ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

ДОКТОР, ПРОФЕССОР Г.ЦОГБАДРАХЫН НЭРЭМЖИТ

“МЭДЭЭЛЭЛ, ХОЛБООНЫ САЛБАРЫН ХӨГЖИЛД БИДНИЙ ГҮЙЦЭТГЭХ ҮҮРЭГ”

2025-2026 ОНЫ ХИЧЭЭЛИЙН ЖИЛИЙН НАМРЫН УЛИРЛЫН МАГИСТР, ДОКТОР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ХУРЛЫН ЭМХЭТГЭЛ

№25(18)365

УЛААНБААТАР ХОТ

2025 ОН

ШИНЖЛЭХ УХААН, ТЕХНОЛОГИЙН ИХ СУРГУУЛИЙН

МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

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

ЭРДЭМ ШИНЖИЛГЭЭНИЙ БҮТЭЭЛИЙН ЭМХЭТГЭЛ

№ 25(18)365

УЛААНБААТАР ХОТ
2025 ОН

ISSN 1560-8794

Бүтээлийн эмхэтгэл хянан магадалсан:

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

MONGOLIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

SCIENTIFIC TRANSACTIONS

№ 25(18)365

ULAANBAATAR 2025

ГАРЧИГ

ДОКТОР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

МАГИСТР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

ХҮНИЙ ХУВИЙН ОРОН ЗАЙД ХАЛДАХГҮЙ ӨДӨР ТУТМЫН ҮЙЛДЛИЙГ ТАНИХАД ЗОРИУЛСАН ӨГӨГДӨЛ, ЗАГВАРУУД

Бадарчийн ЛУУБААТАР[1], Бямбаагийн ДОРЖ[1], Гочоогийн МӨНХЖАРГАЛ[2]

[1]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Электроникийн тэнхим

[2]Арабын Нэгдсэн Эмират Улс, Аль-Айн, Арабын Нэгдсэн Эмират Улсын Их Сургууль, Компьютерийн ухаан, програмчлалын тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: luubaatar@must.edu.mn[1]

***Хураангуй*: Энэхүү судалгааны ажлаар бид 74 оролцогчийн гүйцэтгэсэн 19 төрлийн үйлдлийг инфра улаан (IR) матрицан мэдрэгчүүдээр цуглуулж, уг өгөгдөл дээр R(2+1)D-18, MViTv2, Swin-T зэрэг гүн сургалтын (convolutional болон transformer) загваруудыг сургаж үр дүнг харьцуулсан. Өгөгдлийн сан дахь бичлэгийн дээж бүрийг 32×32×32 хэмжээтэй дулааны тенсор шоо үүсгэхээр зохиойн байгуулж куб хэлбэртэй болгосон. Энэ өгөгдлийн сан нь бусад ижил төрлийн өгөгдлийн сангуудаас илүү олон үйлдэл, хоёр дахин олон мэдрэгч, гурван дахин олон оролцогчтой гэдгээрээ онцлог юм. 8×8 нягтаршилтай есөн ширхэг IR дулааны мэдрэгчээр хүний үйлдлийг бичиж авсан тул хувь хүний орон зайд халдалгүйгээр үйлдлийг таних боломж олгоно.**

Бидний туршилтын хүрээнд хангалттай өндөр үр дүн гарч ийм төрлийн мэдрэгчээр бичсэн өгөгдлөөс орчин үеийн гүн сургалтын аргуудыг ашиглан хүний өдөр тутмын үйлдлийг (ӨТҮ) таних боломжтойг харууллаа. R(2+1)D-18 загварын F1-score нь 0.852 хүрсэн нь хамгийн өндөр үр дүн байлаа. MViTv2, Swin-T зэрэг transformer загварууд нь гар хөлийн хөдөлгөөнийг илэрхийлэх жижиг цэгийн хөдөлгөөнийг үр дүнтэй ялгаж байна.

Энэхүү өгөгдлийн сан болон харьцуулсан үнэлгээ нь бага нягтаршилтай, хүний хувийн орон зайд халдахгүйгээр хүний үйлдэл таних судалгааны чиглэлд дорвитой нөлөө үзүүлэхүйц ажил болсон бөгөөд цаашид хөгжүүлснээр ахмад настны асаргаа, өвчтөний хяналт, ухаалаг гэр гэх мэт хэрэглээнд өргөнөөр хэрэглэж болох юм.

Түлхүүр үг: Хэт улаан туяаны матрицан мэдрэгч, Хэт улаан туяаны зураг, үйлдэл таних, гүн сургалт, трансформер загвар, хувийн орон зайд халдахгүйгээр мэдрэх

I. УДИРТГАЛ (10PT, BOLD)

Дэлхийн хүн ам болон дундаж наслалт нэмэгдэхийн хэрээр ахмад настнуудын эзлэх хувь эрс өсөж байна [1]. 2020 онд 60 ба түүнээс дээш настай хүмүүсийн тоо 5-аас доош насны хүүхдүүдийн тооноос давсан [2, 3]. Үүнээс улбаалаад сүүлийн хэдэн арван жилд ганцаар амьдарч буй ахмад настнуудын тоо эрс өссөн [4]. Энэ чиг хандлага нь тэднийг бие махбодын болон сэтгэлзүйн гэмтэлд өртөх эрсдэлийг нэмэгдүүлж, цаг тухайд нь тусламж авч чадахгүй байдалд хүргэж байна [5, 6]. Гэр бүлийнхэнтэйгээ хамт амьдарч буй ахмад настнууд ч бас заримдаа гэртээ ганцаар үлддэг бөгөөд яаралтай тусламж шаардлагатай нөхцөл үүсэхэд гэр бүлийнхэн нь мэдэхгүй байх тохиолдол түгээмэл байна [7]. Үүний улмаас ганцаараа амьдарч буй ахмад настнуудыг хянах системийн судалгаа хөгжүүлэлтл сүүлийн жилүүдэд ихээхэн анхаарал татаж байна [8, 9].

Камерийн систем нь ахмад настнуудыг гэрт нь хянах хамгийн үр дүнтэй хэрэгслүүдийн нэг юм. Гэхдээ RGB камер нь хүний байрлал, хөдөлгөөний талаар нарийвчилсан мэдээлэл өгдөг ч өндөр нягтаршилтай дүрс бичлэгийн улмаас хувийн орон зай, хувийн нууцлалыг хөнддөг [10]. Үүнийг шийдвэрлэхийн зорилгоор гүний камер ашигладаг [11]. Жишээ нь хувийн мэдээллийг бага хөндөх ба ахмад настны явганаас унахыг илрүүлэх хяналтын системийг хөгжүүлэхэд ашиглаж байна [12]. Хэдийгээр гүний камер нь RGB камертай харьцуулахад хүний дүрслэлийг арай бүдэг харуулдаг ч зарим тохиолдолд нүүр ч таних боломжтой хэвээр байдаг тул нууцлалын эрсдэл бүрэн арилдаггүй [13].

