нь их хэмжээний DNS хүсэлтийг бодит цагт өндөр үр ашигтайгаар шинжилж, томоохон сүлжээн дэх ботнетийг илрүүлэх боломжийг олгодог [4]. Жишээлбэл, Jiang болон Zhou нарын DNS аномали илрүүлэх судалгаагаар, гүнзгий нейрон сүлжээ (DNN) нь сая сая DNS хүсэлтүүдийг боловсруулж 95%-иас дээш нарийвчлалтайгаар ботнетийн хэв маягийг илрүүлж, бусад илрүүлэлтийн аргуудыг давсан байна [9].

Jiang болон Zhou (2018) судалгаанд дурдсанаар шийдвэрийн мод нь DNS өгөгдөл дээр 90%-иас дээш нарийвчлалтайгаар DGA домэйныг ангилах чадвартай байв [9].

Lee болон Park-ийн судалгаагаар RNN нь гүнзгий сургалтыг ашиглаагүй аргуудтай харьцуулахад 15%-иар илүү сайн илрүүлэлтийн түвшинтэй болохыг харуулсан[4]. Хуурамч эерэг илрүүлэлт ба илрүүлэлтийн нарийвчлал нь сүлжээний орчинд чухал байдаг бөгөөд ML-д суурилсан аргууд эдгээрийг давуу тал болгодог. Нарийвчлалтай илрүүлэлтийн системүүд нь сүлжээний үйл ажиллагааг тасалдуулахгүйгээр найдвартай илрүүлэлтийг баталгаажуулдаг. Kolini болон Martin нарын судалгаагаар SVM загвар нь 92%-ийн

нарийвчлалтай байсан бөгөөд энэ нь байгууллагын сүлжээнд найдвартай байдлыг хангахад чухал ач холбогдолтой юм [6].

Баглаа үүсгэх аргуудыг ашиглан хяналтгүй нөхцөлд ботнет илрүүлэхэд 87%-ийн нарийвчлалтай болохыг Wang болон хамтран ажиллагчид харуулсан байна [2][10]. Zeng et al. (2020) хосолмол загварууд нь өндөр хэмжээний DNS асуулгатай орчинд хуурамч илрүүлэлтийг бууруулан, 92%-ийн нарийвчлал үзүүлсэн байна [10].

Xuan Dau Hoang болон Xuan Hanh Vu нарын судалгаа нь DGA ашигладаг ботнетийг илрүүлэхийн тулд Random Forest алгоритм ашиглан DNS лавлагааг хууль ёсны болон хортой гэж ангилах дэвшилтэт машин сургалтын загварыг танилцуулсан. Энэхүү загвар нь илрүүлэлтийн үр дүнг сайжруулж, өмнөх илрүүлэлтийн системд байсан хуурамч эерэг (FPR) болон хуурамч сөрөг (FNR) үзүүлэлтийг бууруулахад чиглэгдсэн[11].

## V. БОТНЕТИЙГ МАШИН СУРГАЛТААР ИЛРҮҮЛЭХ НЬ

Машин сургалт (ML)-д суурилсан илрүүлэлт нь DNS урсгал дахь хэв маягийг суралцдаг алгоритмуудыг ашигласнаар ботнет илрүүлэх хамгийн найдвартай аргуудын нэг юм. ML-д суурилсан илрүүлэлт нь өөрчлөлтөд дасан зохицох чадвар, нарийвчлал, өндөр түвшний өгөгдөлтэй ажиллах чадвараараа бусад аргаас давуу талтай. Өөр өөр төрлийн өгөгдөл болон загваруудыг боловсронгуй болгох боломжтойгоороо ML-д суурилсан аргууд нь ботнетийн заналхийллийг үр дүнтэйгээр илрүүлэх боломжийг олгодог. Жишээ нь, алдартай Conficker ботнет өдөрт 50,000 домэйн нэр үүсгэх боломжтой байсан нь эдгээрийг шууд илрүүлэх боломжгүй болгож байсан [6]. Үүнээс болж ML техникуудыг ашиглан эдгээр нарийн зүй тогтлыг таньж, илрүүлэх шаардлага урган гарсан.

### 1. Машин сургалтыг ашиглах давуу талууд

Хэв маяг дээр суурилсан илрүүлэлт нь мэдэгдэж буй хэв маягт тулгуурладаг бөгөөд шинэ ботнетүүдийг илрүүлэхэд хангалтгүй байдаг. Харин ML алгоритмууд нь урьдчилан тодорхойлсон хэв маяг биш, харин зан үйлийн үндсэн дээр ботнетийн урсгалыг илрүүлдэг. DNS хүсэлтийн давтамж, домэйн нэрийн энтропи, ер бусын асуултын хэв маягийг шинжилж ML загварууд DGA ашиглан байнга өөрчлөгддөг ботнетүүдийг илрүүлэх боломжтой байдаг [1][2].

Идеал хувилбарт бол халдлагын улмаас аюулгүй байдлын асуудал үүсэхээс урьдчилан сэргийлэхийн тулд сүлжээний тал дээр халдлагыг илрүүлэх, хамгаалах нь хамгийн ашигтай байдаг. Сүлжээнд халдлагыг илрүүлж, хамгаалж чадвал хортой пакетууд халдлагын зорилтот хостод хүрэхээс өмнө үр дүнтэйгээр хааж, хортой пакетууд дотоод болон гадаад сүлжээнд тархахаас сэргийлж чадна. Гэсэн хэдий ч, сүлжээний тал дээр халдлага илрүүлэх нь бүх пакетуудыг сүлжээнд ирмэгц аюулгүй байдлын төхөөрөмжөөр шууд бодит цагт шалгах шаардлагатай болдог. Одоогийн аюулгүй байдлын төхөөрөмжүүд,

жишээ нь дараагийн үеийн галт хана болон халдлага илрүүлэх систем (IDS) нь гарын үсэг ашиглан хамгийн ихдээ 100 Giga bit per second (Gbps) хурдтай сүлжээний урсгалыг шалгаж чаддаг. Нөгөө талаас, энэ хурдтайгаар пакетыг шалгахад зөвшөөрөгдөх нэг пакетын боловсруулах хугацаа маш бага байдаг. Тодруулбал, 10 Gbps хурдыг хүргэхийн тулд 64 byte пакетыг хүлээн авахаас илгээх хүртэл нийт 50 наносекунд дотор боловсруулах шаардлагатай байдаг.

ML-ийн гол давуу тал нь асар их хэмжээний сургалтын өгөгдөл дээр үндэслэн илрүүлэлтийн шалгуурыг нарийвчлан боловсруулж хуурамч эерэг илрүүлэлтийг бууруулах чадвар юм. Supervised learning буюу хяналттай сургалтаар домэйн хүсэлтүүдийг ангилах замаар хор хөнөөлтэй хүсэлтүүдийг оновчтойгоор ялгах боломжтой.

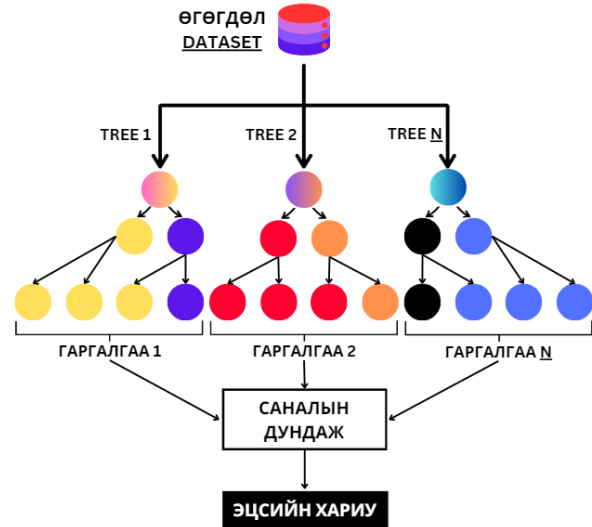
**2. DGA ботнетийг илрүүлэх машин сургалтын аргууд**

DGA илрүүлэх машин сургалтын арга нь DNS асуулгын шинж чанаруудад дүн шинжилгээ хийх замаар илүү үр дүнтэй болсон. Янз бүрийн машин сургалтын аргууд нь домэйны бүтцээс авахуулаад асуулгын зан төлөв, сүлжээний шинж чанараар ангилан ялгах замаар DGA-ийг илрүүлэх нарийвчлалыг сайжруулдаг.

**I. Хяналттай сургалтын загварууд:**

**a. Шийдвэрийн мод ба Random Forests:**

Random Forests 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 олонхийг авдаг. Жишээ нь, өгөгдлийг ямар нэгэн ангилалд хамааруулж буй модны олонхийн санал нь тухайн ангиллыг илэрхийлэх болно. Ингэснээр олон модны дүгнэлтийг нэгтгэснээр төөрөгдөл, хэт тохиролцооноос сэргийлж, нарийвчлалыг сайжруулдаг (5-р зураг).



5-р зураг. Random forest алгоритм.

**b. Мэдрэлийн сүлжээ ба гүн сургалт:**

Гүн сургалтын загварууд, ялангуяа convolutional neural networks (CNN) болон recurrent neural networks (RNN) нь DNS-д суурилсан ботнет илрүүлэлтийг сайжруулдаг. DNS хүсэлтийн дарааллыг боловсруулснаар RNN нь цаг хугацааны хэв маягийг суралцаж, ердийн урсгалаас ботнет урсгалыг ялгах боломжтой. Гүн сургалтын аргууд нь шифрлэгдсэн DNS хүсэлттэй (DNS over HTTPS болон DNS over TLS) холбоотой төвөгтэй асуудлуудыг шийдвэрлэхэд оновчтой байдаг [6].

**II. Хяналтгүй сургалтын загварууд:**

Урьдчилан мэдэгдэхгүй ботнетийг илрүүлэхэд хяналтгүй сургалтад суурилсан ML загварууд нь үр дүнтэй байдаг. Кластерийн техникүүд (жишээ нь, k-means эсвэл DBSCAN) нь өгөгдлийг ижил төстэй байдал дээр үндэслэн бүлэглэж, ботнеттэй холбоотой хэвийн бус урсгалыг илрүүлэх боломжтой.

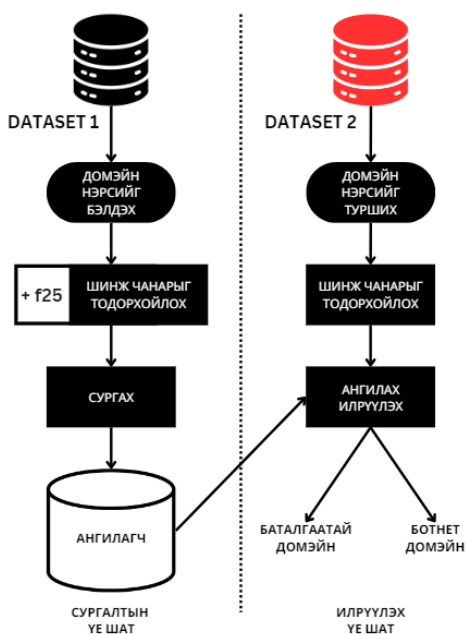
**a. Хосолсон ба нэгдмэл загварууд:**

Хосолмол аргууд нь илрүүлэх нарийвчлалыг нэмэгдүүлэхийн тулд олон алгоритмыг хослуулдаг. Жишээлбэл, эхлээд хэвийн бус асуулгуудыг илрүүлэхээр аномалийг илрүүлэх аргыг ашиглаж, дараа нь хяналттай ангилагчийг ашиглан DGA эсэхийг баталгаажуулна.

**VI. СУДАЛГААНЫ АРГА ЗҮЙ БОЛОН ҮР ДҮН**

Бид судалгаандаа Random Forest нь олон шийдвэрийн модыг агуулах машин сургалтын олонлогийн аргачлал бөгөөд өгөгдлийн үнэн зөвийг сайжруулахад ашиглагддаг аргыг сонгосон бөгөөд энэ нь хүчтэй чанараараа алдартай бөгөөд DGA-д суурилсан ботнет-уудын DNS-ийг илрүүлэхэд өргөнөөр ашиглагддаг, учир нь бот домайнуудаас ялгарах хэв маягийг үр дүнтэй барьж, ялгааг тодруулахад тусалдаг. Gozi зэрэг DGA-д суурилсан ботнет-уудын хувьд Random Forest нь домайны урт, энтропи, давтамжийн тархалт зэрэг шинж чанаруудыг ашиглан хортой бот домэйнуудын өвөрмөц хэв маягийг илрүүлэхэд тусална.

Бидний судалгаа нь DGA ашигладаг ботнетийг илрүүлэхийн тулд Random Forest алгоритм ашиглан DNS лавлагааг хууль ёсны болон хортой гэж ангилэх дэвшилтэт машин сургалтын загварыг ашиглана. Энэхүү загвар нь ангиллын нарийвчлалыг сайжруулах зорилгоор хоёр үндсэн үе шатнаас бүрддэг: сургалт болон илрүүлэлт (6-р зураг). Энэ судалгааны ажлаар DGA-ийг ашиглан үүсгэсэн домэйнуудыг илүү сайн танихын тулд *гийгүүлэгч* болон *эгшигийн* харьцааг илэрхийлэх шинэ Гийгүүлэгч-Эгшигийн Харьцаа (CVR) үзүүлэлтийг 25 дахь шинж чанар болгон нэмж ашиглахыг санал болгож байна. Уг үзүүлэлт нь DGA-аар үүсгэгдсэн домэйн нэрүүдийн хувьд түгээмэл ажиглагддаг фонетик болон бүтцийн онцлоггүй байдлыг илэрхийлдэг хэл зүйн үзүүлэлт юм. Судалгаагаар хууль ёсны домэйн нэрүүдийг уншигдахуйц байлгах үүднээс гийгүүлэгч-эгшигийн зохицолтой байдлыг хадгалдаг бол DGA-аар үүсгэсэн домэйн нэрүүд нь таних загвараас зайлсхийж, хар жагсаалтад орохоос хамгаалах зорилгоор ихэвчлэн гийгүүлэгчийг хэт их агуулсан бүтэцтэй байдаг болохыг тогтоолоо.



6-р зураг. Дэвшүүлж буй загвар.

**I. Сургалтын болон илрүүлэлтийн үе шат**

Сургалтын үе шат нь домэйны урьдчилан тодорхойлсон хууль ёсны болон ботнет үүсгэсэн домэйнууд бүхий өгөгдлийн багц ашиглан ангилагчийг барьж байгуулах үйл явц юм. Энэхүү үе шат нь онцлог шинжийг гаргаж авах, загварыг сургах гэсэн хоёр үндсэн алхмаас бүрдэнэ. Уламжлалт DNS-т суурилсан шинж чанарууд болон Hoang, Vu нарын загварт суурилсан шинж чанаруудыг багтаасан 24 ялгаатай шинж чанар болон шинээр санал болгож буй 25 дахь CVR шинж чанар болгон хувиргасан. Энтропи нь домэйны нэрэнд орсон санамсаргүй байдлыг хэмжиж, жин нь тодорхой n-грамын ач

холбогдлыг тодорхойлдог. Энэ нь хэвийн бус дарааллыг илрүүлэхэд тусалдаг. Домэйны нэрэнд орсон гийгүүлэгч, эгшиг, тоонуудын тархалтыг тооцож, хэвийн бус хослолыг илрүүлэхэд ашигладаг. Учир нь DGA домэйнууд ихэвчлэн ер бусын хослолыг агуулдаг [11][8]. CVR нь бусад хэл зүй болон статистикийн үзүүлэлтүүдтэй хослуулснаар илүү өргөн хүрээний шинжилгээ хийх боломжийг олгодог. Энэхүү үзүүлэлт нь энтропи болон n-грам үзүүлэлтүүдийн давтамж, нарийн төвөгтэй байдлыг хэмжиж, DGA домэйн нэрүүдэд ажиглагддаг ер бусын хэл зүйн онцлогуудыг илэрхийлнэ. CVR-ийн үзүүлэлтийг нэмснээр ангилагчийн нарийвчлалыг нэмэгдүүлж, хууль ёсны болон DGA-гаар үүсгэгдсэн домэйн нэрийн ялгааг тодорхойлох боломжтой [5][6]. Судалгааны үр дүнгээс харахад DNS-д суурилсан ботнет илрүүлэлтийн загварт хэл зүйд суурилсан үзүүлэлтүүдийг нэмж оруулснаар хууль ёсны урсгалтай төстэй домэйн нэрүүдийн хуурамч эерэг илэрцгийг багасгаж, илрүүлэлтийн нарийвчлалыг нэмэгдүүлдэг болох нь тогтоогдсон. Машин сургалтын алгоритмд CVR-ийг нэмснээр домэйн нэрийн бүтцийн шинж чанарыг илүү нарийвчлан шинжилж, гарын үсэгт суурилсан уламжлалт илрүүлэлтийн аргуудаас хараат бус илрүүлэх аргачлалыг бий болгодог.

CVR-ийг оруулснаар энэхүү машин сургалтын загвар нь ботнет илрүүлэлтийн шинэ чиг хандлагад нийцэж, шинээр гарч ирж буй эсвэл одоогийн DGA домэйн нэрүүдийг илүү үр дүнтэй таних боломжийг бий болгоно гэж найдаж байна. Гийгүүлэгч-Эгшигийн Харьцааг тооцоолох томъёо нь доорх байдлаар илэрхийлэгдэнэ:

$$CVR = \frac{countco(d)}{countnv(d)} \tag{1}$$

Үүнд,  $countco(d)$  нь домэйн нэрэнд агуулагдах нийт гийгүүлэгчийн тоо,  $countnv(d)$  нь домэйн нэрэнд агуулагдах нийт эгшигийн тоог илэрхийлнэ.

Илрүүлэлтийн үе шат нь сургалтын үе шатны онцлог шинж гаргаж авах үйл явцтай ижил боловч орж ирсэн домэйныг ангилагчийн тусламжтайгаар ангилдаг. Шинэ DNS лавлагаануудаас орж ирсэн домэйны нэрийг сургалтын үеийнхтэй адил онцлог шинжийн вектор болгон хувиргадаг. Сургалтаар бэлтгэгдсэн Random Forest ангилагчийг ашиглан мод тус бүрийн олонхийн саналаар домэйныг хууль ёсны эсвэл хортой гэж ангилна. Энэ үе шат нь бодит цагийн илрүүлэлтийн хэрэгцээг хангах өндөр үр ашигтай үйл ажиллагаа явуулахад чухал юм [11].

**II. Сургалтын үр дүн**

Туршилтад ашигласан өгөгдлийн багц нь Alexa-гийн топ домэйнуудаас авсан хууль ёсны домэйн 10,000, Cryptolocker, Tinba (7-р зураг) зэрэг DGA ботнетуудын үүсгэсэн 100,000 ботнет домэйныг ашиглана. Мөн нэмэлт 100,000 ботнет домэйн нь Rovnix гэх DGA ботнетээс авсан бөгөөд нийт 210,000 домэйны өгөгдөл дээр туршилт хийсэн байгаа.

isDGA	domain	host	subclass	
2 unique values	160000 unique values	159235 unique values	alexa legit Other (80000)	27% 23% 50%
dga	g1bt1xwhbnpxs	g1bt1xwhbnpxs.ru	cryptoLocker	
dga	ххамарыipbfpk	ххамарыipbfpk.ru	cryptoLocker	
dns_domain_name	dns_top_level_domain	dns_second_level_domain	dns_domain	
.com.	com	athomenet.com	14	
e6eb0362db5ae43cc103986d2d96b5c1d937c...	com	dnscat-txt.com	233	

7-р зураг. Сургалтанд ашигласан dataset.

Эхлээд өгөгдлийн багцын чанарыг улам сайжруулахын тулд өгөгдөл цэвэрлэх процедурыг гүйцэтгэсэн. Үүнд:

- ✓ Давхардсан query-response хосыг устгасан.
- ✓ Буруу шошготой query-response хосуудыг устгасан
- ✓ Query-response үйлдэл дэх командуудад мэдээлэл дутмаг дуу чимээтэй пакетуудыг устгасан
- ✓ ALFlowLyzer-ийн задлан шинжлэх алдааны улмаас өгөгдөл буруу задлагдсан query-response хосуудыг устгасан
- ✓ Сүлжээ эсвэл нэрийн серверийн асуудлаас шалтгаалж алдаатай эсвэл бүрэн бус хариултыг харуулсан query-response хосыг устгасан гэх мэтээр цэвэрлээд дараа нь өгөгдлийн шинж чанарт шинжилгээ хийсэн.

No.	Botnet names	Total domains	Correctly detected	DR (%)
1	emotet	4000	3994	99.85
2	gameover	4000	4000	100
3	murofet	4000	3994	99.85
4	necurs	4000	3947	98.67
5	pykspa_v1	4000	3621	90.53
6	ramnit	4000	3888	97.20
7	ranbyus	4000	3993	99.82
8	rovnix	4000	4000	100
9	shiotob	4000	3892	99.55
10	symmi	1200	1162	96.83
11	tinba	4000	3951	98.77
12	mydoom	50	46	92.00
13	tinynuke	32	31	96.88
14	vidro	100	98	98.00
15	gspy	100	91	91.00
16	pykspa_v2_fake	799	732	91.61
17	padcrypt	168	166	98.81
18	fobber_v1	298	298	100
19	fobber_v2	299	288	96.32
20	dircrypt	762	742	97.38
21	cryptolocker	1000	990	99.00
22	locky	1158	1098	94.81
23	chinad	1000	1000	100
24	qadars	2000	1970	98.50
25	dyre	1000	980	98.00
	<b>Micro DR</b>	<b>49966</b>	<b>48972</b>	<b>98.01</b>
	<b>Macro DR</b>			<b>97.34</b>

8-р зураг. Дэвшүүлж буй загварын 25 ботнет дээрх судалгаа.

No.	Botnet names	Total domains	Correctly detected	DR (%)
1	simda	4000	2944	73.60
2	virut	4000	3293	82.32
3	proslifean	100	84	84.00
4	tempedreve	195	172	88.21
5	pykspa_v2_real	199	178	89.45
6	conficker	495	387	78.18
7	nymaim	480	415	86.46
8	enviserv	500	382	76.40
9	vawtrak	827	692	83.68
10	shifu	2546	2262	88.85
	<b>Micro DR</b>	<b>13342</b>	<b>10809</b>	<b>81.01</b>
	<b>Macro DR</b>			<b>83.11</b>

9-р зураг. Дэвшүүлж буй загварын 10 ботнет дээрх судалгаа.

No.	Botnet names	Total domains	Correctly detected	DR (%)
1	banjori	4000	0	0
2	matsnu	881	10	1.14
3	bigviktor	999	30	3.00
4	suppobox	2205	21	0.95
	<b>Micro DR</b>	<b>8085</b>	<b>61</b>	<b>0.75</b>
	<b>Macro DR</b>			<b>1.27</b>

10-р зураг. Дэвшүүлж буй загварын хууль ёсны домэйнтай төстэй дөрвөн ботнет дээрх судалгаа.

Энэ загварын нэг өвөрмөц онцлог нь DGA ботнетийн төрлүүдийн дагуу илрүүлэлтийн чадварыг ялгавартайгаар тодорхойлох явдал юм. Emotet, Gameover зэрэг илүү ойлгомжтой ботнетууд бараг төгс илрүүлэлтийн түвшинтэй байсан бол Banjori, Matsnu зэрэг хууль ёсны домэйнүүдтэй төстэй ботнетуудын хувьд илрүүлэлтийн түвшин бага байсан нь цаашид сайжруулах боломж байгааг харуулж байна. Ноang болон Vu нарын загвар нь DNS-д суурилсан ботнет илрүүлэлтийн үр ашгийг харуулж, DGA ботнетийг илрүүлэхэд бодит цагийн өндөр үр дүн, бага хуурамч дохиотойгоор үр дүнтэй ажилладаг болохыг баталсан. Бидний дэвшүүлсэн 25 дахь шинж чанарыг нэмж гүйцэтгэсэн судалгааны үр дүнд дараах нарийвчлалыг гарган авсан (11-р зураг):

Overall Detection Accuracy: 96.10%

Classification Report:

	precision	recall	f1-score	support
Legitimate	0.94	0.18	0.30	2943
Botnet	0.96	1.00	0.98	60057
accuracy			0.96	63000
macro avg	0.95	0.59	0.64	63000
weighted avg	0.96	0.96	0.95	63000

11-р зураг. Судалгааны оновчтой байдлын харуу #1.

Эхний сургалтанд ботнет домэйн нэрсийг танихад бараг төгс нарийвчлал, сэргэлтийг үзүүлсэн бөгөөд энэ нь SturtoLocker болон Tinba зэрэг ботнетуудийн үүсгэсэн домэйн нэрсийг илрүүлэх чадвар өндөр байгааг харуулж байна. Гэвч хууль ёсны домэйн нэрсийн recall **18%** буюу бага гарсан нь зарим хууль ёсны домэйнүүд ботнетээр андуурагдаж байгааг илтгэж байна. Энэ ялгаа нь хэрэглэсэн онцлог шинжүүдээс үүдэлтэй байж болох бөгөөд эдгээр шинжүүд нь ботнет домэйн нэрсийг танихад үр дүнтэй байсан ч хууль ёсны домэйн нэрсийн бүрэн шинжийг илэрхийлж чадахгүй байж магадгүй юм.

Дараагийн (12-р зураг) сургалтанд 97.25%-ийн нийт нарийвчлалтай болжээ, энэ нь өндөр үзүүлэлт боловч зөвхөн энэ үзүүлэлт нь алдаа ангилах загварыг бүрэн илэрхийлэхгүй. Ялангуяа "хууль ёсны" домэйнууд нь бодит DGA ботнет домэйнууд байсан гэдгийг харгалзан үзэхэд.

Detection Accuracy: 97.25%  
Classification Report:

	precision	recall	f1-score	support
Legitimate	0.96	0.73	0.83	3017
Botnet	0.97	1.00	0.99	29983
accuracy			0.97	33000
macro avg	0.97	0.86	0.91	33000
weighted avg	0.97	0.97	0.97	33000

12-р зураг. Судалгааны оновчтой байдлын хариу #2.

Recall харьцангуй доогуур, энэ нь модел зөвхөн 73%-ийг нь "хууль ёсны" гэж тодорхойлсон бөгөөд үлдсэн 27%-ийг нь "ботнет" гэж алдаатай ангилсан. "Хууль ёсны" домэйнууд нь бодит DGA ботнет домэйнууд тул тэдний шинж чанарууд ботнет домэйнуудтай төстэй байж магадгүй. Модел нь зарим нэг ботнет домэйнуудын шинж чанарт суралцаж, тухайн "хуурамч" DGA домэйнуудыг ялгаж чаддаггүй, энэ нь алдаа ангилалд хүргэж байна. Энэхүү загвар нь дэлгэрэнгүй шинж чанар, Random Forest алгоритмын оновчтой ангилал болон олон төрлийн домэйнтэй төлөөллийн өгөгдлийн багцтай. Цаашид загварыг хууль ёсны домэйнд ойр төстэй ботнетийг илрүүлэх чиглэлд гүн сургалтын арга нэмэлт байдлаар ашиглах боломжийг судлах хэрэгтэй.

## VII. ДҮГНЭЛТ

Сүүлийн жилүүдэд ботнетууд нь цахим аюулгүй байдлын томоохон заналхийлэл болж, тэдгээрийг илрүүлэхэд улам нарийн төвөгтэй сорилтууд үүссээр байна. DNS нь домэйн нэрийг IP хаяг руу хөрвүүлэх үндсэн үүрэгтэй тул ботнетийн идэвхийг илрүүлэх гол суурь болдог. Энэхүү судалгаагаар DNS-д суурилсан ботнет илрүүлэх аргуудыг гүнзгийрүүлэн судалж, тэдгээрийн кибер аюулаас хамгаалах боломжийг үнэлсэн болно. ML-д суурилсан DNS илрүүлэх технологи нь ботнетийн халдлага болон кибер аюулыг эрт үед нь илрүүлж, хамгаалалтыг сайжруулах боломжийг өгч байгааг судалгаагаар харуулсан ба энэ нь халдлагыг эрт шатанд тодорхойлон, урьдчилан сэргийлэх шинэ хамгаалалтын шийдэл гаргахыг зорьсон. DNS-д суурилсан аюулгүй байдлын аргууд нь кибер аюулыг илрүүлэх үр дүнтэй шийдэл болж байгааг энэхүү судалгаагаараа онцолсон бөгөөд ялангуяа Random Forest алгоритмыг ашиглан ботнетийн идэвхийг илрүүлэхэд үр дүнтэй болохыг харуулсан. Энэхүү судалгааны ажлын хүрээнд Xuan Dau Hoang болон Xuan Hanh Vu нарын дэвшүүлсэн DNS лавлагааг хууль ёсны болон хортой гэж ангилах дэвшилтэт машин сургалтын загварыг судалж үзсэн ба энэхүү загвар нь өмнөх илрүүлэх системүүдийн FPR болон FNR үзүүлэлтийг бууруулж, илрүүлэлтийн нарийвчлалыг нэмэгдүүлэхэд чиглэгдсэн. Загварын

илрүүлэлтийн түвшин болон нарийвчлал 97%-иас дээш байж, уламжлалт аргуудаас илүү сайн үзүүлэлттэй гарсан. Гэвч зарим ботнетууд нь хууль ёсны домэйн нэртэй төстэй бүтэцтэй байсан нь илрүүлэх түвшинд сөргөөр нөлөөлж, сайжруулах боломжийг харуулж байна.

Эцэст нь дүгнэхэд, кибер аюулгүй байдал нь өнөө үед зайлшгүй чухал, учир нь бидний мэдээллийн аюулгүй байдал, системийн найдвартай байдал, кибер орчны аюулгүй байдлыг хамгаалах үндсэн хэрэгцээг хангаж байна. Өнөөгийн эрин үед кибер гэмт хэрэг улам бүр нарийсаж, хүчирхэгжиж буй тул илрүүлэлтийн үр дүнг сайжруулж, тэдгээрийг амжилттай зогсоохын тулд дэвшилтэт арга барилуудыг хөгжүүлэх шаардлагатай. Энэхүү судалгаагаар бодит цагийн DNS-д суурилсан ботнет илрүүлэлтийн өндөр үр дүнтэй, бага хуурамч дохиотой загварыг хэрэгжүүлж болохыг харуулсан. Энэ загвар нь ботнетийн төрөл бүрийн халдлагыг үр дүнтэй илрүүлж, аюулыг хяналтдаа авах боломжийг олгосон ч хууль ёсны домэйнтэй төстэй ботнетийг илрүүлэхэд асуудал байсаар байна. Ирээдүйд эдгээр ботнетийг илрүүлэхийн тулд гүн сургалтын аргуудыг нэмж судлах нь загварыг илүү өргөн цар хүрээтэй, олон төрлийн аюулыг илрүүлэх өндөр чадвартай болгох боломжийг бүрдүүлэх юм.

## АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Singh, M., Singh, M., & Kaur, S. (2019). Issues and challenges in DNS-based botnet detection: A survey. \*Computers & Security\*, 86\*, 28-52. <https://doi.org/10.1016/j.cose.2019.05.019>
- [2] Wang, Y., Zhou, A., Liao, S., Zheng, R., Hu, R., & Zhang, L. (2021). A comprehensive survey on DNS tunnel detection. \*Computer Networks\*, 197\*, 108322. <https://doi.org/10.1016/j.comnet.2021.108322>
- [3] Alieyan, K., Almomani, A., Manasrah, A., & Kadhum, M. M. (2017). A survey of botnet detection based on DNS. \*Neural Computing and Applications\*. <https://doi.org/10.1007/s00521-015-2128-0>
- [4] Lee, J., & Park, Y. (2020). Botnet detection using deep learning techniques: A survey. \*IEEE Access\*, 8\*, 200749-200771. <https://doi.org/10.1109/ACCESS.2020.3035609>
- [5] Chen, T., Yan, Q., Wang, Z., & Liu, Y. (2020). Detecting botnets with network behavior analysis using machine learning. \*IEEE Transactions on Dependable and Secure Computing\*, 17(2), 290-304. <https://doi.org/10.1109/TDSC.2019.2928396>
- [6] Kolini, F., & Martin, J. (2019). Understanding botnet behavior and network characteristics. \*Future Internet\*, 11\*(3), 78. <https://doi.org/10.3390/fi11030078>
- [7] Li, Y., Dai, Y., Zhang, Y., & Chen, W. (2018). Botnet detection via machine learning on flow data. \*IEEE Transactions on Computers\*, 67\*(11), 1572-1585. <https://doi.org/10.1109/TC.2018.2848654>
- [8] Gao, H., Xu, Z., & Li, Y. (2021). A comparative survey on botnet detection in Internet of Things. \*IEEE Internet of Things Journal\*, 8\*(12), 9707-9725. <https://doi.org/10.1109/IIOT.2020.3022165>
- [9] Jiang, M., & Zhou, W. (2018). Botnet detection via DNS anomaly detection using machine learning techniques. \*IEEE Transactions on Network and Service Management\*, 15\*(1), 192-204. <https://doi.org/10.1109/TNSM.2018.2794386>
- [10] Zeng, J., Lou, X., & Liu, J. (2020). A study on DNS-based botnet detection using hybrid approaches. \*Journal of Network and Computer Applications\*, 156\*, 102581. <https://doi.org/10.1016/j.jnca.2020.102581>
- [11] Hoang, X. D., & Vu, X. H. (2021). An improved model for detecting DGA botnets using random forest algorithm. \*Information Security Journal: A Global Perspective\*. <https://doi.org/10.1080/19393555.2021.193419>

## МИКРОМАУС ТЭМЦЭЭНИЙ ХУГАЦАА ХЭМЖИХ ТӨХӨӨРӨМЖИЙН ЗАГВАР

Дашцэрэнгийн НАМУУНАА<sup>1</sup>, Болдын БАТ-ЭРДЭНЭ<sup>2</sup>

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбоо технологийн сургууль, Электроникийн инженерийн салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: bat-erdene@must.edu.mn<sup>1\*</sup>*

**Хураангуй:** Техник, технологийн хурдтай хөгжлийн энэ цаг үед автоматжуулалтын болон ухаалаг системүүдийн хэрэгцээ, шаардлага өсөн нэмэгдэж байна. Энэхүү дипломын ажлын зорилго нь Микромаус роботын уралдааны хугацаа тоолох системийг хөгжүүлэхэд чиглэсэн. Микромаус нь 16x16 нүднээс тогтох талбайд байгуулсан санамсаргүй бүтэцтэй төөрдөг байшин маягийн саадтай замаар 16x16см хэмжээнээс хэтрэхгүй овор хэмжээтэй микромаус нэртэй робот гарааны зурхайгаас барианд хамгийн бага зай туулж очих хугацаагаар өрсөлддөг тэмцээн юм. Байрлал болон туулсан замаа бодож, шинэ тооцоолол хийх алгоритм бүхий программчлалтай ухаалаг робот оролцдог нь энэ тэмцээний онцлог билээ. 2017 оноос Монгол улсад тогтмол зохион байгуулагдаж байгаа тус тэмцээнд оролцогчийн хугацааг хэмжих үйл ажиллагааг автоматжуулж, хүний оролцоог багасгах зорилгоор энэхүү судалгааны ажлыг хийсэн бөгөөд хугацаа тоолох системийн техник ба программ хангамжийн шийдлийг санал болгож байна. Хугацаа тоолох систем нь ESP32 микроконтроллер, лазер гэрэл мэдрэгч, Visual Studio программчлалын орчин зэрэг технологийг ашиглан, тэмцээний талбайн гараа, барианы зурхайн техник хангамж ба бодит хугацаанд нарийвчлалтайгаар роботын туулсан замын хугацааг хэмжиж, өгөгдлийн санд болон хэрэглэгчдэд харуулах программ хангамжаас бүрдэнэ. Энэ системийн техник хангамж нь санамсаргүй бүтэцтэй төөрдөг байшингийн саад ханын хаана ч гараа эсвэл бариан зурхайг төлөвлөхөд нийцтэй овор хэмжээтэй, мэдээллийг утасгүйгээр мэдээллийн санд алдагдалгүй дамжуулдаг, программ хангамж нь тэмцээний бүх оролцогчдын болон тухайн оролцогчийн бүх мэдээллийг нэг дор харуулах, эрэмбэлэх зэрэг хэрэглээний хялбар шийдэлтэй, уралдааныг удирдан зохион байгуулах ажлыг автоматжуулж, цаг хэмжих алдааг багасгасан, үр дүнтэй, найдвартай ажиллагаатай зэрэг давуу талтай.

**Түлхүүр үг:** Микромаус тэмцээн, ESP32

### I. УДИРТГАЛ

1977 онд микромауч тэмцээнийг зохион байгуулах санааг IEEE SPECTRUM сэтгүүл гаргасан бөгөөд 1979-оны 6-р сард НЬЮ-ЙОРК хотод зохион байгуулагдахаар зарлагдсан. Уг тэмцээнээр 6000 бүтээл ирсэн ч 15 робот уралдсан байна.

Техник технологи хөгжсөн одоо цагт хүүхэд багачуудын сонирхолыг татахуйц зүйлсын нэг бол автомат роботын тэмцээн юм. Автомат роботын тэмцээн нь дотроо олон төрөл байх бөгөөд :

- Микромаус
- Шоо цуглуулагч
- Робот рейс гэх мэт төрлүүд байна.

Энэхүү автомат роботын тэмцээнийг 2009 оноос эхлэн Мэдээлэл холбоо технологийн сургуулийн электроникийн салбарын оюутны “HIGH TECH” клубээс санаачлан зохион байгуулж эхэлсэн. 2017 оноос “Робот сонирхогчдын робокон нийгэмлэг” тус тэмцээнийг хамтран зохион байгуулж эхэлсэн.

### II ТЭМЦЭЭНИЙ ЕРӨНХИЙ ЖУРАМ

Тэмцээнийг зохион байгуулагч байгууллага (цаашид зохион байгуулагч гэнэ), шүүгчид болон тэмцээнд оролцогчид (цаашид оролцогч гэнэ) нь бие биений эрх ашиг, бие даасан байдлыг хүндэтгэн тэмцээнийг ёс зүй, дэг журамтай явуулах үүднээс

дараах журмыг баримтлан зохион байгуулж, шүүж, оролцоно. Зохион байгуулагч нь:

- Тэмцээний товгыг тэмцээн явагдахаас 21 хоногийн өмнө веб хуудсаар зарласан байна.
- Оролцогчдыг тэмцээний талаарх бүх мэдээллээр хангана.
- Тэмцээний явц үр дүнг тухай бүрд нь ойлгомжтой мэдээллэнэ.
- Зохион байгуулагчид тэмцээний үеэр мандат зүүсэн байна. Оролцогч нь:
- Тэмцээн эхлэхээс 24 цагийн өмнө заавал вэбээр дамжуулан бүртгүүлсэн байна.
- Их, дээд сургуулийн оюутан эсвэл ерөнхий боловсролын сургуулийн сурагч гэсэн ангиллын шудрагаар сонгон үнэн зөв бөглөсөн байна
- Тэмцээн эхлэхээс нэг цагийн өмнө оюутан эсвэл сурагч болохыг баталсан бичиг баримтын хамт ирж, бүртгэлийн хураамж төлөн мандат авсан байна.
- Тэмцээний явцад мандатаа тогтмол зүүж явна.
- Тэмцээн зохион байгуулагчаас тогтоосон байршилд байрлан бэлтгэлээ хангана.
- Сонгон оролцож байгаа тэмцээний журам болон цагийг ягштал баримтлана.