Өндөр нарийвчлалтай тасралтгүй өгөгдөл цуглуулж чаддаг бөгөөд хэрэглэгчийн хувийн мэдээллийг ил гаргахгүй нэг арга нь биед зүүдэг төхөөрөмжүүдийг хэрэглэх юм [14, 15]. Хэдийгээр зүүдэг төхөөрөмж нь хүний ӨТҮ илрүүлэхэд сайн мэдрэгч болж чадах ч зүүхэд эвгүй, байнга цэнэглэх шаардлагатай, унтаж байхдаа хэрэглэхэд тохиромжгүй зэрэг сул талуудтай [16].

Хаалганы мэдрэгч, хөдөлгөөний мэдрэгч, даралт, усны мэдрэгч зэрэг орчны мэдрэгчүүдийг ашиглан ӨТҮ-ийг хянах нь боломжийн шийдэл болж байна [17]. CASAS төслийн Aruba өгөгдлийн санг ашиглан Yatbaz нар ӨТҮ таних нарийвчлалыг сайжруулсан [18, 19]. Гэвч эдгээр хоёртын буюу тийм/үгүй гаралттай мэдрэгчүүд нь ихэвчлэн маш бага нарийвчлалтай мэдээллээр хангадаг тул ӨТҮ-ийн нарийн ялгаатай үйлдлүүдийг илрүүлэх чадвар хязгаарлагдмал байдаг [17, 20].

Дулааны камер нь өндөр нарийвчлалтай, хүний бүдэг дүрс харуулдаг, зүүдэг бус шийдэл юм [21, 22]. Гэхдээ дулааны камерын үнэ өндөр, зарим тохиолдолд гүний камерийн адил хүний дүрс хэлбэрийг тод харуулдаг тул илүү хямд, хувийн нууцлалыг хамгаалсан хувилбар болох бага нягтаршилтай инфра улаан (IR) матрицан мэдрэгчийг

ашиглах нь илүү тохиромжтой. Эдгээр мэдрэгч нь хямд өртөгтэй, маш бага нягталтай тул хүнийг бараг таних боломжгүй тойм дүрс гаргадаг ч гүн сургалтын аргуудыг ашиглан ӨТҮ таних боломжтой юм. Бидний өмнөх ажилд бид өөрсдийн өгөгдлийн сан дээр transformer загвар сургаж, ӨТҮ танихад сайн үр дүн үзүүлж байсан [23]. Олон судалгаанд HMM, SVM, KNN зэрэг уламжлалт машин сургалтын аргуудыг ӨТҮ танихад ашигласан байдаг [24, 25, 26, 27]. Гэвч сүүлийн жилүүдэд гүн сургалтын загваруудын хөгжил ӨТҮ танилтын гүйцэтгэлийг эрс сайжруулсан [28, 29, 30].

Манай судалгааны ажил нь орчин үеийн гүн сургалтын загваруудыг туршиж, үр дүнг танилцуулах зорилготой. Сүүлийн үеийн судалгаанууд мөн урьдчилан сургасан параметрүүдийг ашиглан transfer learning буюу шилжүүлэн суралцах аргаар амжилттай үр дүн гаргасан. Жишээлбэл, Kareemulla нар sEMG мэдрэгчийн өгөгдлөөс ӨТҮ ангилахад transformer загварыг шилжүүлэн суралцах аргаар сургаж, өндөр үр дүнд хүрсэн [31]. Бидний мэдэхээр одоогоор бага нягтаршилтай IR дулааны матрицан мэдрэгчийн өгөгдлийн санд гүн сургалт болон transformer загварыг шилжүүлэн суралцах аргаар ашигласан судалгаа хийгдээгүй байна.

II. САЛБАРЫН СУДАЛГААНЫ АЖЛУУД

A. IR матрицан мэдрэгчээр бичсэн ӨТҮ танихад зориулсан өгөгдлийн сангууд

Бид ӨТҮ бүртгэхэд инфра улаан (IR) матрицан мэдрэгч ашигласан Multi-modal Ambient [32], Coventry2018 [33, 34], болон Infra-ADL2018 [35] гэсэн гурван өгөгдлийн санг авч үзсэн. Манай өгөгдлийн сантай харьцуулсан дүнг Хүснэгт 1-д үзүүлэв.

Multi-modal Ambient, Coventry-2018, болон InfraADL2018 нь тус бүр 14, 3, 8 оролцогчоос өгөгдөл цуглуулсан бөгөөд 25, 8, 9 төрлийн үйлдлийг агуулдаг. Эдгээр гурван өгөгдлийн санг бүгдийг нь хяналттай лабораторийн орчинд бичиж авсаг. Multi-modal Ambient өгөгдлийн санд үйлдлийн үргэлжлэх хугацаа2.7–200 секундийн хооронд, харин Coventry-2018 болон Infra-ADL2018 өгөгдлийн санд 2–28 секундийн хооронд хэлбэлздэг.

Multi-modal Ambient нь секунд тутамд нэг дүрс авдаг 8×8 хэмжээтэй IR дулааны матрицан мэдрэгчийг ашигласан. Coventry-2018 нь өөр өнцгүүдэд байрлуулсан гурван IR матрицан мэдрэгчийг ашиглаж, секундэд 10 фрэйм хурдтай дүрс бичиж авсан. Харин Infra-ADL2018 нь таазанд суурилуулсан ганц 8×8 IR матрицан мэдрэгчийг ашиглаж, секундэд 10 фрэйм хурдтай дүрс авсан болно. Манай өгөгдлийн нэг секунд дэх фрэймийн тоог 8.35 болгож тохируулсан. Мөн манай өгөгдлийн сан хамгийн олон буюу 74 оролцогчоос өгөгдөл бичсэн нь том давуу тал болж байна.

1-Р ХҮСНЭГТ IR ДУЛААНЫ МАССИВ МЭДРЭГЧЭЭР БИЧИГДСЭН ADL-ИЙН НЭЭЛТТЭЙ ӨГӨГДЛИЙН САНГУУД.