- Тэмцээнд оролцох дарааллаа мэдэж, дарааллын дагуу бусдыг хүлээлгэхгүй оролцоно.

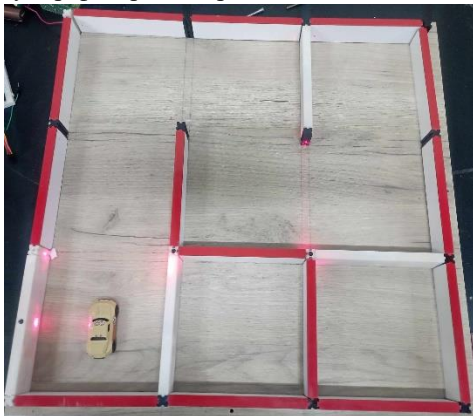
үүсгэн хүлээн авагчид туссанаар хүлээн авагч удирдлагын хэсэгт мэдээллийг дамжуулна.

## II. СУДЛАГДСАН БАЙДАЛ

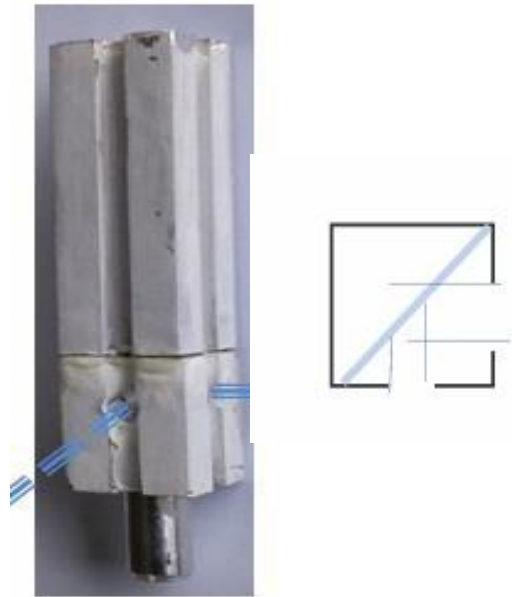
Ашигласан элементүүд:

- Лазер
- ESP32
- Фоторезистор

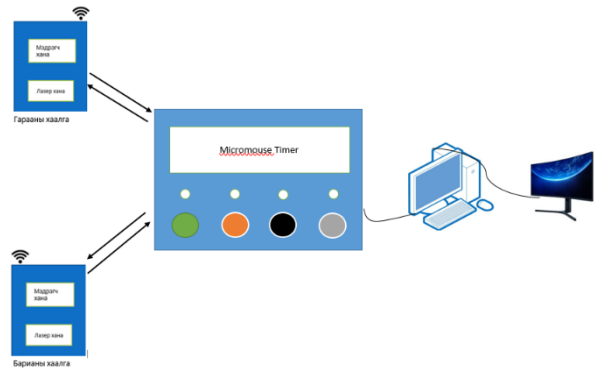
Уг судалгааны ажилд хүлээн авагчаар фоторезистор ашигласан ба яагаад гэвэл уг тэмцээнд ашигладаг хананы өргөн нь 1,2 см байдаг ба энэ хананд багтах ёстой учир фоторезисторыг сонгож авсан.



1-р зураг. Төслийн ажлын бодит харагдах байдал

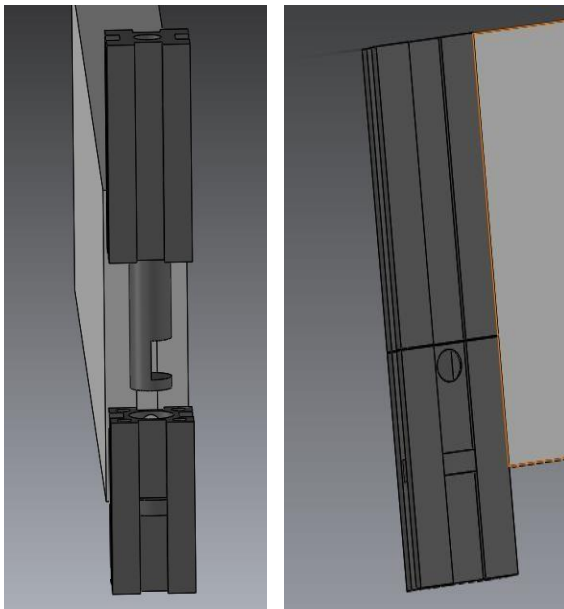


3-р зураг. Төлийн тусгалын хугарал

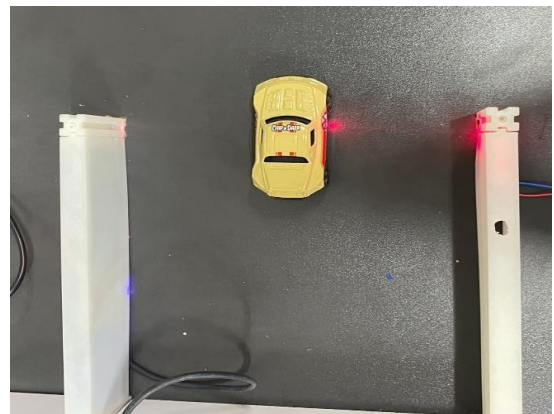


4-р зураг. Системийн бүтцийн схем

## III. СИСТЕМ ИЙН МЕХАНИК ШИЙДЭЛ



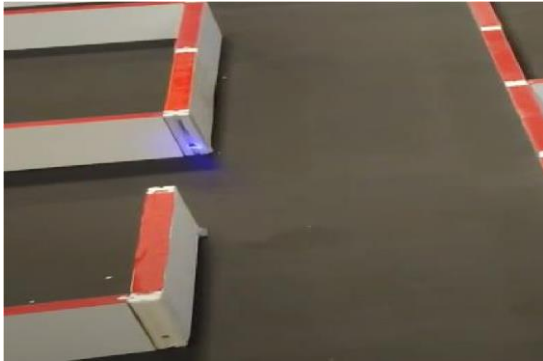
2-р зураг. Системийн механик шийдэл



5-р зураг. Модулуудыг угсарч туршилт хийсэн загвар

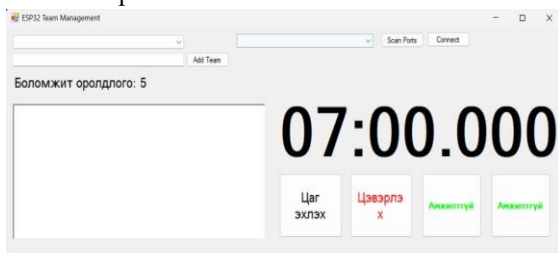
Уралдааны замын баганы голд 45 градусын налуугаар толь байрлуулж өгсөн ба лазер гэрэл нь толинд тусахдаа 90 градусын гэрэлийн хугарал

## ТУРШИЛТЫН ҮР ДҮН



6-р зураг. Уралдааны талбайд байрлуулсан байдал

Уг лазер мэдрүүр нь микромаус тэмцээний гараа болон барианы хэсэгт байрлах ба робот гараанаас гарах болон барианд орход дохио илгээх ба гараанаас гарсан гэх дохио ирхэд хугацаа тоолж эхлээд барианд орход хугацаа автоматаар зогсоно.



7-р зураг. Хугацаа мэдээлэх системийн туршилтын загвар

## IV. ДҮГНЭЛТ

Төсөл ажлын хүрээнд микромаус роботын хугацаа тоолох системийг хөгжүүлэн уралдааныг үнэн зөв

зохион байгуулах талаас нь зорилго тавин ажилласан билээ.

Уг зорилгодоо хүрэхийн тулд ижил төстэй системүүдэд судалгаа хийн микромаус тэмцээний стандарт шаардлагад нийцсэн хугацаа тоолох системийг өөрийн хэмжээнд хийж гүйцэтгэсэн бөгөөд эхний хувилбарыг 2024.11.2 -нд зохион байгуулагдсан Автомат роботын тэмцээнд амжилттай ашигласан.

Тэмцээний хугацаа тоолох төхөөрөмж нь уралдааны хананд багтсан байх шаардлагатай байсан бөгөөд үүнийг механик шийдэл гарган уралдааны замын баганыг дундаа голтой байхаар загварчилсан. Ингэснээр баганын голд эргэдэг гол хийж голын хэсэгт толь байрлуулж өгсөн ингэснээр хана болон баганын хэсэгт илүү гарах зүйл байхгүй цэвэрхэн болж өгсөн.

Программ хангамжийн хэсэгт Visual studio ашигласан ба уг программтай сериалаар холбогдон мэдээллээ хүлээн авч ажилласан. Уг төслийн ажлын хүрээнд механик шийдлийг бүрэн шийдсэн гэж дүгнэж байгаа бөгөөд цаашид хөгжүүлбэл зохих хэсэг нь дэлгэцийн программ юм.

### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

1. [https://en.wikipedia.org/wiki/Laser\\_diode](https://en.wikipedia.org/wiki/Laser_diode)
2. <https://sictelec.wixsite.com/robotcontest>
3. [https://micromouseonline.com/download/MIN\\_OS18-David-Hannaford-RATS.pdf](https://micromouseonline.com/download/MIN_OS18-David-Hannaford-RATS.pdf)

## 2020-2024 ОНЫ СУДАЛГААНД ТУЛГУУРЛАН RANSOMWARE ХАЛДЛАГЫН ЧИГ ХАНДЛАГЫГ ТОДОРХОЙЛОХ

Гантуул НОМИН-ЭРДЭНЭ<sup>1</sup>, Бат-Өлзий УДВАЛ<sup>2</sup>, Золзаяа ЖАВЗАНДУЛАМ<sup>3</sup>

<sup>1</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: javzaazolzaya@gmail.com <sup>1</sup>*

*Хураангуй:* Энэхүү төсөл нь ransomware халдлагын ирээдүйн чиг хандлагыг урьдчилан таамаглах, өгөгдөлд суурилсан загваруудыг ашиглан урьдчилан сэргийлэх зөвлөмж боловсруулахад чиглэгдсэн. Судалгааны эхний шатанд ransomware чиг хандлага, эрсдэлт хүчин зүйлсийг тодорхойлохын тулд сүүлийн үеийн судалгаануудтай танилцана. Дараа нь ransomware хэргүүдийн өгөгдлийг боловсруулж, ARIMA болон GLM загваруудыг ашиглан таамаглал гаргаж, эрсдэлийн түвшнийг тодорхойлно. Загварын нарийвчлалыг шалгасны дараа, олж авсан үр дүнд үндэслэн урьдчилан сэргийлэх зөвлөмж боловсруулна.

*Түлхүүр үг:* ransomware, өгөгдөл, халдлага, халдлагаас сэргийлэх

### I. УДИРТГАЛ

Орчин үеийн дижитал ертөнцөд цахим аюулгүй байдлын асуудал улам бүр чухал болж байна. Байгууллага, хувь хүмүүсийн мэдээллийг барьцаалж, тодорхой төлбөр нэхдэг хортой программ буюу ransomware халдлага нь сүүлийн жилүүдэд хурдацтайгаар нэмэгдэж, дэлхий даяар томоохон эрсдэл үүсгэх болсон. Энэ төрлийн халдлага нь ихэвчлэн компьютерт хадгалагдаж буй мэдээллийг шифрлэж, хандалтыг хязгаарлах эсвэл мэдээллийг задлана гэж сүрдүүлэх замаар төлбөр авах зорилготой байдаг.

Ransomware халдлага нь эдийн засгийн томоохон хохирол учруулж, байгууллагуудын үйл ажиллагааг саатуулах, нэр хүндэд сөргөөр нөлөөлөх эрсдэл дагуулдаг. Халдлагын тоо нэмэгдэхийн хэрээр байгууллагууд урьдчилан сэргийлэх, хамгаалах стратегиудыг сайжруулах шаардлагатай тулгараад байна. Энэхүү судалгаагаар ransomware-ийн халдлагаас хамгаалах арга замуудыг тодорхойлж, дэлхий нийтийн хэмжээнд халдлагад өртөж буй байгууллагуудын туршлага, өгөгдөл дээр дүн шинжилгээ хийнэ.

### II. RANSOMWARE ТӨРЛҮҮД

Ransomware халдлагын төрөл нь мэдээлэлд учруулах хор хөнөөл болон төлбөр нэхэх аргаар бусад халдлагуудаас ялгагддаг бөгөөд дараах үндсэн төрлүүдтэй.

#### 1. Crypto Ransomware

Энэ төрлийн ransomware нь хохирогчийн файлуудыг шифрлэж, шифрлэгдсэн файлуудыг сэргээхэд шаардлагатай нууцлалын түлхүүрийн хариуд төлбөр нэхдэг. Хэрэглэгчдийн чухал

файлуудыг шууд бус замаар хянах боломжийг хаадаг тул санхүүгийн хохирол ихээр учруулдаг.

#### 2. Locker Ransomware

Locker төрлийн ransomware нь хэрэглэгчийг тухайн төхөөрөмжөөс нь шууд хасаж, үйлдлийн систем болон файлуудад нэвтрэх эрхийг хаадаг. Энэ нь системийн түвшний нэвтрэлтийг бүрэн хязгаарладаг бөгөөд мэдээлэлд шууд халдахгүй ч төхөөрөмж ашиглах боломжийг хаадаг.

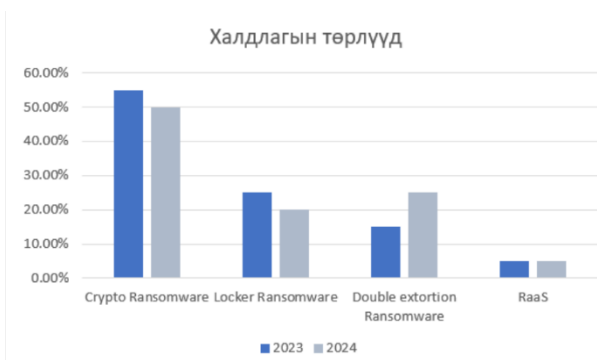
#### 3. Double Extortion Ransomware

Энэ төрлийн халдлага нь хоёр талт барьцаалалтыг ашигладаг бөгөөд эхний ээлжинд мэдээллийг шифрлэн түгжиж, дараа нь төлбөр төлөхөөс татгалзвал тухайн мэдээллийг ил болгоно хэмээн сүрдүүлдэг. Ингэснээр санхүүгийн болон нэр хүндийн эрсдэл дагуулдаг.

#### 4. Ransomware as a Service (RaaS)

Ransomware as a Service буюу RaaS нь кибер гэмт хэрэгтнүүдэд зориулсан үйлчилгээ хэлбэрээр хөгжиж буй ransomware юм. RaaS нь хортой программыг ашиглах эрхийг бусад түрээслэх, эсвэл ашигласны хариуд ашиг орлого хуваалцах нөхцөлтэй байдаг. Ингэснээр ransomware халдлагыг олон янзаар түгээх боломжтой болгож, кибер аюул заналын өргөн тархацад хүргэдэг.

Эдгээр төрлүүд нь байгууллагын мэдээллийн аюулгүй байдалд ноцтой эрсдэл учруулдаг тул ransomware халдлагын талаар гүнзгий ойлголттой байх нь хамгаалалтын үр дүнтэй арга хэмжээ авахад чухал ач холбогдолтой юм.



Зураг 1. Халдлагын төрлүүд

### III. ХАЛДЛАГЫН ХОР УРШИГ

Ransomware халдлага нь байгууллагуудад ихээхэн хор хохирол учруулдаг бөгөөд дараах үндсэн үр дагавруудтай:

#### 1. Мэдээлэл алдагдах (Data Loss)

Халдлагын үеэр шифрлэгдсэн файлуудыг сэргээх боломжгүй болж, чухал мэдээллийг бүр мөсөн алдах эрсдэлтэй. Байгууллагын нууц мэдээлэл, үйлчлүүлэгчдийн хувийн өгөгдөл, санхүүгийн баримт бичиг зэрэг чухал файлуудын алдагдал нь байгууллагын өдөр тутмын үйл ажиллагаанд томоохон саад учруулж, үйлчлүүлэгчид болон ажилтнуудын итгэлийг алдах шалтгаан болдог.

#### 2. Санхүүгийн хохирол (Financial Loss)

Ransomware халдлагад өртсөн байгууллагууд мэдээллээ сэргээхийн тулд төлбөр төлөхөөс гадна, бизнесийн тасалдлын улмаас орлого алдах, сэргээн засварлахад шаардлагатай нэмэлт зардал гаргах хэрэгтэй болдог. Судалгаанаас үзэхэд, ransomware халдлагын дундаж нөхөн сэргээх зардал 2024 онд 1 сая ам.доллараас давсан байна. Хохирогч байгууллагуудын 40% орчим нь нөхөн сэргээхэд 1-ээс дээш сарын хугацаа зарцуулдаг нь бизнесийн томоохон саатал үүсгэдэг.

#### 3. Нэр хүндийн эрсдэл (Reputational Harm)

Мэдээллийн алдагдал, санхүүгийн хохирлоос гадна байгууллагын нэр хүндэд сөрөг нөлөө үзүүлдэг. Үйлчлүүлэгчид болон түнш байгууллагууд байгууллагын мэдээллийн аюулгүй байдалд итгэл алдрах, ирээдүйн харилцаа, бизнесийн боломжуудад нөлөөлөх аюултай. Халдлагад өртсөн байгууллагуудын 59% нь кибер аюулгүй байдлын мэдлэгийг сайжруулах шаардлагатай гэж үзсэн нь энэ төрлийн эрсдэлийн ач холбогдлыг онцолж байна.

#### 4. Халдлагад өртдөг салбарууд (Impacted Sectors)

Ransomware халдлагад өртөх хамгийн өндөр эрсдэлтэй салбаруудад эрүүл мэнд, санхүүгийн

үйлчилгээ, боловсрол, төрийн байгууллагууд болон жижиг дунд бизнесүүд орно. Тухайлбал, эрүүл мэндийн байгууллагад учруулах хохирол нь зөвхөн санхүүгийн талаас бус, үйлчлүүлэгчдийн амь насанд хүртэл аюул учруулж болзошгүй байдаг.

Ransomware халдлагын эдгээр хор уршиг нь кибер аюулгүй байдлын урьдчилан сэргийлэх болон хариу арга хэмжээний чадавхийг сайжруулах шаардлагыг улам тодотгож байна.

### IV. УРЬДЧИЛАН СЭРГИЙЛЭХ АРГА ХЭМЖЭЭ

Ransomware халдлагаас урьдчилан сэргийлэхийн тулд байгууллагуудын кибер аюулгүй байдлын урьдчилан сэргийлэх арга хэмжээг сайжруулах шаардлагатай. Эдгээр арга хэмжээг хэрэгжүүлэх нь халдлагад өртөх эрсдэлийг бууруулж, мэдээллийг хамгаалах боломжийг нэмэгдүүлдэг.

#### 1. Програм хангамжийг тогтмол шинэчлэх (Regular Software Updates)

Програм хангамжийн шинэчлэлтүүд нь аюулгүй байдлын сул талыг засаж, халдлагад өртөх эрсдэлийг бууруулдаг.

#### 2. Хандалтын хяналтыг сайжруулах (Access Control Management)

Байгууллагын мэдээлэлд зөвшөөрөлтэй ажилчид л нэвтрэх боломжтой байх ёстой. Энэ нь зөвшөөрөлгүй нэвтрэлтийг хязгаарлаж, ажилтнуудын эрхийг тодорхой хэмжээнд хязгаарласнаар хэрэгждэг.

#### 3. Сүлжээний сегментчилэл (Network Segmentation)

Байгууллагын сүлжээг олон сегментэд хувааж, тус бүрийн хандалтыг хянах замаар халдвар тархах эрсдэлийг бууруулах боломжтой. Халдлага нэг сегментэд үүссэн тохиолдолд бусад сегментүүдэд хяналтгүйгээр тархахаас сэргийлнэ.

#### 4. Ажилчдыг фишинг илрүүлэхэд сургах (Employee Training on Identifying Phishing Threats)

Фишинг нь ransomware халдлагын хамгийн нийтлэг эх үүсвэр бөгөөд ажилчид фишинг имэйлийг таньж чаддаг байх ёстой. Ажилчдад сэжигтэй имэйл, линк, хавсралтыг таних талаар сургалт явуулах нь халдлагыг эхнээс нь зогсооход тусална.

#### 5. Нөөц файлуудыг тусад нь хадгалах (Regular Backups Stored Off-Network)

Өгөгдлийг тогтмол нөөцлөх нь ransomware халдлагын үед мэдээллийг хурдан сэргээх боломжийг бүрдүүлнэ. Эдгээр нөөц файлуудыг

үндсэн сүлжээнээс тусад нь хадгалж, ransomware халдлагад өртөхөөс хамгаалах хэрэгтэй.

Эдгээр арга хэмжээнүүдийг тогтмол хэрэгжүүлснээр байгууллагууд ransomware халдлагаас хамгаалалтаа сайжруулж, мэдээллийн аюулгүй байдлаа хангах боломжтой болно.

## V. ХАЛДЛАГАД ӨРТСӨНИЙ ДАРААХ ХАРИУ АРГА ХЭМЖЭЭ

Ransomware халдлагад өртсөн тохиолдолд байгууллагууд хурдан бөгөөд зохион байгуулалттай хариу арга хэмжээ авах нь хохирлыг бууруулахад чухал үүрэгтэй. Дараах арга хэмжээнүүд нь халдлагын хор уршгийг багасгаж, мэдээллийн аюулгүй байдлыг сэргээхэд чиглэгдэнэ:

### 1. Халдварлагдсан системийг сүлжээнээс салгах (*Disconnect Affected Systems from the Network*)

Халдлага системийн бусад хэсэгт тархахаас урьдчилан сэргийлэхийн тулд халдвар авсан төхөөрөмжүүдийг сүлжээнээс нэн даруй салгах хэрэгтэй. Энэ нь ransomware-ийг сүлжээний бусад төхөөрөмжүүдэд нөлөөлөхөөс сэргийлнэ.

### 2. Төлбөр төлөхөөс зайлсхийх (*Avoid Paying Ransoms*)

Хохирогч байгууллагуудын хувьд төлбөр төлөх нь асуудлыг шийдэх биш, гэмт этгээдүүдийг урамшуулж болзошгүй юм. Төлбөр төлсөн ч мэдээлэл бүрэн сэргэх баталгаа байхгүй бөгөөд энэ нь ирээдүйн халдлагыг өөгшүүлэх аюултай тул аль болох төлбөрөөс татгалзах нь зүйтэй.

### 3. Кибер аюулгүй байдлын мэргэжилтнүүдтэй зөвлөлдөх (*Consult Cybersecurity Experts*)

Мэргэжлийн кибер аюулгүй байдлын багтай хамтран ажиллах нь халдлагын талаар гүнзгий ойлголт авах, халдлагын эх үүсвэрийг олж тогтоох, сэргээн засварлах, цаашдын халдлагад өртөхөөс сэргийлэхэд тусална.

### 4. Нөөц файлуудаас өгөгдлөө сэргээх (*Restore Data from Secure Backups*)

Байгууллага ransomware халдлагын эсрэг урьдчилан сэргийлэх арга хэмжээ авч нөөц файлуудыг тусад нь хадгалсан бол тэдгээрээс өгөгдлөө сэргээж болно. Энэ нь мэдээллийг хурдан бөгөөд найдвартай сэргээх арга бөгөөд нөөцлөлтийн системүүдийн найдвартай байдлыг баталгаажуулах нь чухал.

### 5. Ирээдүйд хамгаалалтаа бэхжүүлэх (*Strengthen Defenses to Prevent Future Attacks*)

Халдлагад өртсөний дараа хамгаалалтыг сайжруулж, шинэ арга хэмжээнүүдийг нэвтрүүлэх нь дахин халдлагаас урьдчилан сэргийлэхэд чухал үүрэгтэй. Үүнд тогтмол програм хангамжийн шинэчлэлт, ажилтнуудад фишингээс сэргийлэх сургалт явуулах, олон шатлалт нэвтрэлт (MFA) зэрэг аюулгүй байдлын практикуудыг нэвтрүүлэх багтана.

Эдгээр хариу арга хэмжээнүүд нь ransomware халдлагад өртсөн байгууллагуудад хохирлыг багасгаж, мэдээллийн аюулгүй байдлаа сэргээхэд туслах бөгөөд цаашид дахин халдлагад өртөхөөс сэргийлэх боломжийг бүрдүүлнэ.

## VI. ӨГӨГДЛИЙН БЭЛТГЭЛ

### 1. Мэдээлэл цуглуулах:

Ransomware-ийн тодорхой чиглэлийн дата дээр тулгуурлан шинжилгээ хийх учир мэдээлэл цуглуулах шаардлагатай. Өгөгдөлд ransomware-ийн төрлүүд, онцлог шинжүүд, цаг хугацааны тэмдэглэл, өртсөн хохирогчдын байршил зэрэг холбогдох үзүүлэлтүүд багтсан болно.

### 2. Мэдээлэл цэвэрлэх:

Буруу, дутуу эсвэл давхар мэдээллийг арилгах, дундаж утгаар орлуулах.

Алдаатай эсвэл хоосон утгууд: Алдаатай буюу дутуу утгуудыг орлуулах, дундаж утгаар солих эсвэл устгах аргуудыг хэрэглэсэн болно.

Давхардсан мэдээлэл: Өгөгдөлд давхардсан мөр байгаа эсэхийг шалгаж, шаардлагатай бол устгах, солих.

Өөр өөр нэгжтэй утгууд: Өгөгдлүүдийг ижил нэгжид хөрвүүлэх хэрэгтэй (жишээлбэл, хугацааг секундээр эсвэл хоногоор ижил нэгжид илэрхийлэх).

### 3. Мэдээллийн бүтэц сайжруулах

Мэдээллээ тухайн загварт тохируулж өөрчлөх.

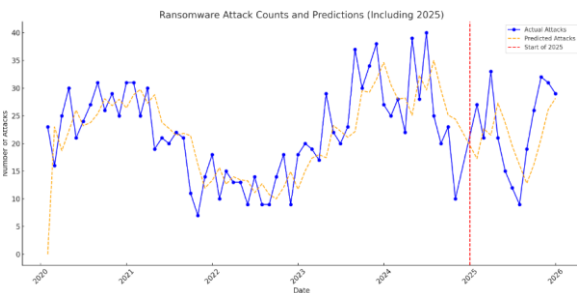
Ангилал болон бүлэглэх: Категорит суурилсан анализ хийх шаардлагатай бол өгөгдлөө ангилж, бүлэглэнэ.

### 4. Шинэ чанар гаргаж авах (*Feature Engineering*):

Шинэ хувьсагчууд үүсгэх: Өгөгдлөөсөө шинэ хувьсагчууд гаргаж авах, жишээлбэл, ransomware-ийн нийт гарсан тоо эсвэл тодорхой хамааралтай хувьсагчуудын нийлбэрийг гаргах.

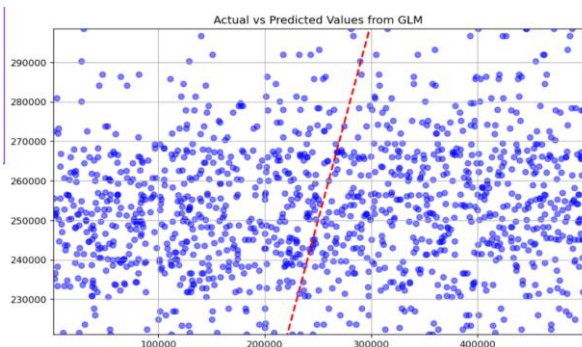


Өмнөх онуудын статик мэдээлэл дээр тулгуурлан 2025 оны мэдээллийг ARIMA загвар ашиглан урьдчилан таамагласан.



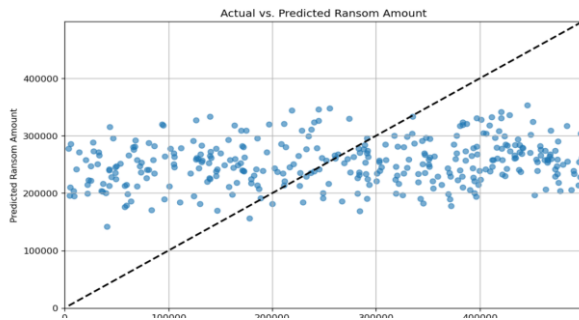
Зураг 7. ARIMA ашиглан ирээдүйг таамагласан.

2025 оны мэдээллийг GLM загвар ашиглан урьдчилан таамагласан.



Зураг 8. GLM ашиглан ирээдүйг таамагласан.

Ransomware халдлагын төлбөрийн чиг хандлага.



Зураг 9. GLM ашиглан өсөлтийн график.

### VII. ДҮГНЭЛТ

Ransomware халдлага нь орчин үеийн байгууллагуудын гол асуудлуудын нэг болж,

кибер аюулгүй байдлын тулгамдсан сорилтыг үүсгэж байна. Энэхүү халдлага нь зөвхөн санхүүгийн хохирол учруулаад зогсохгүй, байгууллагын үйл ажиллагааг тасалдуулж, нэр хүндэд нь ноцтой эрсдэл үүсгэдэг. Судалгааны явцад ransomware халдлагын төрөл, хор уршиг, урьдчилан сэргийлэх болон хариу арга хэмжээнүүдийг нарийвчлан авч үзэж, халдлагын эсрэг урьдчилан сэргийлэх шаардлагыг онцоллоо.

Байгууллагууд ransomware халдлагаас сэргийлэхийн тулд нэгдсэн урьдчилан сэргийлэх арга хэмжээ авах нь зайлшгүй шаардлагатай бөгөөд ажилчдын боловсрол, өгөгдөл нөөцлөлт, хурдан хариу арга хэмжээ авах зэрэг нь хамгаалалтын чухал элементүүд болдог.

Иймд ransomware халдлагыг амжилттай даван туулах, ирээдүйн эрсдэлийг бууруулахын тулд байгууллагууд аюулгүй байдлын хандлагыг байнга хянаж, кибер аюулгүй байдлын системээ тогтмол сайжруулан хөгжүүлэх шаардлагатай байна.

Мөн бид өмнөх онуудын статик мэдээлэл дээр тулгуурлан урьдчилсан таамаглал хийж үзэхэд 2025 онд ransomware-ийн халдлагад 62.5%-д хүрэх магадлалтай байна.

### АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

- [1] Matt Freeman, matt.freeman@hawaiiantel.com “Is there a Yelp for Ransomware?” Incident response planning that does not rely on Plan B. July 18th, 2016
- [2] Justin Harris, justin.r.harris@hotmail.com Family Ties: Multigenerational Ransomware Family Analysis Using Intezer December 15, 2022
- [3] Shafqat Mehmood, shafqat.mehmood@me.com Enterprise Survival Guide for Ransomware Attacks April 30th, 2016
- [4] Anthony Luna, aluna@angrysecurity.com 2021 Ransomware Case Study: Identifying High Priority Security Controls for Public Institutions October 22, 2021
- [5] The State of Ransomware 2024. January-February 2024.
- [6] <https://www.kaggle.com/datasets/hiranomanabu/ransap-2022-ransomware-behavioral-features/>

## САНСРЫН ХОЛБООНЫ СИСТЕМД МАШИН СУРГАЛТЫН АРГЫГ ХЭРЭГЛЭХ БОЛОМЖИЙН СУДАЛГАА

Өнөржаргал ЦЭЛМҮҮН<sup>1</sup>, Баянмөнх БОЛОРЖИН<sup>2</sup>, Рагчаа БАЯРМАА<sup>3</sup>

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбооны технологийн сургууль, Холбооны салбар

*Холбоо барих зохиогчийн и-мэйл хаяг: tselmvvk@gmail.com<sup>1</sup>*

**Хураангуй:** Сансрын холбооны систем олон давуу талтай ба Монгол улсын хувьд ялангуяа хөдөө орон нутагт алслагдал, тархан суурьшсан холбооны үйлчилгээ хүрээгүй газруудад интернэт, харилцаа холбоо зэрэг хэрэгцээнд өөрийн гэсэн хиймэл дагуултай болох нь нууцлал, аюулгүй байдлын үүднээс өндөр ач холбогдолтой. ИТУ (Олон Улсын Цахилгаан Холбоо)-с хиймэл дагуул хөөргөх тодорхой байршлыг дэлхийн улс орон бүрийн хувьд хуваарилсан байдаг ба сүүлийн 10 гаруй жилийн хугацаанд Монгол улс өөрийн хуваарилагдсан байршил болох 113.60E дээр геостационар тойрог замд хиймэл дагуул хөөргөх техник, эдийн засгийн тооцоолол эрчимтэй хийгдэж байна. Үүнтэй холбоотойгоор бид бүхэн инженер, техникийн тооцоо, судалгааны ажил хийх зайлшгүй шаардлагатай билээ. Бид уг судалгааны ажлаараа Монгол улсын хувьд хөөргөх хиймэл дагуулаас Наран (мөн бусад 4) газрын станцын хувьд дохиог найдвартай хүлээж авах шугамын тооцоог хийсэн. Мөн үүнтэй холбоотойгоор борооны унтралтын моделиуд болон атмосферийн нөлөөллийн харьцуулалт хийсэн. Тооцооллоор гаргаж авсан өгөгдөл дээрээ үндэслэн цаашид машин сургалтын аргаар оновчлол хийх нөөц хуваарилалтыг дээшлүүлэх зорилт тавьсан. Уг моделийн тусламжтай газрын станцын нөөц хуваарилалтын үр ашгийг дээшлүүлэх, оновчлол хийх боломжтой болно. Сансрын холбооны системд олон төрлийн хэрэглээнд машин/гүн сургалтын аргыг гүйцэтгэл, үр ашиг, найдвартай байдлыг сайжруулах зорилгоор ашигладаг.

**Түлхүүр үг:** Хиймэл дагуул, шугамын тооцоолол, газрын станц

### I. УДИРТГАЛ (САНСРЫН ХОЛБООНЫ СИСТЕМД МАШИН СУРГАЛТЫН АРГЫГ ХЭРЭГЛЭХ БОЛОМЖИЙН СУДАЛГАА 1)

Олон Улсын Цахилгаан Холбооны Байгууллага-ын Монголын тойрог замын төлөвлөгөөт байрлалууд FSS-113.6° E, BSS-74° E. [1].

Дэлхийн олон орон сансрын холбооны болон тандан судалгааны өөрийн хиймэл дагуулыг олон талт хэрэглээндээ тулгуурлан үр өгөөжтэй ашигласнаар тухайн улсын үндэсний аюулгүй байдал, нийгэм, эдийн засгийн хөгжлийг нь дэмжих томоохон хөшүүрэг болж байна.

Монгол Улсын хэмжээнд холбооны хиймэл дагуулын зурвас ашиглалт сүүлийн 10 жилийн хугацаанд 5.3 дахин нэмэгдэж 338 Мгц-д хүрсэн бөгөөд ойрын 20 жилд энэ нь 3 дахин өсөх хандлагатай байна.

Төрийн болон хувийн хэвшлийн хөрөнгө оруулалтаар орон нутгийг шилэн кабелийн сүлжээгээр холбох ажлыг эрчимтэй хийж байгаа боловч манай орны хувьд өргөн уудам нутаг дэвсгэрт тархан суурьшсан иргэн, өрх бүрт харилцаа холбооны бүх төрлийн үйлчилгээг тэгш хүртээмжтэй хүргэх асуудлыг сансрын холбооны хиймэл дагуул хөөргөснөөр шийдвэрлэх боломж бүрдэх юм.

**“Исатком” ХХК-ийн гүйцэтгэх захирал Ц.Дөлгөөнтэнгис** “Гаднаас түрээсэлж буй зурвасын хэмжээндээ 3.5-4 сая ам.долларыг жилийн хугацаанд түрээсэнд зарцуулж байна. Янз бүрийн бэрхшээлүүд гардаг. Жишээлбэл, тухайн хиймэл дагуулын насжилт, хугацаа дуусаж, үйлчилгээ үзүүлэх боломжгүй болно. Дэлхийн эдийн засгийн хямралтай холбоотойгоор үнэ нэмэх тохиолдлууд ч гарч байна. Энэ бүх асуудал үндэсний хиймэл дагуул хөөрсгөснөөр шийдвэрлэгдэнэ гэж харж байна” гэж

хэлжээ. 2012-2013 оноос эхлэлтэй. Олон Улсын Цахилгаан Холбооны Байгууллага (ОУЦХБ)-аас өгсөн 74°E градус геостационар тойрог замын байрлал, 113.6°E градусын хиймэл дагуулын байрлалд 800Мгц зурвас бий. Үүнээс суурин үйлчилгээ болон өргөн нэвтрүүлгийн үйлчилгээг аль алийг нь хэрэглэгчдэд хүргэхэд 113.6°E байрлал тохирно гэж эрдэмтэн судлаачид үзэж байна. Мөн өөрийн хүссэн байрлалд хиймэл дагуул нисгэхийг хүсвэл өөр улсуудтай тохиролцох, ярилцах асуудал сөхөгдөнө. Энэ бүхэн сансрын задгай орон зайг ашиглах, үр шимийг нь хүртэх тухай ойлголт юм. Өмнө нь сансар судлалыг хөгжүүлэхээр ОХУ-ын “Роскосмос”-той хамтран ажиллах санамж бичиг байгуулжээ. Мөн БНХАУ-тай сансрын техник технологи нэвтрүүлэх, зохион байгуулах, зайнаас тандан судлах, газрын станц байгуулах, Монголд иж бүрэн лаборатори байгуулах, мэргэжилтэн бэлтгэх зэрэг асуудлаар дөрвөн талт гэрээ хийсэн. Үүнийг сансрын техник технологи бүтээх, мэдээлэл боловсруулах эхлэлийн цэг гэж харж, “Үндэсний хиймэл дагуул” хөөргөхөд анхаарал хандуулж байгаа юм. [2]

Бид энэ судалгааны ажлаараа Геостационар Орбитод байрлах сансрын хиймэл дагуул болон газрын станц хоорон дахь шугамын тооцоллыг хийж цаашдаа суваг хуваарилалтанд шинэ технологи машин сургалт ашиглах боломжийн талаар судалж байгаагаараа онцлог.

### II. САНСРЫН ХОЛБООНЫ ДАВУУ ТАЛУУД

1. Өргөн цар хүрээ: Сансрын холбоо нь нэгэн зэрэг өргөн талбайг хамардаг. Энэ нь хөдөө орон нутагт, хүн ам сийрэг орших бүс нутагт ч

хүртээмжтэй байж, хэрэглэгчдэд хурдтай, найдвартай интернет, холбоо барих боломжийг олгоно.

2. Тогтвортой байдал: Хүчтэй байгалийн үзэгдлүүд, газар хөдлөлт зэрэг нь газрын холбооны шугамыг гэмтээж болзошгүй байдаг. Сансрын холбоо нь үүнээс үл хамаарах бөгөөд байгалийн саадгүйгээр мэдээлэл дамжуулах боломжтой байдаг.

3. Өндөр хурдтай мэдээлэл дамжуулалт: Өндөр давтамж дээр ажиллах хиймэл дагуулууд нь хурдтай, чанартай мэдээлэл дамжуулах боломжтой бөгөөд телевиз, интернэт, радио зэрэг төрөл бүрийн үйлчилгээ үзүүлэхэд тохиромжтой.

4. Тохиромжтой өртөг: Газарзүйн хувьд хол байгаа бүс нутагт холбооны дэд бүтэц байгуулахад ихээхэн зардал шаарддаг бол хиймэл дагуулын холбоо нь хямд өртөгтэй, үр ашигтай байдаг.