Өгөгдлийн сангууд	Мэдрэгч 8x8	Фрэйм хурд	Үйлдлүүд	Оролцогчид
Coventry-2018	3	3	3	3
Infra-ADL2018	10	10	10	10
Multi-modal	8	8	8	8
Ambient	3	3	3	3

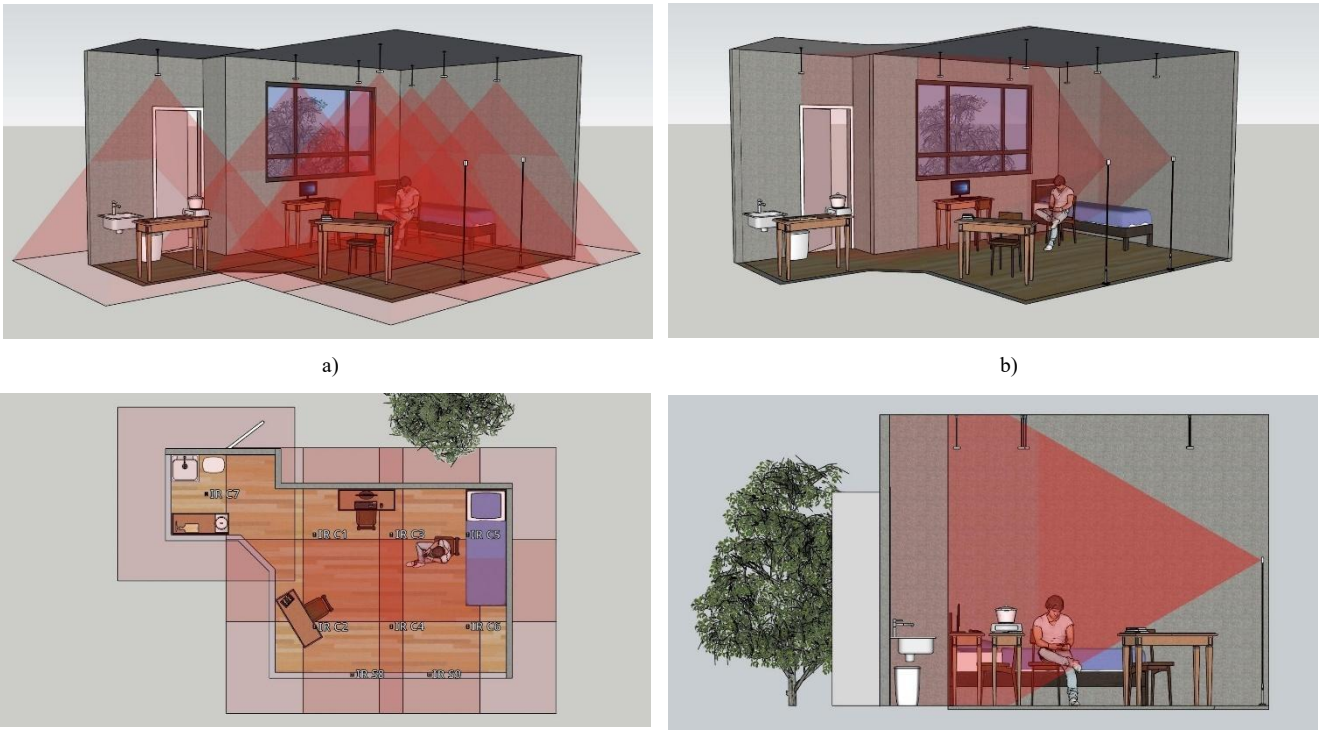
B. IR матрицан мэдрэгчийн өгөгдлөөс өдөр тутмын үйлдлийг таних загварууд

Олон судалгаанд инфра улаан (IR) дулааны матрицан мэдрэгчээр бүртгэсэн ӨТҮ-ийг ангилах аргуудыг судалсан бөгөөд голлон уламжлалт машин сургалтын аргуудыг ашигласан байдаг. Mashiyama нар 8×8 хэмжээтэй мэдрэгчээр таван төрлийн үйлдэл дээр Support Vector Machines (SVM), k-Nearest Neighbors (KNN), болон энгийн Неороны сүлжээ (NN) ашиглан ангилж, Унах үйлдлийг 100%-ийн нарийвчлалтай таньсан байна [24]. Muthukumar нар хоёр 32×24 хэмжээтэй IR матриц мэдрэгчээр зургаан төрлийн үйлдлийг CNN болон LSTM сүлжээний хослолоор таньж 97%-ийн нарийвчлалд хүрсэн [28]. Naser нар дөрвөн 24×32 хэмжээтэй IR матриц мэдрэгчээр бичсэн үйлдлүүд дээр Linear Regression (LR), SVM, KNN, болон Linear Discriminant Analysis (LDA) зэрэг уламжлалт аргуудыг туршсан [25]. Тэдний гурав дахь туршилтын тохиргоонд, мэдрэгчийг хананд янз бүрийн өндрөөр байрлуулсан бөгөөд LR ба SVM аргуудаар 96.1%-ийн дээд нарийвчлалд хүрсэн байна. Muthukumar нарын өөр нэг судалгаанд [29] таазанд суурилуулсан ганц 24×32 хэмжээтэй IR дулааны массив мэдрэгчээр бүртгэсэн үйлдлүүдийг CNN болон CNN+LSTM загваруудаар таньсан бөгөөд өгөгдлийг өргөтгөсний (augmentation) дараа CNN+LSTM загвараар 98.12%-ийн хамгийн өндөр нарийвчлалд хүрчээ.

III. ӨГӨГДЛИЙН САН

A. Өгөгдөл цуглуулах орчин

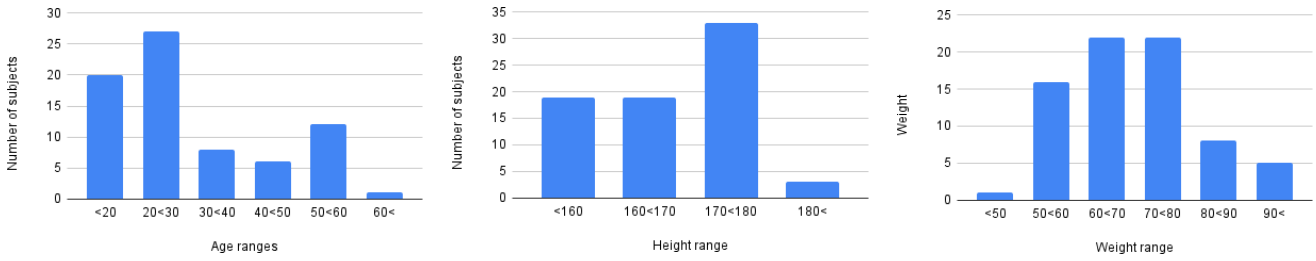
Өдөр тутмын үйлдлийн өгөгдөл цуглуулах лабораторийн орчин: Бид ӨТҮ-ийг бүртгэх зорилгоор есөн ширхэг Panasonic AMG8831 (8×8) инфра улаан (IR) дулааны массив мэдрэгч ашигласан хяналттай лабораторийн орчныг байгуулсан. Мэдрэгчүүдийн байрлалыг Зураг 1-д үзүүлэв. Үндсэн өрөөнд IR C1–IR C6 мэдрэгчийг таазанд, харин IR C7 мэдрэгчийг гал тогооны хэсгийн таазанд 2.65 метрийн өндөрт суурилуулсан. Үндсэн өрөөний хажуу хананд байрлах IR S8 болон IR S9 мэдрэгчийг 1.5 метрийн өндөрт байрлуулсан.