### III. САНСРЫН ХОЛБООНЫ ОДООГИЙН ХЭРЭГЛЭЭ

Байгаль орчны хяналт, цаг уурын урьдчилсан мэдээлэл дамжуулах тал дээр ч сансрын холбоог ашиглах боломжтой байдаг. Жишээ нь: **"Монголын ус цаг уур, орчны судалгаа"** байгууллага алслагдсан цэгүүдэд сансрын холбоог ашиглан мэдээллээ дамжуулж, цаг агаарын урьдчилсан мэдээг нийтэд хүргэдэг.

Бид энэ судалгааны ажлаараа Наран станц дээр байрлах газрын станц болон хиймэл дагуулын хоорон дахь шугамын тооцоллыг хийж гүйцэтгэнэ. Ингэснээр

1. **Дохионы чанарыг сайжруулах:** Шугамын тооцооллоор дохионы алдагдал, тараалт болон бусад хүчин зүйлийг тооцож, холбооны чанарыг сайжруулж, дохионы алдаг багасгах боломжтой. Энэ нь газрын станц болон хиймэл дагуулын хооронд найдвартай харилцаа тогтоох үндэс суурийг тавина.

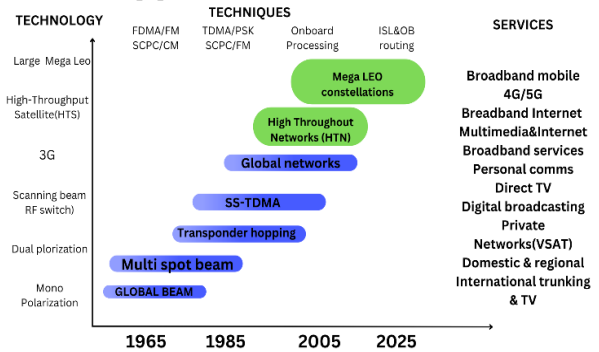
2. **Эрчим хүчний зардлыг оновчтой болгох:** Хиймэл дагуулын эрчим хүчний хэрэглээг оновчтой түвшинд барихад шугамын тооцоолол нь тус дөхөм үзүүлнэ. Үүний үр дүнд дохио илгээх, хүлээн авахад шаардагдах эрчим хүчний зардал буурч, системийн нийт үр ашиг сайжирна.

3. **Интерференцээ сэргийлэх:** Шугамын тооцооллоор холбооны сувгуудын хуваарилалтыг зөв төлөвлөж, бусад дохионоос хөндлөнгийн нөлөөллийг багасгаж, харилцааны тогтвортой байдлыг хангана.

4. **Харилцааны найдвартай байдлыг дээшлүүлэх:** Найдвартай шугамын тооцоолол хийснээр газрын станц болон хиймэл дагуулын хооронд холбоо тасалдах магадлалыг бууруулж, мэдээлэл дамжуулалтын тогтвортой байдлыг нэмэгдүүлнэ. Энэ нь онцгой нөхцөл байдалд ч тасралтгүй харилцаа тогтоох боломжийг хангах юм.

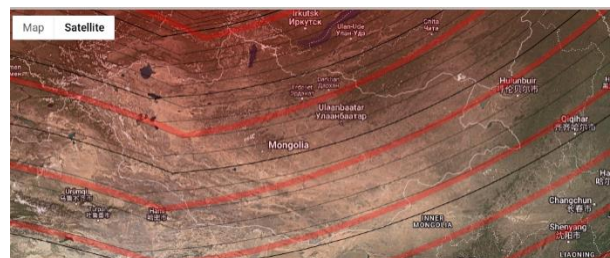
5. **Зардал хэмнэлт:** Урьдчилсан тооцоолол хийснээр, хиймэл дагуул болон газрын станцын тоног төхөөрөмжийн зардлыг багасгаж, урт

хугацааны ашиглалтын зардлыг бууруулах боломжтой[3].

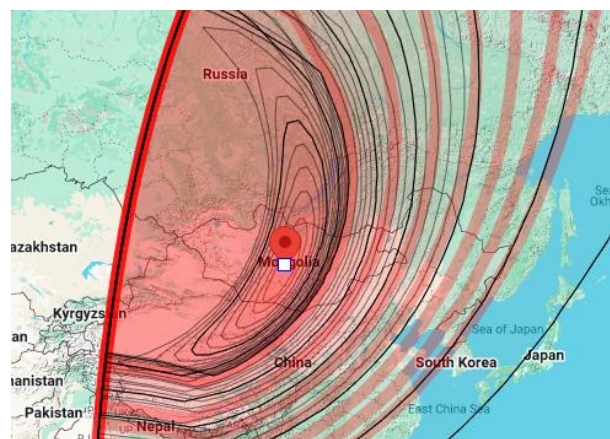


Зураг 1 Сансрын холбооны технологийн хөгжил

**ОБЕГ-ын Мэдээллийн технологийн хэлтсийн дарга, дэд хурандаа Д.Содномрагчаа** “Онцгой байдлын байгууллага бол радио холбоо, үүрэн холбоо, интернэт сүлжээ, Starlink, Iridium зэрэг хэрэгслүүдийг ашиглаж байна. Эдгээр нь өөр өөр байгууллагын үйлчилгээ, зарим нь олон улсын байгууллагын үйлчилгээнүүд юм. Үндэсний хиймэл дагуултай болсноор энэ олон үйлчилгээг нэгтгээд, дотооддоо хөрөнгө оруулах боломжтой” гэв[4].



Зураг 2 Хиймэл дагуулын бүрхэл



Зураг 3 Гео орбит дахь хиймэл дагуулын бүрхэлт 113.6 degree East

Дээрх зургийг [www.satellite-calculations.com](http://www.satellite-calculations.com) ашиглан 113.6 degree East манай улсын хуваарилагдсан зурваст хиймэл дагуулын бүрхэлтийн байдлыг харуулав.

**IV. ГАЗРЫН СТАНЦУУД, ХИЙМЭЛ  
ДАГУУЛЫН БАЙРШЛААС ХАМААРСАН  
ТЕХНИКИЙН ТООЦООЛОЛ**

Сансрын холбооны системийн шугамын тооцоог Монгол улсын хувьд хиймэл дагуулын хуваарилсан байршил болох 113.6<sup>0</sup> болон төлөвлөсөн 5 газрын станцын байршлаас Наран станцын хувьд дараах техникийн өгөгдөл дээр тооцоолол хийлээ.

**СИСТЕМИЙН ӨГӨГДӨЛ**

1-Р ХҮСНЭГТ

Системийн өгөгдөл	Утга
Adjacent system interferer Uplink (dB)	32
Adjacent system interferer Downlink (dB)	32
Тархалтын загвар	Цэлмэг тэнгэр
C/Im satellite downlink (dB)	23
Filtering guard band (MHz)	1
Системийн нөөц түвшин FWD (dB)	1
System margin RTN (dB)	1
Longitude grid step (°)	0.6
Latitude grid step (°)	0.6
Payload uncertainties (dB)	1
Waveform in FORWARD	DVBS2X
Waveform in RETURN	RCS2
Terminal in RETURN	85% of 1.0m terminals 15% of 1.8m terminals

**ХЭРЭГЛЭГЧИЙН ТӨХӨӨРӨМЖИЙН ӨГӨГДӨЛ**

2-Р ХҮСНЭГТ

Хэрэглэгчийн төхөөрөмж	Утга
Антенны диаметр	1.1m
Антенны АҮК (%)	65
Ханалтын EIRP (dBW)	44.5
EIRP тулгуур давтамж (MHz)	13200
XPД	26
Станцын ОВО (dB)	0.5
C/Im (dB)	26
G/T тулгуур давтамж (MHz)	16
G/T (dB/K)	11200
XPI (dB)	26
Хэмжээ	0.9m elliptical (0.8m x 1.1m)

Шугамын тооцооллыг хийхдээ MS-Excel програм дээр шугамын тооцоолол хийх томъёонуудыг ашиглан дараах байдлаар хийсэн.

Сансрын холбооны систем шугамын тооцоо			
Өгөгдөл	Нэгж	Утга	Томъёо
2.4 TO 2.4			
D4	<b>A: Мэдээний өгөгдөл</b>		
D5	Мэдээллийн хурд	2048	
D6	RS кодчил	YES	
D7	RS кодчиллын харьцаа	1.0898	
D8	FEC Code Rate	3/4	
D9	Модуляцийн төрөл	QPSK	
D10	Modulation Factor	2.0	F(D9="BPSK",1:F(D9="QPSK",2:F(D9="msk",1.5,1)))
D11	DEMODO BT PRODUCT	1.30	
D12	BER босго	1.00E-07	
D13	Ев/Но шаардлага	5.80	
D14	Ев/Но Margin/System Margin	dB	1
D15			
D16	Мэдээллийн түвшин	dB	63.11 10*LOG(D5*1000)
D17	Noise Bandwidth	KHz	1933.97 (D5*D7/D8)*D11/D10
D18		dB	62.86 10*LOG(D17*1000)
D19	Дохионы чимээ шуугины харьцаа (C/N)	dB	7.05 (D13+D14)+D16-D18
D20	Дамжуулагчийн зайны фактор		1.10
D21	Carrier Spacing	KHz	2127 D20*D17
D22	<b>B: Зөвгчийн өгөгдөл</b>		
D23			
D24	Uplink давтамж	MHz	13000
D25	Downlink давтамж	MHz	11000
D26			
D27	<b>C: Унтралууд</b>		
D28	Tx Antenna Feeder Loss	dB	0.5
D29	Tx Earth Station Contour	dB	0.0
D30	Tx Antenna Pointing Loss	dB	0.3
D31	Uplink Atmospheric Loss	dB	0.0
D32	Uplink Rain Margin	dB	4.0
D33	Rx Earth Station Contour	dB	0.0
D34	Tx Antenna Pointing Loss	dB	0.3
D35	Downlink Atmospheric	dB	0.0
D36	Downlink Rain Margin	dB	4.0
D37			
D38	Carrier/Interference Ratio	dB	20.0
D39			
D40	Uplink Free Space Loss	dB	206.00 10*LOG(4*3.14159^2/70^2*1000^2/24*1000000/2397000000^2)
D41	Downlink Free Space	dB	204.66 10*LOG(4*3.14159^2/77^2*1000^2/25*1000000/2397000000^2)
D42			
D43	Total Uplink Loss	dB	4.30 SUM(D29:D32)
D44	Total Downlink Loss	dB	4.30 SUM(D33:D36)

**Зураг 3. Шугамын тооцоололд ашиглагдах өгөгдлүүд**

ТООЦООНЫ ХЭСЭГ:			
D82	Constant1:		
D83	SFD Saturation Flux	dB/m^2	-90.00 D48
D84	Gsq Gain 1 sq m Antenna	dB	43.74 10*LOG(4*3.14159^2/024*1000000/2397000000^2)
D85	G/T satellite	dB/K	-2.00 D49
D86	kb BoltzMan Constant		-228.60
D87			
D88	Nb Noise Bandwidth	dB	62.86 D18
D89	Boip Input backoff		10.00 D52
D90			
D91	K1	dB	20.00 D84-D85+D86-D87-D88-D89
D92			99.96 10(D91/10)
D93	Constant2:		
D94	EIRPsat	dBw	40.00 D52
D95	Ls LossDownlink	dB	4.30 D44
D96	Fsl Free Space Path Loss	dB/K	204.66 D41
D97	G/T Earth Station		26.46 D65
D98	kb BoltzMan Constant		-228.60
D99	Nb Noise Bandwidth	dB	62.86 D18
D100	Boop Output backoff		4.50 D53

D128	Nature of Channel		PW LTD	FID127;D126,"BW,LTD","PW,LTD"
D129				
D130	HPA power Calculation:			
D131				
D132	Earth Station EIRP	dBw	57.52	D84-D85+D43+D40-D124
D133	required Per carrier	w	442.93	D121
D134	HPA power per carrier	dBw	8.72	D132-D88+D28
D135		w	7.456	10*(D134/10)
D136	HPA power per carrier	dBw	9.72	D134+1
D137	with 1db Backoff	w	9.386	10*(D136/10)
D138	Calculation for Required No. of Channels			
D139				
D140	Required No. Of Channels		1	
D141		dB	0.00	10*LOG(D140)
D142	Total HPA power	dBw	8.72	D134+D141
D143		w	7.456	10*(D142/10)
D100	Boop Output backoff		4.50	D53
D101				
D102	K2	dB	18.74	D94-D95-D96+D97-D98-D99-D100
D103			74.76	10*(D102/10)
D104	C/N	dB	7.05	D18
D105			5.07	10*(D104/10)
D106	C/IM	dB	20.00	D38
D107			100.00	10*(D106/10)
D108	No of Channels N		8.01	(10*(D105)-1*(D107))/(1*(D92)-1*(D103))
D109		dB	9.04	10*LOG(D108)
D110	C/N Uplink	dB	10.96	D91-D103
D111			12.48	10*(D110/10)
D112	C/N Downlink	dB	9.70	D102-D103
D113			9.33	10*(D112/10)
D114	C/N total		5.07	1*(D111)+1*(D113)+1*(D107)
D115		dB	7.05	10*LOG(D114)
D116				
D117	Max Satellite EIRP	dBw	35.50	D94-D93
D118	Available	w	3548.13	10*(D117/10)
D119				
D120	Satellite EIRP required Per carrier	dBw	26.46	D94-D93-D109
D121		w	442.93	10*(D20/10)
D122		%	12.48	D121*100/D118
D123	Output Backoff per Carrier	dB	13.54	D94-D120
D124	Input backoff per carrier	dB	19.04	D123+D92-D93
D125				
D126	Power BandWidth	KHz	4494.00	D122*(D51*1000)/100
D127	Noise BandWidth	KHz	62.86	D88

Зураг 4: Тооцооллын хэсэг

**V. ТООЦООЛЛЫН ҮР ДҮН**

Монгол Улс өндөрлөг газар байрладаг тул дохио дамжуулах болон хүлээн авах нөхцөлүүдийн хувьд бусад бүс нутгаас өөр байдаг. Өндөрлөг байдал нь дохионы хүчийг хадгалахад сайн нөхцөл болдог хэдий ч цаг уурын өөрчлөлтөөс үүсэх алдагдал харьцангуй их байдаг. Тиймээс Монголд байрлах газрын станцын ашигт ажиллагааг тооцоход дараах хүчин зүйлсийг анхаарч үзэх нь чухал: Уур амьсгалын нөлөө: Монголд цаг агаар их өөрчлөмтгий байдаг тул бороо, цас зэрэг нь дохионы түвшинд нөлөөлөх магадлалтай. Үүнээс үүсэх алдагдлыг (борооны улмаас дохио буурах) тооцож оруулах шаардлагатай. Өндөрлөг газрын нөлөө: Монголын газар нутаг харьцангуй өндөрлөгт байрладаг тул дохионы түвшинг нэмэгдүүлж болно. Гэвч энэ нь өргөн хүрээний дохионы хязгаарлалтад нөлөөлөхгүй байж болох юм.

C/N<sub>0</sub>-ийн үзүүлэлт: Монголд байрлах газрын станцын хувьд C/N<sub>0</sub>-ийн харьцаа өндөр байх нь дохионы чанарыг баталгаажуулахад чухал байдаг. Дээрх үзүүлэлтүүд дээр үндэслэн C/N<sub>0</sub>-ийг тооцоход Монголд тохиромжтой дохионы чанартай ажиллах боломжтой гэж үзэж болно.

G/T: Дохио дамжуулах болон хүлээн авахдаа өндөр G/T-тэй байхад Монголд ашигтай. Дээрх өгөгдөлд G/T нь 15.5 байна. Энэ нь Монголын нөхцөлд хангалттай гэж үзэж болно. Системд ашиглагдаж буй C/N буюу зөөгч шуугианы харьцаа харьцаа 22 дБ байна, энэ нь дохионы чанарын хувьд харьцангуй сайн үзүүлэлт юм.

Хамгаалах зурвас (guard band) нь 0 МГц, энэ нь ойролцоох сувгуудтай хоорондын хөндлөн холболт үүсч болзошгүйг илэрхийлж байна. Хүлээн авах антенны утргтраг, өргөргийн тохиргоо нь 0.6, 0.6 хэмээр тохируулсан, энэ нь харьцангуй ойролцоох байрлалын хэмжээсүүдэд тохируулсан байгааг илэрхийлнэ. 1 метрийн хэрэглэгчийн станцын тохируулга: Антенны диаметр нь 1 метр байна. Ашиглалтын үр ашгийн харьцаа нь 60% байгаа нь дунд зэргийн үр ашигтай ажиллагаатай антен гэж дүгнэж болно. Станцын ОВО буюу дохионы бууруулагдсан хэмжээ 0.7 дБ байгааг харуулж байна, энэ нь өндөр хүчдэлээс шалтгаалсан муруйлтаас сэргийлж байгаа бөгөөд харьцангуй бага алдагдалтай ажиллаж байгааг илэрхийлнэ. G/T буюу системийн ашигт ажиллагааны хэмжүүр нь 15.5дБ/К, энэ нь харьцангуй сайн үзүүлэлт бөгөөд дохионы чанарын хувьд зохих түвшинд байгааг илэрхийлж байна. ХРІ буюу туйлшралын тусгаарлалт нь 25 дБ, энэ нь ойролцоох туйлшралд нөлөөлөл багатай байгааг илтгэнэ.

Харьцуулсан дүгнэлт: Нийт системийн параметрууд дундаж үзүүлэлтүүдээс харьцангуй өндөр байгааг илэрхийлж байна. Хэрэглэгчийн станцын хувьд, 1 метрийн диаметр бүхий антенны үр ашиг дунд зэргийн байгаа бөгөөд дохионы чанарыг хангалттай түвшинд барих чадвартай. Энэ параметрууд дээр үндэслэн системийн ажиллах чадварыг харьцангуй сайн гэж дүгнэж болохоор байна.

**VI. МАШИН СУРГАЛТЫН АРГУУД**

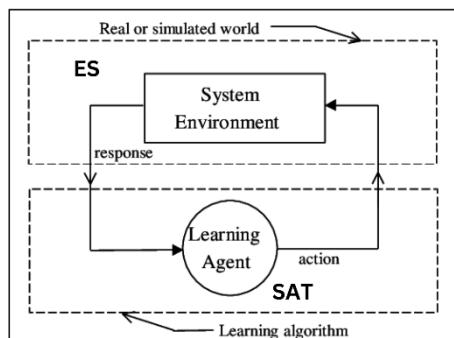
Сувгийн нөөц хуваарилалтыг оновчлоход reinforcement learning (RL) ашиглах нь өндөр үр дүнтэй арга байх боломжтой. RL нь ухаалаг шийдвэр гаргах, системийн гүйцэтгэлийг тасралтгүй сайжруулахад тохиромжтой бөгөөд сувгийн нөөцийн хуваарилалт, ашиглалтанд тохируулан ажиллахад илүү үр дүнтэй байдаг [5].

**Reinforcement Learning**-онцлог: Хувьсах орчинд дасан зохицох RL-ийн гол онцлог нь динамик буюу хувьсамтгай орчинд (жишээ нь, сувгийн ачаалал, өгөгдлийн урсгалын өөрчлөлт, интерференц) дасан зохицох чадвартай байдаг. Энэ нь сувгийн нөөцийн хэрэглээг бодит цаг хугацаанд оновчтой хуваарилах, ачааллын өөрчлөлтийг бодит цагт мэдэрч хариу үйлдэл үзүүлэх боломжийг олгоно.

Өөрөө суралцах: RL агент өөрийн туршлага дээрээс суралцаж, шийдвэр гаргах процессоо тасралтгүй сайжруулж байдаг. Энэ нь сувгийн нөөцийг уламжлалт статик аргуудаас илүү үр дүнтэй ашиглах боломжтой юм.