a) b)

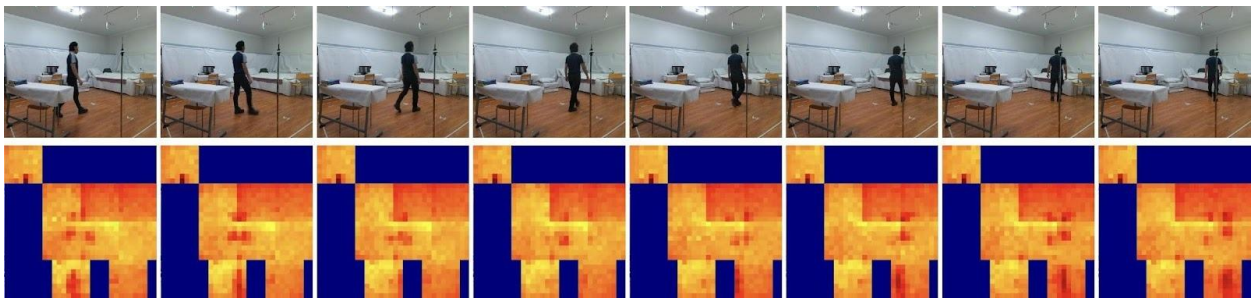
c) d)

1-р зураг. Өгөгдөл бичих орчин: (a) таазны мэдрэгчүүдийн бүрхэлт, (b) хажуугийн мэдрэгчүүдийн бүрхэлт, (c) дээрээс харсан 2 хэмжээст зураг, мэдрэгчүүдийн бүрхэлт, (d) хажуугаас харсан 2 хэмжээст зураг, мэдрэгчүүдийн бүрхэлт.



a) b) c)

Зураг 2: Сайн дурын оролцогчдын тархалтыг (a) насны бүлэг, (b) өндөр, (c) жингээр харуулсан



3-р зураг. Оролцогч өрөөнд алхах үйлдэл гүйцэтгэж буй байдал

)

Өгөгдөл цуглуулах систем нь секундэд 6–10 кадрын хурдтайгаар түүхий өгөгдөл бичиж авсан ба хурд нь мэдрэгч бүрийн хооронд бага зэрэг ялгаатай байсан. Лабораторийн орчны хэмжээ нь 4 м × 3.2 м хэмжээтэй үндсэн өрөө болон 1.4 м × 1.4 м хэмжээтэй гал тогооны буланд хуваагдана.

B. Оролцогчдын мэдээлэл

Бид нийт 74 сайн дурын оролцогчоор өдөр тутмын 19 төрлийн үйлдэл гүйцэтгүүлэн бичлэг хийсэн. Оролцогчдын нас 16–61 хооронд, жин 45–120 кг, өндөр 152–184 см байв. Эдгээрийн 56 нь эрэгтэй, 18 нь эмэгтэй оролцогч байлаа. Нас, өндөр, жингийн тархалтыг Зураг 2-д баганан графикаар үзүүлсэн. Оролцогчдын ихэнх нь 30-аас доош

2-Р ХҮСНЭГТ ХҮНИЙ ӨДӨР ТУТАМД ГҮЙЦЭТГЭДЭГ 19 ӨГӨГДӨЛ

#	Үйлдлүүд	Бичлэгийн тоо	Дундаж фрэймийн тоо	Дундаж урт (секунд)	Нийт фрэймийн тоо	Нийт урт (секунд)
1	Өрөө цэвэрлэх	74	733.02	87.95	54244	6509.02
2	Идэх	74	886.01	106.31	65565	7867.48
3	Өрөөнд орох	73	44.21	5.30	3227	387.22
4	Дасгал хийх	74	969.35	116.32	71732	8607.49
5	Унах	124	25.31	3.04	3139	376.67
6	Хүндээр амьсгалах	73	137.74	16.53	10055	1206.55
7	Өрөөнөөс гарах	73	40.21	4.82	2935	352.19
8	Унасны дараа хэвтэх	91	102.68	12.32	9344	1121.23
9	Хоол бэлтгэх	74	2837.45	340.48	209972	25195.61
10	Унших	74	1474.81	176.97	109136	13095.79
11	Амарах	74	1428.09	171.36	105679	12680.96
12	Унтах	74	1724.69	206.95	127627	15314.62
13	Зогсох	74	283.57	34.02	20984	2517.98
14	Утсаар ярих	75	486.29	58.35	36472	4376.46
15	Хувцас тайлах	74	77.22	9.27	5714	685.65
16	Компьютер дээр ажиллах	74	1494.99	179.39	110629	13274.94
17	Өрөөнд алхах	74	522.34	62.68	38653	4638.17
18	Аяга угаах	74	309.73	37.17	22920	2750.29
19	Зураг үзэх	74	1733.51	208.01	128280	15392.97
20	Бүгд	1471	772.47	9269.00	1136307	136351.29

3-Р ХҮСНЭГТ ЗАГВАРУУДЫН ХАРЬЦУУЛСАН ХҮСНЭГТ

#	Загварууд	Гарсан жил	Суурь архитектур	Параметрийн тоо	Анхны жин
1	R(2+1)D-18	2017	CNN	31,309,359	KINETICS400_V1
2	Swin-T	2021	former	27,864,312	KINETICS400_V1
3	MViTv2	2022	former	34,243,986	KINETICS400_V1

4-Р ХҮСНЭГТ СУРГАЛТЫН ҮР ДҮНГҮҮДИЙН ХАРЬЦУУЛАЛТ

#	Загварууд	Recall	Precision	F1-score
1	Swin-T	0.833	0.842	0.825
2	MViTv2	0.854	0.857	0.846
3	R(2+1)D-18	0.861	0.863	0.852

насныхан (Зураг 2a), харин оролцогчдын тал орчим нь 170–180 см өндөртэй (Зураг 2b) байв. Жингийн тархалт нь нас, өндөртэй харьцуулахад илүү жигд (нормаль) хуваарилалттай байсан (Зураг 2c).

С. Өгөгдөл боловсруулалт

Өгөгдлийн урьдчилсан боловсруулалт

Түүхий өгөгдөл нь тогтмол бус дээж авах хурд, цуваагаар бичигдсэн мэдрэгчийн утгууд, шуугиан, буруу шошго тавигдсан зэрэг асуудлуудтай байсан тул эдгээр асуудлуудыг засах шаардлагатай болсон. Өгөгдлийг 8.35 Hz тогтмол давтамжтай болгож шугаман интерполяциар нөхсөн. Есөн ширхэг 8×8 IR дулааны массив мэдрэгчээс ирсэн анхны 64 пикселийн нэг хэмжээст векторыг 32×32 хэмжээтэй дүрсэнд хувиргасан. Энэ нь мэдрэгчүүдийн байрлалыг орон зайн хувьд хадгалж, хүний дүрсийн дулааны “бүдүүн дүрслэл”-ийг Зураг 3-д үзүүлсэнтэй адил харагдуулсан. Зарим үйлдлийн эхлэл ба төгсгөлийн шошго нь бодит бичлэгийн цагтай зөрүүтэй байсан тул гар аргаар засварласан. Фрэйм хоорондын огцом өөрчлөлтийг дарахын тулд хугацааны дугаа медиан шүүр хэрэглэсэн. Мөн 15-

5-Р ХҮСНЭГТ ҮЙЛДЭЛ ТУС БҮРИНЙ RECALL, PRECISION, AND F1-SCORE ОНООНУУД

#	Үйлдлүүд	Recall				Precision				F1-score			
		R(2+1)D-18	MViTv2	Swin_T	Дундаж Recall	R(2+1)D-18	MViTv2	Swin_T	Дундаж Precision	R(2+1)D-18	MViTv2	Swin_T	Дундаж F1-score
1	Өрөө цэвэрлэх	0.907	0.845	0.804	0.852	0.855	0.899	0.869	0.874	0.880	0.871	0.835	0.862
2	Идэх	1.000	0.993	0.966	0.986	0.794	0.790	0.851	0.812	0.885	0.880	0.905	0.890
3	Өрөөнд орох	0.928	0.939	0.777	0.881	0.966	0.993	0.799	0.919	0.947	0.965	0.788	0.900
4	Дасгал хийх	0.844	0.818	0.838	0.833	0.628	0.545	0.532	0.568	0.720	0.654	0.651	0.675
5	Унах	0.932	0.939	0.946	0.939	1.000	0.986	0.986	0.991	0.965	0.962	0.966	0.964
6	Хүндээр амьсгалах	0.203	0.297	0.284	0.261	0.714	0.733	0.808	0.752	0.316	0.423	0.420	0.386
7	Өрөөнөөс гарах	0.884	0.919	0.723	0.842	0.929	0.944	0.770	0.881	0.906	0.932	0.746	0.861
8	Унасны дараа хэвтэх	0.986	0.986	0.993	0.988	0.973	0.973	0.936	0.961	0.980	0.980	0.964	0.975
9	Хоол бэлтгэх	1.000	0.980	0.986	0.989	0.986	0.967	0.980	0.978	0.993	0.973	0.983	0.983
10	Унших	0.766	0.791	0.858	0.805	0.799	0.854	0.825	0.826	0.782	0.821	0.841	0.815
11	Амарах	0.849	0.818	0.838	0.835	0.810	0.877	0.844	0.844	0.829	0.846	0.841	0.839
12	Унтах	1.000	1.000	1.000	1.000	0.955	0.886	0.949	0.930	0.977	0.940	0.974	0.963
13	Зогсох	0.605	0.385	0.453	0.481	0.597	0.500	0.663	0.587	0.601	0.435	0.538	0.525
14	Утсаар ярих	0.822	0.966	0.959	0.916	0.779	0.911	0.717	0.802	0.800	0.938	0.821	0.853
15	Хувцас тайлах	0.782	0.709	0.649	0.713	0.898	0.868	0.842	0.869	0.836	0.781	0.733	0.783
16	Компьютер дээр ажиллах	0.919	0.912	0.851	0.894	0.965	0.993	1.000	0.986	0.941	0.951	0.920	0.937
17	Өрөөнд алхах	0.925	0.973	0.905	0.934	0.845	0.787	0.812	0.815	0.883	0.870	0.856	0.870
18	Аяга угаах	1.000	0.993	1.000	0.998	1.000	0.980	0.993	0.991	1.000	0.987	0.997	0.994
19	Зураг үзэх	1.000	0.959	1.000	0.986	0.899	0.802	0.818	0.840	0.947	0.874	0.900	0.907
Дундаж утга		0.861	0.854	0.833		0.863	0.857	0.842		0.852	0.846	0.825	
Стандарт хазайлт		0.195	0.204	0.200		0.126	0.145	0.124		0.170	0.173	0.159	

6-Р ХҮСНЭГТ ХАМГИЙН ӨНДӨР ХООРОНДЫН АНДУУРАЛТАЙ ҮЙЛДЛҮҮДИЙН ХОСЛОЛЫГ MUTUAL ОНООНЫ УТГААР ЭРЭМБЭЛЖ ХҮСНЭГТЛЭН ХАРУУЛАВ

#	*i*	*j*	*Pij*	*Pji*	Mutual	Delta
1	Дасгал хийх	Зогсох	0.093	0.293	0.193	-0.200
2	Хүндээр амьсгалах	Зогсох	0.209	0.036	0.123	0.173
3	Дасгал хийх	Хүндээр амьсгалах	0.002	0.221	0.111	-0.218
4	Өрөөнд орох	Өрөөнөөс гарах	0.112	0.077	0.094	0.035
5	Идэх	Унших	0.002	0.179	0.091	-0.177
6	Хүндээр амьсгалах	Утсаар ярих	0.140	0.014	0.077	0.126
7	Өрөө цэвэрлэх	Өрөөнд алхах	0.092	0.034	0.063	0.058
8	Дасгал хийх	Хувцас тайлах	0.005	0.115	0.060	-0.111
9	Компьютер дээр ажиллах	Зураг үзэх	0.104	0.000	0.052	0.104
10	Унших	Амарах	0.009	0.082	0.045	-0.072

аас доош утгатай пикселийн утгыг 0 болгож арын шуугианыг дарсан. Үйлдлийн дараалал бүрийн өмнө болон дараа 7 кадр нэмж оруулсан. Үүний дараа 32 фрэймийн урттай, нэг алхамын клип үүсгэж, 32×32×32 хэмжээтэй 3 хэмжээст тенсорууд үүсгэсэн.

Тэнцвэржүүлсэн санамсаргүй хуваалт

Өгөгдөлд ангиллын хугацааны ялгаанаас шалтгаалах гажуудал үүсэхээс сэргийлж, тэнцвэртэй дэд өгөгдлийн сангууд үүсгэсэн. Эхлээд өгөгдлийг хүн тус бүрийн түвшинд 70% сургалт, 15% баталгаажуулалт, 15% тест гэсэн хуваалттайгаар ангилж, нэг оролцогчийн өгөгдөл давхардаж орохоос сэргийлсэн. Дараа нь тус бүрийн ангилал дахь хамгийн бага тенсорын тоо Nmin-ийг тодорхойлж, үйлдэл бүрээс Nmin ширхэг тензорыг санамсаргүйгээр сонгон тэнцвэртэй төлөөлөл бүрдүүлсэн.