Оновчтой шийдвэр гаргах: RL нь аливаа шийдвэрийн урт хугацааны нөлөөг тооцоолж ажилладаг тул сувгийн нөөцийг зөвхөн одоогийн ачаалал дээр биш, ирээдүйн ачааллын таамаглал дээр үндэслэн үр дүнтэй ашиглах боломжтой.

**RL ашиглан сувгийн нөөцийн оновчлол хийх үйл явц:**



Зураг 4 Reinforcement Learning ажиллах зарчим

**Төлөв (State):**

Сувгийн ачаалал, дохионы чанар (C/N0), G/T, дамжуулах зурвасын өргөн зэрэг параметруудийг төлөв байдлаар тодорхойлж болно. Монгол улсын нөхцөлд цаг уурын нөлөөлөл болон газрын байрлал (өндөрлөг байдал гэх мэт) ч бас оролцож болох юм.

**Үйлдэл (Action):**

Сувгийн хуваарилалт, өгөгдлийн урсгалын хурдны тохиргоо, дохионы давтамжийг өөрчлөх гэх мэт үйлдлүүдийг гүйцэтгэнэ. RL агент нь аливаа сувгийн ачааллыг бодит цагт зохицуулан, хамгийн оновчтой үйлдлийг сонгоно.

**Шагнал (Reward):**

Шагналын функц нь системийн гүйцэтгэлийг сайжруулах зорилготой байх бөгөөд үүнд сувгийн ашиглалтын үр ашгийг нэмэгдүүлэх, хоорондын интерференцийг бууруулах, сувгийн зөрчилгүй ажиллагааг хангах зэрэг нь орно. Агент нь хамгийн их шагнал авах үйлдлийг сонгож, үр дүнтэй шийдвэр гаргахад суралцана.

**Монголын нөхцөлд RL ашиглах боломжийн давуу талууд:**

Дохионы тогтворгүй байдлыг зохицуулах: Монголд уур амьсгалын өөрчлөлтөөс шалтгаалан дохионы чанар болон сувгийн ачаалал өөрчлөгддөг тул RL агент орчны нөхцөлд тохируулан ажиллаж, сувгийн ашиглалтын үр ашгийг нэмэгдүүлэх боломжтой. Өндөрлөг газрын нөлөөг зохицуулах:

Өндөрлөг газар байрласан станцуудад дохионы интерференц болон сувгийн зөрчил нэмэгдэх магадлалтай. RL агент нь эдгээр нөхцөлийг харгалзан үйлдэл хийж, шаардлагатай үед сувгийн параметруудийг өөрчлөх боломжтой.

**Урт хугацааны оновчлол:**

RL агент нь ирээдүйд гарах өөрчлөлтүүдийг (жишээ нь, нэмэгдэх ачаалал, шинэ хэрэглэгчид холбогдох) таамаглан, урт хугацааны туршид оновчтой шийдвэр гаргах чадвартай.

**Reinforcement Learning загварын төрлүүд:**

Q-learning эсвэл Deep Q-Network (DQN) зэрэг загваруудыг ашиглан сувгийн тохиргоог хийж болно. DQN нь олон параметртэй орчинд ажиллахад тохиромжтой бөгөөд сувгийн тохиргооны нарийн асуудлуудыг шийдвэрлэхэд үр дүнтэй.

**Policy Gradient Methods:**

Энэ аргыг ашиглан агент нь сувгийн хуваарилалтын нарийн хяналт хийх боломжтой. Policy Gradient аргууд нь тасралтгүй орчинд илүү сайн ажилладаг тул сувгийн параметруудийг байнга оновчтой байлгахад ашиглаж болно.

Монголын нөхцөлд сувгийн нөөцийн оновчлолд RL ашиглах нь динамик орчинд тохиромжтой тул сувгийн ачаалал, уур амьсгалын өөрчлөлт, дохионы чанар зэрэг параметруудийг оновчтой удирдах боломжийг олгоно. RL нь урт хугацааны туршид хамгийн их өгөөж өгөх шийдвэр гаргах, өөрөө суралцаж сайжрах давуу талуудтай тул сувгийн нөөцийг илүү үр дүнтэй ашиглах боломжтой. Иймд Монгол улсад байрлах газрын станцын хувьд RL ашиглах нь уламжлалт аргуудаас илүү үр дүнтэй байж, сувгийн ашиглалтын үр ашгийг нэмэгдүүлнэ.

Монгол Улсад байрлах газрын станцын сувгийн нөөцийн ашиглалтыг reinforcement learning (RL) ашиглан хэрхэн сайжруулж, хэр хугацаанд хэдэн хувиар нэмэгдүүлэх боломжтойг тодорхойлохын тулд дараах хүчин зүйлсийг анхаарч үзнэ :

1. RL Моделийг Сургалтын Хугацаа:

Эхний сургалтын үе шат: RL загварыг анх сургаснаар бодит цагт тохируулах, сувгийн ачааллыг таних, хэрэглэгчдийн урсгалын мэдээллийг боловсруулах зэрэгт зориулж эхний суралцах хугацааг шаардана. Энэ нь ихэвчлэн хэдэн долоо хоногоос хэдэн сар хүртэл хугацаа шаарддаг.

Бодит орчинд дасан зохицох:

Загварын сургалт дууссаны дараа бодит орчинд RL агент ажиллаж, өөрчлөгдөж буй нөхцөлд дасан зохицох нь 1–2 сар орчим үргэлжлэх боломжтой. Хурдтай ажилладаг, боловсронгуй алгоритмуудыг ашиглах нь сургалтын явцыг хурдасгах бөгөөд энэ тохиолдолд нийт сургалтын хугацаа 3–6 сарын дотор багтаж дуусах боломжтой.

2. Сувгийн Нөөцийн Ашиглалтын Үр Дүнгийн Нэмэгдэл:

RL аргын давуу тал нь сургалт сайжрах тусам сувгийн нөөцийн ашиглалтыг нэмэгдүүлэх боломжтой байдаг. RL агент нь тасралтгүй суралцаж, оновчлол хийдэг тул системийн нийт үр ашгийг дараах байдлаар нэмэгдүүлэх боломжтой: Эхний 3–6 сар: RL агент системд суурилсны дараа анхны дасан зохицох явцад сувгийн нөөцийн ашиглалтыг 15–20%-иар нэмэгдүүлж боломжтой . 6–12 сарын дараа: RL агент илүү олон мэдээлэл хуримтлуулж, системийн нөхцөлд илүү сайн дасан зохицсоны дараа нийт ашиглалтын үр ашгийг 30–50%-иар нэмэгдүүлэх боломжтой. Урт хугацааны хувьд (1 жилээс дээш): RL агентын суралцах процесс тасралтгүй явагддаг тул 1 жилийн дотор 50%-иас

дээш нэмэгдүүлж, байнгын оновчлол хийснээр урт хугацааны ашиглалт 70%-аас дээш үр ашигтай ажиллах боломжтой гэж тооцогддог.

3–6 сарын дотор RL агент эхний сургалтын үед сувгийн нөөцийн ашиглалтыг ойролцоогоор 15–20% нэмэгдүүлэх боломжтой гэж тооцолж байгаа. Бидний судалгаа одоогоор зөвхөн нэг газрын станц дээрх судалгаа тооцоо бөгөөд цаашдаа уг станц дээрх шугамын тооцоллын жишээгээр бусад станцуудын тооцооллыг хийж. Судалгааны 2 дахь үед RL моделийг сурган симуляцийн туршилтыг хийж гүйцэтгэхээр төлөвлөсөн байгаа.

## ТАЛАРХАЛ

Эрдэм шинжилгээний ажлыг гүйцэтгэхэд хамтран ажиллаж мэдээлэл, туршлагаа хуваалцсан удирдагч багш болон холбооны салбарын багш нартаа талархал илэрхийлж байна.

## НОМ ЗҮЙ

- [1] Otgonbayar Bataa, 2017 “SATELLITE COMMUNICATION IN MONGOLIA” Satellite Symposium, 2017
- [2] <https://mddc.gov.mn/mn/2024/10/19605/> 2024 он
- [3] [www.namem.gov.mn](http://www.namem.gov.mn)
- [4] <https://mddc.gov.mn/mn/2024/10/19605/> 2024 он
- [5] Richard S.Sutton and Andrew G.Barto “Reinforcement Learning: An Introduction” second edition MIT Press,Cambridge, 2018
- [6] Мөн Б.Дамдинсүрэн “Радио Холбооны Тоон Системийн Үндэс” 2000 он
- [7] ММТ 2024 Эрдэм шинжилгээний хурлын эмхтгэл, 2024 он.

# НЭЭЛТТЭЙ ЭХИЙН EDR АШИГЛАН ВИНДӨҮЗ ҮЙЛДЛИЙН СИСТЕМИЙН СҮЛЖЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ

Дэлгэрбатын ЛУВСАННОРОВ<sup>1</sup>, Ганзоригийн АРИУН-ЭРДЭНЭ<sup>1</sup>, Бат-эрдэнийн МӨНХБАЯР<sup>2</sup>

<sup>1,2,3</sup>Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Мэдээллийн сүлжээ, Аюулгүй байдлын салбар

*Холбоо барих и-мэйл хаяг: munkhbayar.b@must.edu.mn<sup>1\*</sup>*

**Хураангуй:** Энэхүү ажлаар нээлттэй эхийн EDR системийг ашиглан хэрхэн өнөөгийн нийгэмд хамгийн их хэрэглэгчтэй виндөүз үйлдлийн систем дэх өдөр тутам илэрж буй олон төрлийн хорт програмд тохирох арга хэмжээ авах нээлттэй эхийн системийг судлаж Мэдээллийн эмзэг байдал, өгөгдлийн аюулгүй байдлыг үнэ төлбөрийн хувьд төрийн байгууллага, их сургууль, дунд хэмжээний борлуулалтын байгууллага зэрэг эмзэг мэдээлэл болон, санхүүгийн мэдээлэл, хувь хүний мэдээллийг агуулдаг объектэд тохирох бодит цагийн мониторинг хийх боломжтой, ослын хариу арга хэмжээ авах чадвартай, халдлагын дараах шинжилгээ, анализ хийдэг, системийн бүтцийн зураглал гарган админ талд илүү ээлтэй байдалтай байх EDR системийг судлан хэрэгжүүлсэн.

**Түлхүүр үг:** кибер халдлага, төгсгөлийн төхөөрөмж, клауд, өгөгдлийн алдагдал, ослын хариу арга хэмжээ

## I. УДИРТГАЛ

Өндөр төвшний кибер халдлагаас үүдсэн аюул заналхийлэл нь төгсөгчийн хамгаалалтын стратегийн шинэчлэл шаарддаг. EDR нь урьдчилан сэргийлэх арга барил бөгөөд энэ нь тасралтгүй хяналт, аюул илрүүлэлт, түргэн хариу үйлдэл хийхэд чиглэгддэг бөгөөд аюултай халдлагуудын нөлөөллийг бууруулахад тусална. Энэ нь төгсөгчийн үйлдлүүдийг бодит цаг хугацаанд хянах боломжийг олгодог бөгөөд ахисан түвшний аналитик болон машин сургалтын алгоритмуудыг ашиглан байгууллагуудад аюул заналхиэлтүүдийг илрүүлж, арилгах боломжийг олгодог. [1] EDR-ийг дэмжих үүднээс EPP нь олон төрлийн хамгаалалтын үйлчилгээг нэгтгэж, төгсөгчийн хамгаалалтыг нэгэн цогц платформоор санал болгодог. Вирусын эсрэг, эсрэг-малтвар, firewall зэрэг аюулгүйн функцүүдийг нэгтгэсэнээр EPP нь төгсөгчийг олон төрлийн аюул заналхаас, үүнд танигдсан вирусуудаас эхлээд шинэ үеийн "zero-day" халдлагуудаас хүртэл хамгаалах боломжийг олгодог. Мөн түүний төвлөрсөн удирдлага, бодлогын хэрэгжилтийн чадвар нь аюулгүй байдлын үйл ажиллагааг илүү хялбаршуулж, нийт аюулгүй байдлын үр ашгийг нэмэгдүүлдэг.[2]

### A. Төгсгөлийн цэгийг илрүүлэх ба хариу үйлдэл үзүүлэх (EDR)

Endpoint Detection and Response (EDR) нь төгсгөлийн төхөөрөмжүүд дээрх дэвшилтэт аюулыг илрүүлэх, судлах, хариу үйлдэл үзүүлэхэд зориулагдсан кибер аюулгүй байдлын багц хэрэгсэл, процессуудыг хэлнэ. Байгууллагууд дижитал технологид улам бүр найдахын хэрээр халдлагын цар хүрээ өргөжиж, уламжлалт аюулгүй байдлын арга

хэмжээг хангалтгүй болгож байна. EDR шийдлүүд нь аюулгүй байдлын багуудад аюул заналыг үр дүнтэй тодорхойлж, бууруулахад нь туслахын тулд бодит цагийн хяналт, мэдээлэл цуглуулах, дүн шинжилгээ хийх боломжийг олгодог.[8]

### B. EDR-ийн үндсэн шинж чанарууд

Тасралтгүй хяналт: EDR хэрэгслүүд нь эцсийн цэгийн үйл ажиллагааг тасралтгүй хянаж, бодит цаг хугацаанд сэжигтэй үйлдлийг илрүүлэх боломжийг олгодог.[4] Аюул илрүүлэх: Машины сургалт, зан үйлийн шинжилгээг ашиглан EDR систем нь аюулгүй байдлын болзошгүй зөрчлийг илтгэж болох гажигийг тодорхойлох боломжтой.

Ослын хариу арга хэмжээ: EDR шийдлүүд нь аюул заналхийллийн эсрэг хурдан хариу арга хэмжээ авах боломжийг олгодог бөгөөд аюулгүй байдлын багуудад ослыг хурдан шуурхай арилгах, арилгах боломжийг олгодог[4].Шүүхийн шинжилгээ: EDR хэрэгслүүд нь эцсийн цэгийн өгөгдлийг цуглуулж, хадгалж, мөрдөн байцаалтад тусалж, байгууллагуудад ослын хамрах хүрээ, үр нөлөөг ойлгоход тусалдаг.

### C. EDR батлах, үр дүнтэй байдлын статистик

Зах зээлийн өсөлт: Дэлхийн EDR зах зээл 2022 онд ойролцоогоор 3 тэрбум доллар байсан бол 2028 он гэхэд 9 тэрбум гаруй доллар болж өсөх төлөвтэй байгаа нь жилийн нийлмэл өсөлтийн хурд (CAGR) 20 орчим хувийг тусгаж байна.[6]

Үрчлэлтийн хувь: 2023 оны судалгаагаар байгууллагуудын 65% нь EDR шийдлийг баталсан нь 2020 онд 45% байсан нь тэдний ач холбогдлыг улам бүр хүлээн зөвшөөрч байгааг харуулж байна.

Үр дүнтэй байдал: Судалгаанаас үзэхэд EDR шийдлийг ашигладаг байгууллагууд зөрчлийг илрүүлэх дундаж хугацааг 60% хүртэл бууруулж, кибер ослын болзошгүй нөлөөллийг мэдэгдэхүйц бууруулж чадна.[5]

*D. Зардлын талаар анхаарах зүйлс*

EDR шийдлүүдийг хэрэгжүүлэх зардал нь байгууллагын хэмжээ, мэдээллийн технологийн орчны нарийн төвөгтэй байдал, тодорхой борлуулагчийн санал гэх мэт хүчин зүйлээс хамаарч өөр өөр байж болно. Ерөнхийдөө байгууллагууд дараахь чиглэлээр хөрөнгө оруулалт хийх боломжтой.

Лицензийн зардал: EDR шийдлүүд нь захиалгын загвар дээр ажилладаг бөгөөд зардал нь эцсийн цэг бүрт сард 20-100 доллар хооронд хэлбэлздэг.

Хэрэгжүүлэлт ба интеграцчилал: Анхны тохиргоо болон одоо байгаа аюулгүй байдлын хэрэгслүүдтэй нэгтгэх нь хэдэн мянгаас хэдэн арван мянган доллар хүртэл нэмэлт зардал гаргах боломжтой.

Сургалт ба боловсон хүчний хангамж: EDR-ийг үр дүнтэй хэрэгжүүлэх нь ихэвчлэн тусгай мэдлэг шаарддаг бөгөөд энэ нь боловсон хүчнийг сургах эсвэл чадварлаг боловсон хүчнийг ажилд авахтай холбоотой зардалд хүргэдэг.

**II. ШАЛТГААН**

Кибер аюул улам боловсронгуй болж байгаа тул байгууллагууд өөрсдийн өвөрмөц орчинд дасан зохицож чадах аюулгүй байдлын найдвартай шийдлүүдийг хайж байна. Trellix EDR гэх мэт өмчийн EDR шийдлүүд нь дэвшилтэт боломжууд болон дэмжлэгийг санал болгодог ч нээлттэй эхийн EDR хэрэгслүүд анхаарал татахуйц давуу талтай байдаг.

1. Зардлын хэмнэлттэй байдал: Нээлттэй эхийн EDR шийдлүүд нь ихэвчлэн лицензийн хураамж авдаггүй бөгөөд энэ нь байгууллагуудад, ялангуяа нөөц багатай жижиг байгууллагуудад илүү төсөвт ээлтэй сонголт болдог. Энэхүү боломжийн үнэ нь бизнес эрхлэгчдэд кибер аюулгүй байдлын бусад чухал салбарт хөрөнгө хуваарилах боломжийг олгодог.

2. Тохируулах боломж: Нээлттэй эхийн EDR нь байгууллагын тодорхой хэрэгцээнд нийцүүлэн програм хангамжийг өөрчлөх, сайжруулах уян хатан байдлыг хангадаг. Энэхүү дасан зохицох чадвар нь байгууллагуудад EDR-ийн үйл ажиллагаа, интеграцчлал, хэрэглэгчийн интерфэйсийг өөрийн үйл ажиллагааны шаардлагад нийцүүлэн тохируулах боломжийг олгодог бөгөөд энэ нь өмчийн шийдлүүдийн хувьд илүү төвөгтэй байж болох юм.

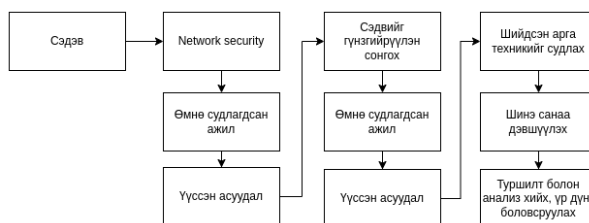
3. Ил тод байдал ба итгэлцэл: Нээлттэй эхийн программ хангамжийн тусламжтайгаар байгууллагууд кодыг сул байгаа эсэхийг шалгаж, далд арын хаалга, хортой бүрэлдэхүүн хэсгүүд байхгүй эсэхийг баталгаажуулах боломжтой. Байгууллагууд шийдлийн бүрэн бүтэн байдал, аюулгүй байдлыг шалгаж чаддаг тул энэхүү ил тод =байдал нь итгэлцлийг бий болгодог.

4. Олон нийтийн дэмжлэг ба хамтын ажиллагаа: Нээлттэй эхийн EDR хэрэгслүүд нь байнгын сайжруулалтад хувь нэмрээ оруулж, дэмжлэг үзүүлдэг хөгжүүлэгч, аюулгүй байдлын мэргэжилтнүүдийн идэвхтэй нийгэмлэгээс ашиг тус хүртдэг. Энэхүү хамтын ажиллагааны орчин нь хурдацтай инновацийг дэмжиж, байгууллага хамт олны хамтын мэдлэгээс ашиг хүртэх боломжийг олгодог.[6]

Энэхүү ажил нь Trellix EDR нь өмчийн шинж чанартай хэдий ч үр ашиг, дасан зохицох чадвар, кибер аюулгүй байдлын стратегид үзүүлэх ерөнхий нөлөөллийн хувьд нээлттэй эхийн EDR шийдлүүдтэй хэрхэн харьцуулж байгааг судлах зорилготой юм. Эдгээр ялгааг судалснаар байгууллагууд өөрсдийн хэрэгцээнд тохирсон EDR аргачлалын талаар мэдээлэлтэй шийдвэр гаргаж чадна.[1]

**III. ХУВЬ НЭМЭР**

Энэхүү ажил нь Trellix EDR-ийн онцлогууд болон гүйцэтгэлийн хэмжүүрүүдэд нарийвчилсан дүн шинжилгээ хийснээр EDR шийдлүүдийн талаарх одоо байгаа мэдлэгт хувь нэмэр оруулдаг. Энэ нь програм хангамжийн хортой програм, ransomware болон дотоод аюул зэрэг янз бүрийн төрлийн аюулыг илрүүлэх, хариу арга хэмжээ авах чадварыг үнэлдэг. Нэмж дурдахад энэхүү судалгаанд Trellix EDR-ийг байгууллагын кибер аюулгүй байдлын стратегид нэгтгэх шилдэг туршлагыг авч үзсэн болно. Энэхүү ажлыг хийж гүйцэтгэхийн тулд доорх зураглалд харуулснаар энэхүү ажлын сэдвийг сонгосон болно.



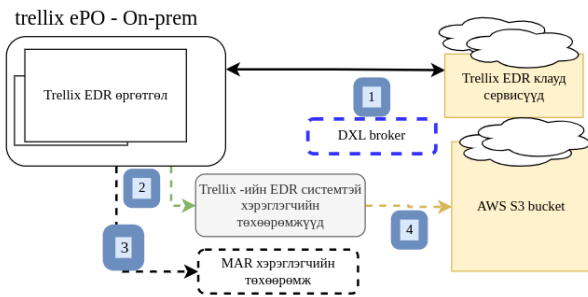
*1-р зураг. Төслийн ажил гүйцэтгэх бүтцийн зураглал*

1-р зурагт сэдэв сонгохын тулд бид сүлжээний аюулгүй байдал гэсэн үндсэн сэдвийн хүрээнд өмнө судлагдсан ажилуудаас ямар техник ба аюулгүй байдлын асуудал үүссэн, тэрхүү асуудлыг шийдхийн тулд ямар арга ашиглах ёстой байгаа вэ? гэх асуулт дээр тулгуурлан энэхүү ажлын сэдвийг сонгосон болно.

*A. Холбоо хамаарал*

Сүлжээний аюулгүй байдал гэдэг нь дотроо маш олон хэсгээс бүрддэг. Бид сүлжээний аюулгүй байдалд дараах зүйлсийг заввал судалсан байх хэрэгтэй учир дараах зүйлсийг судалсан. Үүнд:

1. Firewall - Галт хана
2. IDS болон IPS халдлага илрүүлэх болон хариу арга хэмжээ авах системүүд
3. Antimalware system
4. Encryption - сүлжээний урсгалаар дамжиж буй мэдээллийн бүрэн бүтэн байдал, нууцлагдсан байдал
5. DLP data loss prevention - өгөгдлийн алдагдалаас сэргийлэх систем
6. Security policies - аюулгүй байдлыг бодлого журам
7. Secure communications - аюулгүй холбоос
8. Monitoring - Сүлжээний урсгал, хандалтын лог бүртгэл зэрэг чухал мэдээллийг 24/7 хянаж чадах систем



2-р зураг. EDR ажиллагааны зарчим

**В. Орчин үеийн чиг хандлага**

Бид дээрх сүлжээний түвшинд аюулгүй байдлыг хангах хэд хэдэн сэдвийг судалсны үндсэн дээр эдгээр системүүдийг орлож, нөхөн ажиллах чадвартай бөгөөд зах зээлийн хувьд ээлтэй байх шийдлийг хайсан.

Олж харсан шийдлүүдээс өнөөгийн нийгэмд зардал хэмнэж, хүний ажиллах цаг, зарцуулах зардлыг ч мөн багасгаж чадах систем нь доорх шинж чанартай байгааг анзаарсан.

- Enhanced threat detection /сайжруулсан аюул илрүүлэлт/
- Систем хариуцаж буй админ, мэргэжилтэнд харагдах иж бүрэн байдал
- Осол, аюул занал, зөрчлийн үед хурдан шуурхай мэдэгдэх, хариу арга хэмжээ авах
- Өргөтгөх боломжтой байдал
- Өгөгдлийн алдагдалаас сэргийлэх дүрэм
- Системийн үр ашигтай байдал

**СУДАЛСАН EDR -ИЙН ХАРЬЦУУЛАЛТ**

*1-Р ХҮСНЭГТ*

EDR систем	Үнэ		
	EDR системийн нэр	Хэмжээ (\$)	үнэлгээ 5(max)
1	Trellix EDR	25-100	4.7
2	Crowd strike	8-20	3.9
3	SentinelOne	45-75	3.9
4	Forti EDR	5-15	4
5	Palo Lato Networks Cortex XDR	30-30	4.1
6	cybereason	35-60	3.8

**IV. СУДАЛГАА**

Хүснэгт 1-т үзүүлсэн EDR төрлүүдийн судалгааг хийхдээ тус бүрийг зорилтот хэрэглэгчид буюу их дээд сургуулиуд, дунд болон түүнээс дээш хэмжээний байгууллагын сүлжээнд, эмзэг өгөгдөл байршиж байгаа төрийн байгууллагуудад тохирох EDR -ийг сонгон авах зорилгоор судалсан. Олон төрлийн EDR байгаа хэдий ч төрийн байгууллага болон сургуульд ашиглаж болох нь доор үзүүлэлтүүдээр хязгаарлагдаж байна [2]. Үүнд:

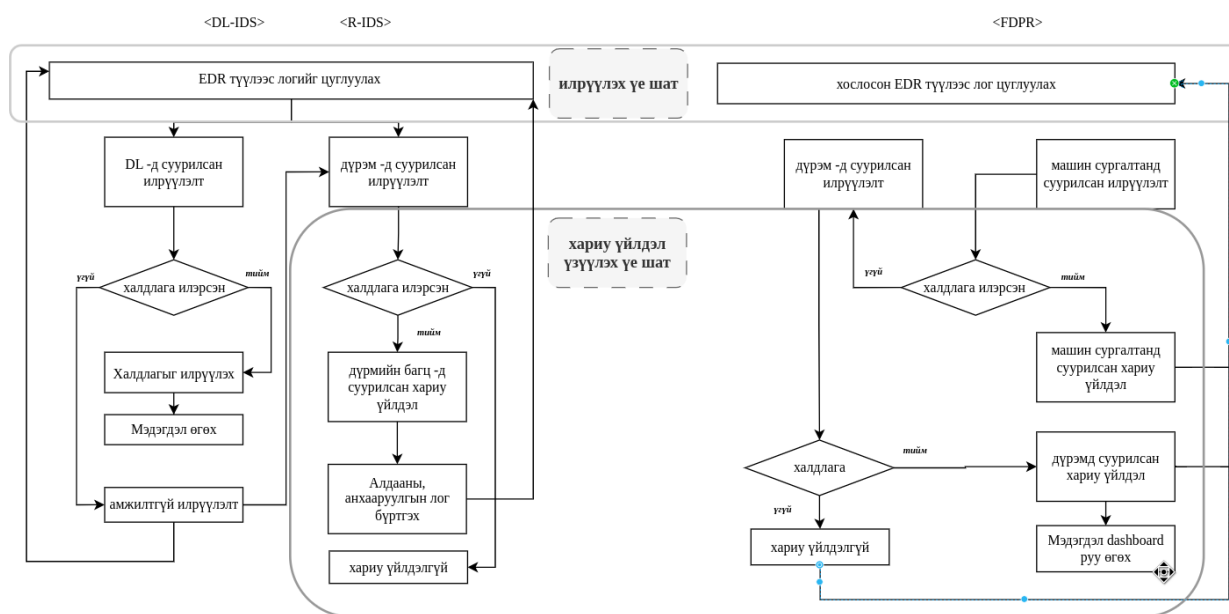
- Үнэ өртөг
- Мэдээллийн төрлөөс хамааран хийж чадах үйл ажиллагаа
- Их хэмжээний төгсгөлийн төхөөрөмжийг нэг дороос хянах
- Хялбар ашиглалт
- Халдлагад хариу арга хэмжээ авах чадавхи
- Сүлжээний загварчлалыг хянах мониторинг
- Систем хариуцан ажиллах хүнд ойлгомжтой зураглал, дүрслэлтэй байх

Энэхүү ажлын хүрээнд бидний сонгон авсан EDR нь дээрх үндсэн шаардлагатай бүрэн нийцэж байна гэж үзэн судалгааны ажлыг Trellix EDR -аар гүнзгийрүүлэн судласан. Юун түрүүнд EDR хэрхэн ажилладаг болохыг ойлгох хэрэгтэй учир дараах бүтцийн зураглалыг гаргасан.

**А. Халдлага илрүүлэх үе шат**

EDR ийн гол зорилго нь халдлага тохиолдсон үед уг халдлагыг илрүүлэн түүнд зориулсан хариу арга хэмжээг авах юм. [10]

Халдлагыг илрүүлэхдээ хамгийн энгийн байдлаар ашиглаж буй EDR систем нь төгсгөлийн төхөөрөмжийн системийн лог мэдээллийг цуглуулдаг байх хэрэгтэй. Хэрэв халдлага илэрвэл хоёр аргаар илрүүлж болно.



3-р зураг. Халдлага илрүүлэх ба хариу үзүүлэх үе шат

1. Өгөгдлийн бүтцэд зөвшөөрөлгүй өөрчлөлт орсон бол тухайн event -ийг халдлага хэмээн бүртгэж EDR -ийн dashboard талбарлуу анхааруулга илгээнэ.[12]

Анхааруулга нь тухайн event -д тохирох статустай байна. Жишээ нь: Informational, Alert, Error, Critical, High гэх мэт.

2. Халдлагын мэдээллийг Өгөгдлийн өөрчлөлтөд суурилсан аргаар илрүүлж чадаагүй өөрөөр тухайн халдлагын шинж чанарыг илрүүлээгүй тохиолдолд дүрэмд суурилсан илрүүлэлтрүү шилжинэ.

Дүрэмийг EDR дээр сүлжээний болон төгсгөлийн төхөөрөмжийн хэрэглэгч дээр тохируулсан бүхий л системд хамааралтай дүрэм гэж ойлгох нь зүйтэй.[3]

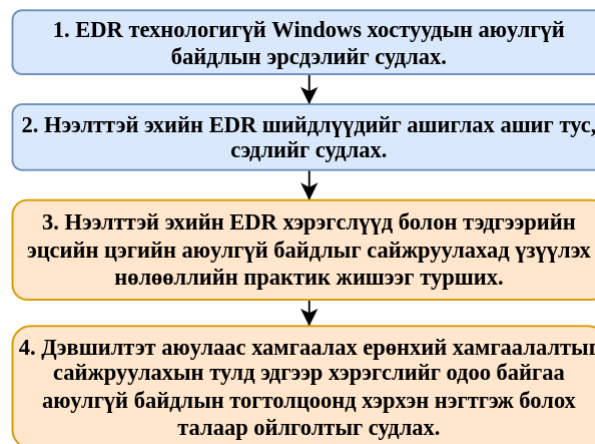
В. Халдлагад хариу арга хэмжээ үзүүлэх үе шат  
Халдлага амжилттай илэрсэн бол EDR систем өөрийн хариу арга хэмжээ авах функц дээр тулгуурлан авах ёстой хариу арга хэмжээнүүдийг хэрэгжүүлнэ. Үүнд:

Бидний сонгосон EDR -ийн халдлага болон ослын үед авах хариу арга хэмжээ нь машин сургалтад суурилсан бөгөөд өмнө нь бүртгэгдэж байсан халдлагуудыг хугацааны хувьд маш хурдан мэдээллэж чадна.

Харин тухайн аюул занал нь шинэ төрөл зүйл бол чадвахи дээрээ тулгуурлан хариу арга хэмжээг авах болно. Ямар хариу арга хэмжээг авах талаар өмнөх илрүүлэлтийн шатанд

гаргасан мэдээлэл дээр тулгуурлан түргэн шуурхай мэдээллэхэд EDR ийн гол чанар оршино.

Дээрх аргачлалыг ашиглаж халдлага, аюул заналд хариу арга хэмжээ авах системийг ажиллагаанд оруулахын тулд доорх схемийг гаргав.



4-р зурагт EDR системийг судлах ажлын дараалал үзүүлэв

1. Эхний хэсэгт бид EDR систем суугаагүй төгсгөлийн төхөөрөмжид учирч болох эмзэг байдалыг судалсан. Үүнд:

А. Халдлагад өртөмтгий байдал нэмэгдсэн

Хортой програм ба Ransomware: EDR байхгүй бол эцсийн цэгүүд нь хортой програм болон ransomware халдлагад илүү өртөмтгий байдаг бөгөөд энэ нь эмзэг өгөгдлийг эвдэж, үйл ажиллагааг тасалдуулж болзошгүй юм.

Фишинг: Хэрэглэгчид фишинг халдлагын золиос болж, зөвшөөрөлгүй хандалт болон өгөгдөл зөрчигдөж болзошгүй.

**В. Аюулыг илрүүлэх байдал байхгүй**

Ул мөр: Мэдээллийн технологийн багууд эцсийн цэгийн үйл ажиллагаанд харагдахгүй байж болзошгүй тул ер бусын зан үйл эсвэл халдлагын анхны шинж тэмдгийг илрүүлэхэд хэцүү болгодог.[14]

Хойшлуулсан хариу арга хэмжээ: Хяналт хийхгүй бол тохиолдлууд удаан хугацаанд анзаарагдахгүй байж болзошгүй хохирлыг нэмэгдүүлнэ.

**С. Ослын хариу өгөх хугацаа**

Гарын авлагын процессууд: Автоматжуулсан илрүүлэлт, хариу арга хэмжээ авахгүй бол ослыг зохицуулах нь гар ажиллагаатай болж, хариу арга хэмжээ авах хугацаа уртасч, нөхөн сэргээх зардал өндөр болно.

Өгөгдлийн алдагдал: Цаг тухайд нь хариу өгөхгүй байх нь өгөгдөл алдагдах, системийн зогсолт, нэр хүндэд хохирол учруулж болзошгүй.

**Д. Зохицуулалт дагаж мөрдөх эрсдэл**

Зохицуулахгүй байх: Байгууллагууд эцсийн цэгийн аюулгүй байдлын зохих арга хэмжээ авалгүйгээр салбарын дүрэм журам, стандартуудыг (жишээ нь, GDPR, HIPAA) биелүүлэхийн төлөө тэмцэж, торгууль болон хууль эрх зүйн асуудалд хүргэж болзошгүй.

Нөөцийн хуваарилалт: Мэдээллийн технологийн багууд аюулгүй байдлын зөрчлийг арилгах, гараар хяналт тавих, нөөцийг бусад чухал төслүүдээс холдуулахад илүү их цаг зарцуулж болно.[11]

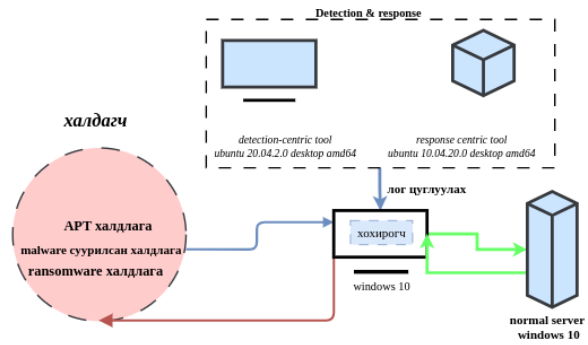
Өндөр зардал: Зөрчлийн нөхөн төлбөр (засах, хууль ёсны төлбөр, нэр хүндэд учирсан хохирол зэрэг) нь EDR шийдлийг хэрэгжүүлэх зардлаас хамаагүй давж гардаг.

**Е. Өгөгдөл зөрчих магадлал өндөр**

Зөвшөөрөлгүй хандалт: EDR-гүй бол нууц мэдээлэлд зөвшөөрөлгүй хандах магадлал нэмэгдэж, улмаар тухайн байгууллага болон түүний үйлчлүүлэгчдэд хохирол учруулах мэдээлэл зөрчигддөг.

Зорилтот халдлага: EDR-гүй байгууллагууд кибер гэмт хэрэгтнүүдийн хялбар бай болж, халдлагад өртөх магадлалыг нэмэгдүүлдэг. [12]

5-р зураг. EDR системгүй үед хийх халдлагын бүтэц



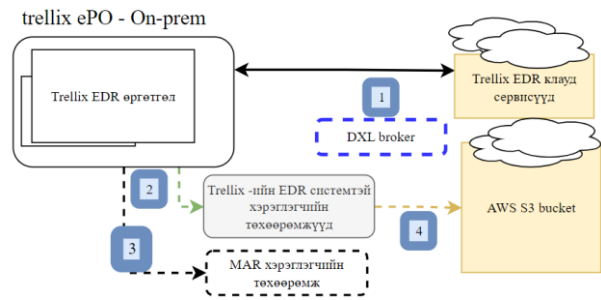
**2. Харин EDR системийг төгсгөлийн төхөөрөмж дээр суурилуулан хянаж эхэлсэн цагаас дараах ашиг тус бий болж эхэлнэ. Үүнд:**

- Хэрэглэгч ямарваа нэгэн файлыг татах үед тухайн файлыг EDR скан хийх ба файлыг устгах, сануулга өгөх(alert), ачааллуулах боломжгүй болгох гэх мэт хариу үйлдэлтэй байна. Ингэснээр хэрэглэгч хүссэн файлаа санаатай болон санаандгүйгээр системд ачааллуулах боломжгүй болно.

- Админ талаас хэрэглэгч бүр дээр суурилсан олон шинж чанар бүхий үйлдлийг хийж гүйцэтгэх боломж бүрдэнэ. Жишээ нь хэрэглэгчийн системд хандах оролдого(нууц үг) бүрийг keylogger ашиглан лог бүртгэлээс хадгалдаг учир хэрэглэгчийн нууц үгийг буруу оруулсан бол лог бичигдэж хандалтыг хаах хүртэл арга хэмжээг авч болно.

- Мөн Trellix EDR нь хэрэглэгчийн зөврийн компьютерийн өгөгдлийн алдагдлаас сэргийлхийн тулд хэрэв гар утас, дижитал камераар дэлгэцийн зураг авах үед тухайн үеийн дэлгэцийн screenshot файл админ талруу alert болон илгээгднэ.

**3. Энэ хэсэгт бид сонгосон EDR-ийн ажиллагааг мэдэж авхын тулд ямар зүйлсүүдийг хамарч ажижлладаг тэдгээр нь яаж EDR-ийг бүрдүүлж байгааг судалсан.**



6-р зураг. Trellix EDR ажиллагааны схем

Зураг 6-т үзүүлснээр EDR-ийн ажиллагааны бүтэц нь зүүн гар талаас:

- trellix EDR систем суусан төгсгөлийн цэгийн extension. Энэхүү төгсгөлийн төхөөрөмж нь ePO(end-point) On-prem(permission is accepted)

буюу дүрэмтэй бөгөөд зөвшөөрөгдсөн үйлдлүүдийг хийх боломжтой.[3]

- DXL брокеруудыг удирддаг системүүд

дээр суулгаж, холбогдсон үйлчлүүлэгчдийн хооронд мессежийг чиглүүлдэг бөгөөд энэ нь үйлчлүүлэгчийг DXL-д үр дүнтэй холбох боломжийг олгодог. Холбогдсон үйлчлүүлэгчдийн жишээ бол Threat Intelligence Exchange модуль, Active Response сервер эсвэл OpenDXL ашигладаг гуравдагч талын бүтээгдэхүүн юм /1 дугаартай холболт/.