IV. ТУРШИЛТ

A. Туршилтын загварууд

Бид (32×32×32) хэмжээтэй тенсор өгөгдлүүдийг ашиглан, машин сургалтын загваруудыг харьцуулах зорилгоор дараах архитектуруудыг сонгосон:

- R(2+1)D-18 [36]: 2 хэмжээст онцлогуудыг 2D conv давхаргаар, хугацааны онцлогуудыг 1D conv давхаргаар боловсруулдаг ResNet-18-ийн хувилбар.
- Swin-T [37]: Хөдөлгөөнт цонхтой видеонд зориулсан трансформерийн “Tiny” хувилбар. • MViTv2 [38]: Олон хэмжээст видео трансформерийн (Multiscale Vision Transformer) хоёр дахь хувилбар.

Эдгээр загваруудыг Хүснэгт 3-д нэгтгэн харуулсан бөгөөд бүгд гурван хэмжээст тенсор оролт дээр ажилладаг. R(2+1)D-18 загвар нь орон зайн шинж чанарыг илрүүлэхэд 2D конволюцийн шүүрийн давхаргуудыг, харин цагийн хугацааны хэмжээсийн шинж чанарыг илрүүлэхэд 1D конволюцийн шүүрийн давхаргуудыг ашигладаг. Swin-T болон MViTv2 нь vision transformer архитектурт хамаарах бөгөөд орongийн болон хугацааны өгөгдөл дэх урт хамаарлуудыг үр дүнтэй илрүүлж чаддаг.

B. Туршилтын үр дүнгүүд

Өгөгдлийн сан нь нийт 19 төрлийн ялгаатай үйлдлийн бичлэгүүдийг агуулсан. Бүх загваруудын сургалтыг урьдчилан сурсан жингүүдтэйгээр эхлүүлэн сургах үед загварууд тогтвортойгоор суралцаж байсан бол, дурын жингийн утгатайгаар эхлүүлэхэд сургалт тогтворгүй болж, үр дүнд хүрээгүй.

Загваруудын үр дүнгүүд

R(2+1)D-18, MViTv2, SwinT загваруудын гүйцэтгэлийг Хүснэгт 4-д нэгтгэн харуулсан. Recall-ийн утга 0.833–0.861-ийн хооронд хэлбэлзэж, R(2+1)D-18 загвар хамгийн сайн үр дүнд хүрсэн бол Swin-T хамгийн доод үзүүлэлттэй байв. Precision болон макро F1-score нь тус тус 0.842–0.963, 0.825–0.852-ийн хооронд байна.

Хүснэгт 5-д үзүүлсэн ангилал тус бүрийн дундаж Recall нь 0.261–1.000-ийн хооронд хэлбэлзэж байна. Унтах (1.000), Аяга угаах (0.998), Хоол бэлтгэх, Унасны дараа хэвтэх үйлдлүүд бараг төгс танигдсан бол Хүндээр амьсгаадах, Зогсох, Хувцас тайлах үйлдлүүд нь танихад хамгийн хүнд ангиллууд байв. Precision болон F1-score-ийн хандлага мөн адил байсан ба ойролцоогоор 0.568–0.991 болон 0.387–0.994-ийн хооронд хэлбэлзжээ.

Хамгийн сайн гүйцэтгэлтэй R(2+1)D-18 загвар ч зарим үйлдлүүд дээр хамгийн доод үзүүлэлттэй байсан. Жишээлбэл, Хүндээр амьсгаадах (0.203) болон Унших (0.766)-ийн Recall, Амрах (0.810)-ийн Precision, Өрөөнд алхах (0.883)-ийн F1-score зэргийг дурьдаж болно. Харин нийт дүнгээр сул гүйцэтгэлтэй Swin-T загвар нь зарим ангилал дээр бусдаасаа илүү үзүүлэлттэй байсан. Тухайлбал, Унах (0.946), Унших (0.858)-ийн Recall, Идэх (0.851)-ийн Precision, мөн F1-score-ын хувьд ч давуу үзүүлэлттэй байв.

Үйлдлүүдийн үр дүнгүүд

Үр дүнгээс харахад үйлдэл бүрийн ялгарал тодорхой ажиглагдсан. Дундаж Recall 0.391–0.999-ийн хооронд хэлбэлзэж, хамгийн өндөр үзүүлэлтүүд нь Унтах (0.999), Аяга угаах (0.989), Идэх (0.988) үйлдлүүдэд, хамгийн бага нь Standing (0.391) болон Хувцас тайлах (0.665) үйлдлүүдэд ажиглагдсан. Эдгээрээс бусад бүх үйлдлүүдийн дундаж Recall 0.700-аас дээш байв.

Дундаж Precision ихэнхдээ өндөр буюу 0.75-аас дээш байсан боловч Дасгал хийх (0.521) болон Зогсох (0.622) үйлдлүүдэд харьцангуй доогуур гарсан. Өрөөнд алхах үйлдэл мөн 0.702 гэсэн бага Precision-тэй байсан бол хамгийн өндөр үзүүлэлтүүд нь Аяга угаах (0.980) болон Унтах (0.979) байв.

Дундаж F1-score мөн адил хандлагатай байсан бөгөөд Зогсох (0.472) хамгийн бага, Унтах (0.989) хамгийн өндөр байсан. Аяга угаах (0.984) болон Хоол бэлдэх (0.965) нь мөн өндөр танигдсан үйлдлүүдийн тоонд ордог. Нийт дундаж F1-score нь бүх үйлдлүүдийн хувьд 0.731-ээс дээш байсан бөгөөд зөвхөн Зогсох (0.472) болон Дасгал хийх (0.601) үйлдлүүдэд бага гарсан.

Хувьсах чанарын хэмжүүрүүдийг харвал, Recall-ийн стандарт хазайлт 0.003–0.176, Precision 0.022–0.173, F1-score 0.014–0.156-ийн хооронд байв (Хүснэгт 6). Унтах болон Аяга угаах үйлдлүүд нь бүх хэмжүүрт хамгийн жигд (narrow) тархалттай байсан бол хамгийн өргөн тархалттай нь Утсаар ярих (Recall: 0.165), Зогсох (Precision: 0.173), мөн Утсаар ярих (F1: 0.156) байв. Мөн Өрөөнд алхах болон Өрөө цэвэрлэх үйлдлүүд илүү өргөн стандарт хазайлттай ангиллууд байна.

Эдгээр хэлбэлзлүүд нь ямар үйлдлүүдийг загварууд тогтвортой таньж чаддаг, мөн ямар үйлдлүүдийн гүйцэтгэл архитектурын бүтэц, тохиргоонд мэдрэмтгий байдгийг тодорхой харуулж байна.