- Компьютерийн санах ойн хаягийн

бүртгэл (MAR) нь CPU регистр рүү өгөгдөл дуудах санах ойн хаяг эсвэл системийн автобусаар өгөгдөл илгээж, хадгалах хаягийг хадгалдаг CPU бүртгэл юм.

Өөрөөр хэлбэл, энэ бүртгэл нь заавар гүйцэтгэх үе шатанд санах ойноос өгөгдөл болон зааварт хандахад ашиглагддаг. MAR нь хандах шаардлагатай өгөгдлийн санах ойн байршилыг хадгалдаг. Санах ойноос уншиж байх үед MAR-аар хаяглагдсан өгөгдлийг MDR (санах ойн өгөгдлийн бүртгэл) руу оруулж, дараа нь CPU ашигладаг. Санах ой руу бичих үед CPU нь MDR-ээс MAR-д хаяг нь хадгалагдсан санах ойн байршил руу өгөгдлийг бичдэг. CPU дотор байдаг MAR нь RAM (санамсаргүй хандалтын санах ой) эсвэл кэш рүү ордог.[7]

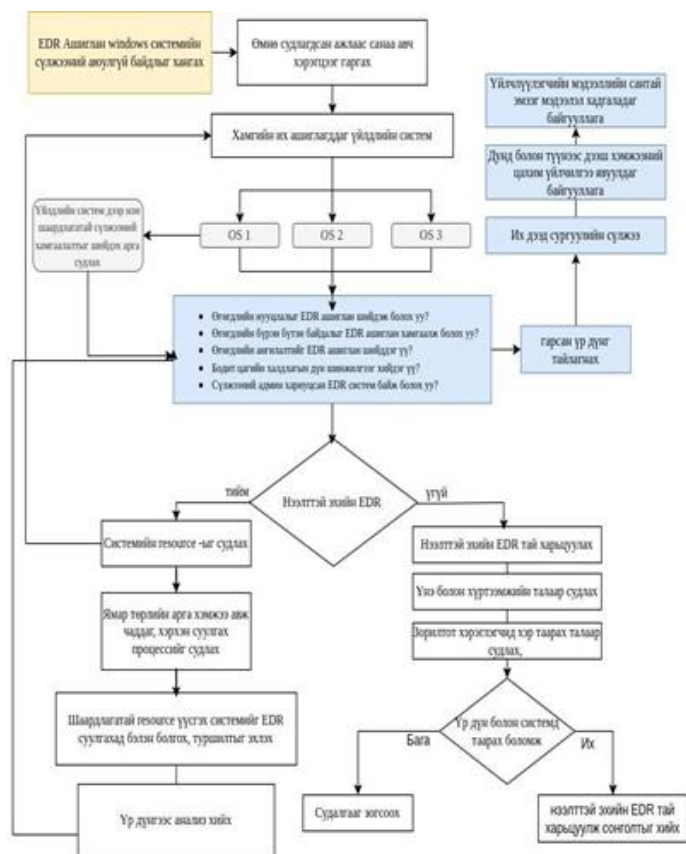
MAR бүртгэл нь микропрограм ба компьютерийн санах ойн хоорондох хамгийн бага интерфэйсийн хагас юм; нөгөө тал нь MDR.

Ерөнхийдөө MAR нь дараагийн санах ойн хаяг, тухайлбал унших эсвэл бичих дараагийн хаягийг агуулсан зэрэгцээ ачааллын бүртгэл юм.(3)

- AWS S3 (Amazon Simple Storage Service)

Bucket нь Amazon Web Services (AWS)-аас хангадаг үүлэн хадгалах нөөц бөгөөд хэрэглэгчдэд хүссэн үедээ ямар ч хэмжээний өгөгдлийг хадгалах, авах боломжийг олгодог.(4)

**V. ТУРШИЛТ**



Энэхүү ажлын туршилтыг хийхэд доорх схемийн дарааллаар хийж гүйцэтгэсэн.

A. Ашигласан хортой программ

Хүснэгт 2-т халдлагын туршилтыг хийхэд ашигласан хорт кодыг харуулав.

**АШИГЛАСАН ХОРТ ПРОГРАМ**

2-Р ХҮСНЭГТ

Хорт програм	EDR систем туршилт		
	нэр	event type	Файл
1	shinoLocker	process	.exe
2	Winword	process	.exe
3	procdump	process	.exe
4	ThreatSample	process	.exe
5	Powershell	process	.exe
6	whoami	process	.exe

**ShinoLocker.exe:** Энэ нь 2021 оны 5-р сард DarkSide кампанит ажилд ашиглагдаж байсан алсын зайнаас хуулбарлах хэрэгсэл.

**Тактик ба техник:** Spear phishing Link T1192 (Анхны хандалт) энэ файлыг Endpoint Protection шийдлээр

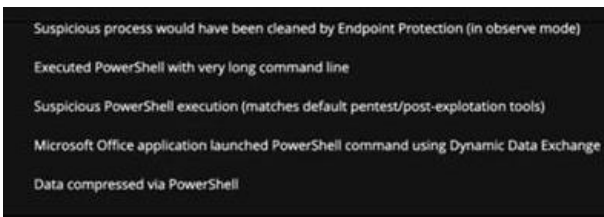
эцсийн цэгийн podclient2 дээр ажиллахыг амжилттай хаасан.

**Winword.exe:** Төхөөрөмж (төгсгөлийн цэгүүдэд нөлөөлсөн) — хохирогч1.

**Тактик ба техник:** Dynamic Data Exchange T1173

Spearg фишинг хавсралт T1193 (Анхны хандалт)

Файл эсвэл мэдээллийн кодыг тайлах T1140 (Батлан хамгаалахаас зайлсхийх Microsoft Оффис програм нь Dynamic Data Exchange (DDE) ашиглан PowerShell командыг эхлүүлсэн. Динамик өгөгдлийн солилцоо (DDE) технологи нь програмууд хоорондоо харилцах, санах ойг хуваалцах боломжийг олгодог. Энэ технологийг олон жилийн турш халдлагын вектор болгон ашигладаг. Тушаалын



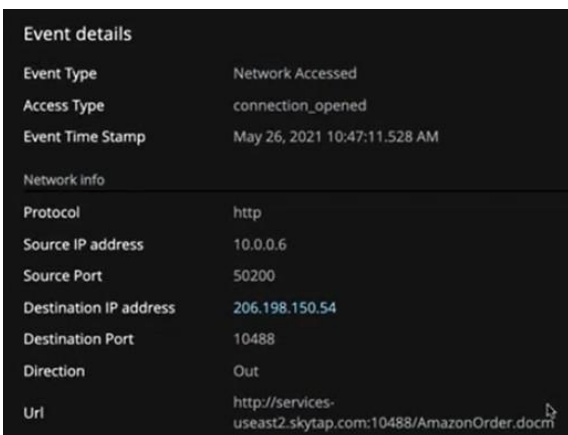
7-р зураг. Powershell.exe аюулын мэдээлэл

мөр бүхий PowerShell-ийг гүйцэтгэсэн. PowerShell-ийн сэжигтэй гүйцэтгэл гэх мэт.

**Powershell.exe:**

PowerShell.exe-ийн гүйцэтгэлийн талаархи нэмэлт судалгаа нь PowerShell.exe-г ажиллуулахаас өмнө сүлжээний холболт үүссэн болохыг үйл явдлын дэлгэрэнгүй харуулж байна. Үйл явдлын дэлгэрэнгүй мэдээлэлд дараахь сэжигтэй үйлдлүүд ажиглагдаж байна.

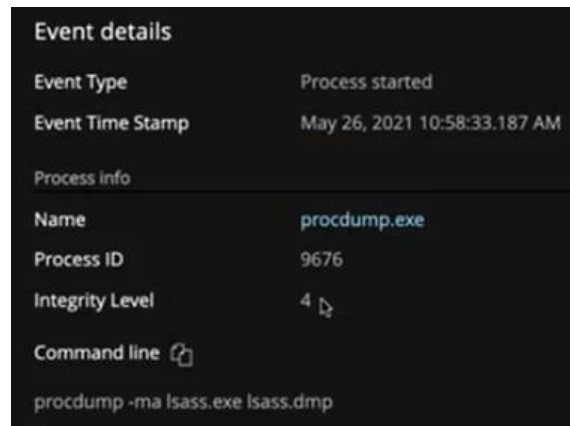
- Стандарт бус очих порт (10488) ба гадагш чиглэсэн холболт.
- Гүйцэтгэсэн URL нь AmazonOrder.docm байсан
- AmazonOrder.docm файл гадаад түгээлтийн серверээс татаж авсан.



8-р зураг. Халдлага болсон event харагдах байдал

**procdump.exe:**

Procdump.exe процессыг бүрэн бүтэн байдлын 4-р түвшнээс эхлүүлсэн. Халдагч нь нэрлэсэн дүр эсгэх аргыг ашиглан зөвшөөрлийн түвшинг дээшлүүлж чадсаныг харуулж байна. Ихэвчлэн Svchost.exe нь өшиглөх үүрэгтэй унтраах UAC хяналтууд, хэрэв ямар нэгэн UAC bypass эсвэл UAC хүлээн зөвшөөрөлт байгаа бол Svchost.exe гинжээр дамжиж байсан.



9-р зураг. Хохирогчийн 24 цагийн халдлагад өртсөн мэдээлэл

Зураг 9. Цагийн мэдээллийг EDR тохируулсан систем дээр UTC горимоор тохируулаагүй учир цаг тухайн систем нээгдсэн цагаар ажиллаж байна.

Халдагч системд Procdump.exe дуудлагын процесс эсвэл үйлчилгээний процессыг Svchost.exe-тэй ижил түвшинд хүргэхийн тулд Svchost.exe-г нэрлэсэн хоолой руу холбох тушаал. Svchost.exe процесс нь үргэлж бүрэн бүтэн байдлын 4-р түвшинд ажилладаг. Тиймээс Procdump.exe процесс нь мөн адил бүрэн бүтэн байдлын түвшинд хийгддэг.

В. ХАЛДЛАГЫН ХАРИУ АРГА ХЭМЖЭЭ

Өмнөх хэсэгт үзүүлсэн хортой програмууд дээр EDR систем нь хэрхэн хариу арга хэмжээ авах зааврыг хавсралт хэсэгт оруулсан гарын авлагаар дэлгэрэнгүй харуулсан. ShinoLocker.com домайныг IP-ээр сонгож ShinoLocker.com домэйн нэр дээр үндэслэн энэ домэйн нэр сэжигтэй харагдаж байна. Нэмэлт судалгаа хийхийн тулд IP хаягийг Нотлох Тэмдэглэлд хуулж, буулгаж болно.

Төгсгөлийн цэг болон гадаад орчны хооронд үүссэн залгуурыг судлахын тулд Shinolocker.com нэртэй DNS хүсэлтийн дүрсийг сонго. Нэр хүнд дээр дарвал домэйн нэрний Trellix GTI нэр хүндийг Өндөр эрсдэлтэй гэж харуулна.

Та орчин тойрныхоо төгсгөлийн цэг нь гадаад орчинтой холбоотой гэдгийг мэдэж байгаа тул та сэжигтэй үйл явцын хүрээлэн буй орчны нөлөөллийг судлах боломжтой.[8]

А. Сэжигтэй үйл явцын хүрээлэн буй орчинд үзүүлэх нөлөөг судлах

Trellix EDR Судалгааны гарын авлага нь хүрээлэн буй орчинд сэжигтэй үйл явцын нөлөөллийг судлахад тусалсан. Энэхүү функц нь олох сэжигтэй файл байгаа төгсгөлийн төхөөрөмжийн



10-р зураг. shinolocker.exe сүлжээнд орсон хаяг

тоо файлын орчинд илэрсэн зураглалыг гаргана. График харахыг сонгон хурдан харах боломжтой өртсөн PuttyXs.exe сэжигтэй процессын улмаас төгсгөлийн цэгүүдийн График харагдац нь төгсгөлийн цэгүүд болон зангилаа хоорондын хамаарлыг өрөмдөж үзэхэд тусалдаг. Эдгээр зангилааны заримын хооронд шугаман хамаарал байдаг бөгөөд тэдгээр нь гол олдворууд болон онцолсон байдаг.

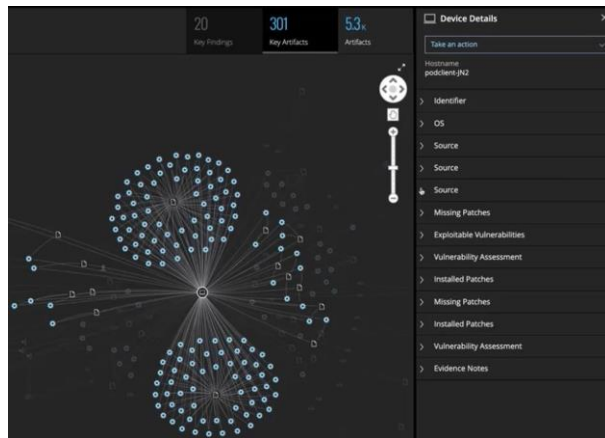


11-р зураг. График үзүүлэлт

Мөрдөн байцаалтад дурдсан эцсийн цэгийн нэрийг харахын тулд компьютерийн дүрс дээр дарна уу. Энэ тохиолдолд эцсийн цэгийн нэр нь podclient—JN2 байна.

*В. Төгсгөлийн агшин зуурын өгөгдлийг ашиглан судалгааг баяжуулах*

Төгсгөлийн цэгийн агшин зуурын зургийг авах үйлдлийг дуусгасны дараа одоо байгаа мөрдөн байцаалтын талаар мэдээлэл бөглөх ба дараах өөрчлөлтүүд хийгдэнэ.



12-р зураг. Төгсгөлийн төхөөрөмжийн зураглал

- Мөрдөн байцаалтын удирдамжийн шинэ асуултуудад хариулт авах боломжтой.
- Мөрдөн байцаалтын гарын авлагын одоо байгаа хариултууд илүү их мэдээллээр баяжуулагдсан.
- Илүү олон гол олдворууд болон олдворуудыг харж эхэлнэ. Өөрчлөлтүүд нь илүү их өгөгдөл орж ирэхэд тохиолддог бөгөөд үүнийг дэмждэг хиймэл оюун ухаан.

**VI. ДҮГНЭЛТ**

Trellix EDR нь орчин үеийн кибер аюулгүй байдлын стратегид зайлшгүй шаардлагатай төгсгөлийн цэгийг илрүүлэх, хариу үйлдэл үзүүлэх найдвартай тогтолцоог бүрдүүлдэг. Бодит цагийн аюул заналыг илрүүлэх, автомат довтолгоонд хариулах чадвар нь байгууллагын аюулгүй байдлын байр суурийг ихээхэн сайжруулдаг. Машин сургалтын дэвшилтэт алгоритмууд болон зан үйлийн аналитикийг ашигласнаар Trellix EDR нь гажуудал болон болзошгүй аюулыг өндөр нарийвчлалтайгаар тодорхойлж, хуурамч эерэг үр дүнг багасгаж, аюулгүй байдлын баг жинхэнэ аюул заналхийлэлд анхаарлаа төвлөрүүлэх боломжийг олгодог.

Платформын ослын хариу арга хэмжээ нь илэрсэн аюулыг хурдан дарж, арилгахад тус дөхөм болж, байгууллагын орчинд дайсны оршин суух хугацааг багасгадаг. Нэмж дурдахад, Trellix-ийн аюулгүй байдлын мэдээлэл, үйл явдлын менежментийн (SIEM) системүүдтэй нэгтгэсэн нь бүх төгсгөлийн цэгүүдэд иж бүрэн харагдах боломжийг олгож, байгууллагууд шинээр гарч ирж буй аюул заналхийлэлд идэвхтэй хариу үйлдэл үзүүлэх боломжийг олгодог.

**VII. АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ**

[1] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yılmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.

[2] Furdek, M., Natalino, C., Lipp, F., Hock, D., Giglio, A. D., & Schiano, M. (2020). Machine learning for optical network security monitoring: A practical perspective. *Journal of Lightwave Technology*, 38(11), 2860-2871.

[3] Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yılmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1334.

[4] Furdek, M., Natalino, C., Lipp, F., Hock, D., Giglio, A. D., & Schiano, M. (2020). Machine learning for optical network security monitoring: A practical perspective. *Journal of Lightwave Technology*, 38(11), 2860-2871.

[5] Katulić, F., Groš, S., Sumina, D., & Erceg, I. (2024, March). Enhancing Industrial Automation and Control Systems Cybersecurity Using Endpoint Detection and Response Tools. In *International Conference on Science and Technology Education* (pp. 186-197). Cham: Springer Nature Switzerland.

[6] Dong, F., Li, S., Jiang, P., Li, D., Wang, H., Huang, L., ... & Chen, X. (2023, November). Are we there yet? an industrial viewpoint on provenance-based endpoint detection and response tools. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2396-2410).

[7] Kaur, H., SL, D. S., Paul, T., Thakur, R. K., Reddy, K. V. K., Mahato, J., & Naveen, K. (2024). Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. In *E3S Web of Conferences* (Vol. 556, p. 01006). EDP Sciences.

[8] GEORGE, D. A. S., George, A. H., Baskar, T., & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*, 8(1), 493-501.

[9] Mocanu, B. C., Stoleriu, R., Mocanu, A. E., Negru, C., Drăgoțoiu, E. G., Moisescu, M. A., & Pop, F. (2024, March). NextEDR-Next generation agent-based EDR systems for cybersecurity threats. In *2024 32nd Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP)* (pp. 183-190). IEEE.

[10] Karmakar, G., Thakkar, U. D., & Kashid, S. (2024). Leveraging Cyber Hunt and Investigation on Endpoints Using Elastic XDR/EDR. In *Computer Science Engineering and Emerging Technologies* (pp. 466-471). CRC Press.

[11] Udipi, S. (2021). The event data management problem: getting the most from network detection and response. *Network Security*, 2021(1), 12-14.

[12] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. *Procedia Computer Science*, 48, 503-506.

[13] Aydın, M. A., Zaim, A. H., & Ceylan, K. G. (2009). A hybrid intrusion detection system design for computer network security. *Computers & Electrical Engineering*, 35(3), 517-526.

[14] Wolf, W., White, G. B., Fisch, E. A., Crago, S. P., Pooch, U. W., McMahon, J. O., ... & Lebak, J. M. (2017). Computer system and network security. CRC press.

[15] Stott, B., & Marinho, J. L. (1979). Linear programming for power-system network security applications. *IEEE Transactions on Power Apparatus and Systems*, (3), 837-848.

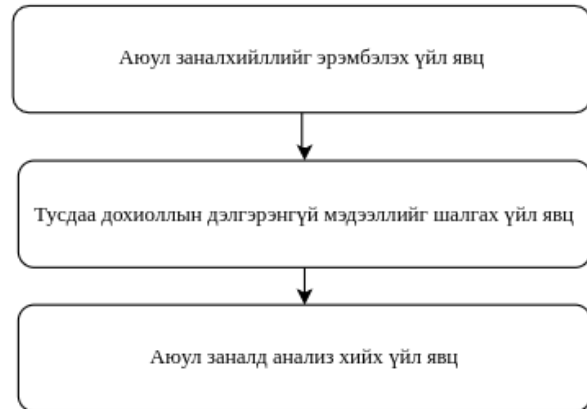
[16] Cho, Y. H., & Mangione-Smith, W. H. (2005, June). A pattern matching coprocessor for network security. In *Proceedings of the 42nd annual Design Automation Conference* (pp. 234-239).

[17] Lippmann, R. P., Ingols, K. W., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M., & Cunningham, R. (2005). Evaluating and strengthening enterprise network security using attack graphs. *Project Report IA-2, MIT Lincoln Laboratory*.

[18] Bejtlich, R. (2013). *The practice of network security monitoring: understanding incident detection and response*. No Starch Press.

**VIII. ХАВСРАЛТ**

**Аюул заналхийллийг хянах(monitoring)**



**Trellix EDR ашиглах тохиолдол**