Үйлдэл хооронды андуурал

Хамгийн их андуурагдсан 10 хос үйлдэл (Хүснэгт 6)-ийн дийлэнх нь Дасгал хийх–Зогсох (0.193), Хүндээр амьсгаадах–Зогсох (0.123), Дасгал хийх–Хүндээр амьсгаадах (0.111) хослолууд байв. Хамгийн өндөр чиглэлтэй андуурал нь Дасгал хийх → Хүндээр амьсгаадах (-0.218) болон Дасгал хийх → Зогсох (-0.200) байсан нь эдгээр үйлдлүүдийг ялгахад тогтвортой тэгш хэмт бус ялгаа байгааг харуулж байна. Хамгийн өндөр Mutual оноонууд зөвхөн Дасгал хийх, Зогсох, Хүндээр амьсгаадах гэсэн гурван ангилалд л хамаарч байгаа нь эдгээрийн хооронды төстэй хөдөлгөөний хэв шинж буйг харуулж байна.

C. Туршилтын үр дүнгүүд

Өгөгдлийн сан нь нийт 19 төрлийн ялгаатай үйлдлийн бичлэгүүдийг агуулсан. Бүх загварууды сургалтыг урьдчилан сурсан жингүүдтэйгээр эхлүүлэн сургах үед загварууд тогтвортойгоор суралцаж байсан бол, дурын жингийн утгатайгаар эхлүүлэхэд сургалт тогтворгүй болж, үр дүнд хүрээгүй.

V. ХЭЛЭЛЦҮҮЛЭГ

A. Өгөгдлийн сан

Энэхүү өгөгдлийн сан нь нууцлалыг хамгаалсан ADL таних зорилготойгоор бүтээгдсэн хамгийн том өгөгдлийн сан бөгөөд 74 оролцогч, 9 ширхэг IR дулааны массив мэдрэгч, 19 төрлийн ялгаатай үйлдэлийн бичлэгийг багтаасан. Оролцогчдын дийлэнх нь харьцангуй залуу хүмүүс байсан ч 50-аас дээш настай хүмүүс мөн оролцсон бөгөөд биеийн жингийн тархалт нь нормаль хуваарилалттай байна. Үйлдлүүдийн бичлэгүүдийг адил болгохын тулд тэнцвэржүүлсэн дэд өгөгдлийн сан (balanced subdataset) үүсгэн сургалтад ашигласан. Энэ тэнцвэржүүлсэн өгөгдлийн сантай хийгдсэн туршилтуудыг сургалтад ашиглагдаагүй оролцогчдын өгөгдөл дээр шалгахад өндөр үр дүн гарсан.

B. Загварууд

R(2+1)D-18 нь нийт гүйцэтгэлийн хувьд хамгийн сайн загвар бөгөөд F1-score 0.900, таамаглалын хурд 4.8 мс, иймээс бодит цагийн (real-time) хяналтын системд, ялангуяа нарийвчлалд илүү ач холбогдол өгдөг нөхцөлд, тохиромжтой шийдэл юм. Сургалтанд урьдчилсан суралцсан жингийн коэффициент ашиглах нь шийдвэрлэх үүрэгтэй болохыг баталсан. Загварууды нарийвчилсан шинжилгээгээр эдгээр нь өөр өөр Recall, Precision, F1-score-той байна. Жишээлбэл, R(2+1)D-18-ийн хувьд гурван хэмжүүрий утгууд тэнцвэртэй байгаа

бол MViTv2 нь бүх үйлдлүүдийн хооронд илүү тогтвортой гүйцэтгэл үзүүлдэг бол Swin-T нь Дасгал хийх, Унших, Компьютер дээр ажиллах зэрэг жижиг, нарийн хөдөлгөөнтэй үйлдлүүд дээр илүү сайн ажилладаж байна. Энэ нь transformer архитектурын анхаарал (attention) механизм нь уламжлалт конволюц шүүрийн анзаарахгүй орхидог нарийн өөрчлөлтийг илүү сайн барьж авдгийг харуулж байна.

C. IR дулааны мэдрэгчээр бичигдсэн үйлдлүүдийн өгөгдлүүд

8×8 хэмжээтэй IR дулааны матрицан мэдрэгчээс авсан өгөгдөл нь нарийвчлал багатай дулааны зураг үүсгэдэг бөгөөд тэдгээрийг нүдээр шууд тайлбарлахад хүндрэлтэй байдаг. Гүн сургалтын загварууд нь эдгээр өгөгдлөөс ялгаатай оронгийн болон хугацааны шинж тэмдгийг оновчтой ялган авч, үйлдлийг таних чадвартай болохыг харуулж байна. Хүснэгт 5-ийн үр дүнгийн үндсэн дээр үйлдлүүдийг дараах дөрвөн ангилалд хувааж болно:

Хялбар танигддаг үйлдлүүд

Идэх, Унасны дараа хэвтэх, Хоол бэлтгэх, Унтах, Компьютер дээр ажиллах, Аяга угаах зэрэг нь өндөр дундаж оноотой хамгийн сайн танигдсан үйлдлүүд юм. Эдгээр нь өрөөний тодорой цэгт гүйцэтгэгдэх юм уу тодорхой биеийн байрлалтай үйлдлүүд бөгөөд загварууд хувьд ялгахад хялбар байна.

Дундаж түвшинд тогтвортой танигддаг үйлдлүүд

Унших (F1-score: 0.780, 0.025), Зурагт үзэх (F1-score: 0.894, 0.072) нь энэ бүлэгт хамаарна. Аль аль нь сууж буй байрлалтай, гарын хөдөлгөөн хязгаартай үйлдлүүд бөгөөд энэ нь тэдний тогтвортой боловч дундаж нарийвчлалтай танигдах шалтгаан болж байна.

Дундаж түвшинд боловч загварууд хооронд тогтворгүй танигддаг үйлдлүүд

Өрөө цэвэрлэх, Өрөөнд орох, Өрөөнөөс гарах, Амарах, Утсаар ярих, Өрөөнд алхах зэрэг нь дундаж оноотой үйлдлүүд. Эдгээрийн ихэнх нь алхалттай холбоотой хөдөлгөөний хэв маягтай.

Танихад хүнд үйлдлүүд

Дасгал хийх, Зогсох, Хувцас тайлах нь бүх загварууд хамгийн багийн оноотой гарсан. Эдгээрийн нийтлэг шинж нь босоо байрлалтай бөгөөд байршлын хувьд оролцогчоос хамааран өөрчлөгддөг.

D. Андуурал болон тэгш хэмт бус байдал

Хүснэгт 6-д үзүүлсэн андуурал нь аль үйлдэл альтайгаа төстэй онцлог хуваалцдаг болохыг харуулна. Хэрэв үйлдлүүд гүйцэтгэх байрлал болон биеийн хэв зэрэг хүчтэй нийтлэг шинжтэй бол тэдгээр нь хамгийн их андуурагддаг. Зогсох ба Дасгал хийх нь хоёулаа өрөөний төв хэсэгт, босоо байрлалтай хийгддэг. Унах ба Унасны дараа хэвтэх нь хэвтээ байрлал болон байршлын хувьд төстэй.

ДҮГНЭЛТ

Бид энэхүү ажлаар IR дулааны матрицын олон мэдрэгчийн өгөгдлөөр хүний ӨТҮ-ийг таних судалгааны ажлын үр дүнг танилцуулж байна. Уг өгөгдөл дээр Resnet CNN-ийн төлөөлөл болох R(2+1)D-18, Transformer-ийн төлөөлөл болох MViT, Swin−T загваруудаар өгөгдөл сургасан үзүүлэлтийг оруулсан.

Энэ судалгаанд пикселийн огцом шилжилтийг хадгалахын тулд зөвхөн хугацааны тэнхэлгийн дагуу Median шүүр хэрэглэсэн. Туршилтын үр дүн нь IR дулааны тойм дүрслэл ашиглан нарийвчлалтай, хувь хүний нууцлалыг хадгалсан өдөр тутмын үйлдэл таних системийг хэрэгжүүлэх бүрэн боломжтойг харуулсан. Өгөгдлийг 4 сек үргэлжлэх клипүүдэд хуваасан бөгөөд түүн дээр өндөр үр дүн үзүүлж байгаа нь цаашид бодит цагийн танилт хийх боломжтойг харуулж байгаг.

Цаашдын ажлын хүрээнд бид:

Бие даасан, бодит цагийн ӨТҮ таних зориулалттай жижиг, хөнгөн загвар хөгжүүлэх,

Гэрийн орчны өдөр тутмын үйлдлийг дуурайлгах хиймэл өгөгдлийн сан үүсгэн системийн бодит цагийн ангиллын гүйцэтгэлийг үнэлэх,

Мөн IR дулааны матрицан мэдрэгчийн өгөгдлийн шүүлтүүрийн аргуудыг оновчтой болгоно.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] D. Gu, K. Andreev, M. E. Dupre, Major trends in population growth around the world, China CDC weekly 3 (28) (2021) 604.

[2] WHO, Un decade of healthy ageing: plan of action (2021-2030).(2020) (2020).

[3] WHO, Advocacy brief: Social isolation and loneliness among older people (2021).

[4] Y.-D. Wu, J.-X. Dong, F.-M. Yu, Z.-H. Dong, W. Ma, Y. Cai, Y.-Q. Cai, Y. Mu, X. Cui, Y.-R. Wang, et al., Mapping the global research landscape and trends of older people living alone: a bibliometric analysis, Frontiers in Aging 6 (2025) 1524673.

[5] H. Lee, J. H. Lim, Living alone, environmental hazards, and falls among us older adults, Innovation in aging 7 (6) (2023) igad055.

[6] I. Lage, F. Braga, M. Almendra, F. Meneses, L. Teixeira, O. Araujo, Falls in older persons living alone: the role of individual, social and environmental factors, Enfermeria clinica (English Edition) 32 (6) (2022) 396–404.

[7] J. Fleming, C. Brayne, Inability to get up after falling, subsequent time on floor, and summoning help: prospective cohort study in people over 90, Bmj 337 (2008).

[8] D. Kim, H. Bian, C. K. Chang, L. Dong, J. Margrett, In-home monitoring technology for aging in place: scoping review, Interactive journal of medical research 11 (2) (2022) e39005.

[9] Y. J. Tian, N. A. Felber, F. Pageau, D. R. Schwab, T. Wangmo, Benefits and barriers associated with the use of smart home health technologies in the care of older persons: a systematic review, BMC geriatrics 24 (1) (2024) 152.

[10] C.-Y. Wang, F.-S. Lin, Ai-driven privacy in elderly care: Developing a comprehensive solution for camera-based monitoring of older adults, Applied Sciences 14 (10) (2024) 4150.

[11] T. T. Zin, Y. Htet, Y. Akagi, H. Tamura, K. Kondo, S. Araki, E. Chosa, Real-time action recognition system for elderly people using stereo depth camera, Sensors 21 (17) (2021) 5895.

[12] M. S. Momin, A. Sufian, D. Barman, P. Dutta, M. Dong, M. Leo, In-home older adults' activity pattern monitoring using depth sensors: A review, Sensors 22 (23) (2022) 9067.

[13] W. Mucha, M. Kampel, Beyond privacy of depth sensors in active and assisted living devices, in: Proceedings of the 15th International Conference on Pervasive Technologies Related to Assistive Environments, 2022, pp. 425–429.

[14] A. D. R. Fern´andez, D. R. Fern´andez, M. G. Ja´en, J. M. Cortell-Tormo, et al., Recognition of daily activities in adults with wearable inertial sensors: Deep learning methods study, JMIR Medical Informatics 12 (1) (2024) e57097.

[15] S. J. Ray, J. Cherian, A. M. Liberty, T. A. Hammond, P. K. Shireman, Recognition of basic activities of daily living using wearable devices for older adults: Scoping review, Journal of Medical Internet Research 27 (2025) e67373.

[16] K. Moore, E. O'Shea, L. Kenny, J. Barton, S. Tedesco, M. Sica, C. Crowe, A. Alam¨aki, J. Condell, A. Nordstr¨om, et al., Older adults' experiences with using wearable devices: qualitative systematic review and meta-synthesis, JMIR mHealth and uHealth 9 (6) (2021) e23832.

[17] M. T. R. Khan, E. Ever, S. Eraslan, Y. Yesilada, Human activity recognition using binary sensors: A systematic review, Information Fusion 115 (2025) 102731.

[18] H. Y. Yatbaz, S. Eraslan, Y. Yesilada, E. Ever, Activity recognition using binary sensors for elderly people living alone: Scanpath trend analysis approach, IEEE Sensors Journal 19 (17) (2019) 7575–7582.

[19] T.-H. Tan, L. Badarch, W.-X. Zeng, M. Gochoo, F. S. Alnajjar, J.-W. Hsieh, Binary sensors-based privacy preserved activity recognition of elderly living alone using an rnn, Sensors 21 (16) (2021) 5371.

[20] B. Yu, Y. Liu, K. Chan, A survey of sensor modalities for human activity recognition, in: Proceedings of the 12th International Joint Conference on Knowledge Discovery, Budapest, Hungary, 2020, pp. 2–4.

[21] C. Silver, T. Akilan, Thermal fall 66: A robust dataset for thermal imaging-based fall detection and eldercare, Engineering Applications of Artificial Intelligence 160 (2025) 111819.

[22] K. Naik, T. Pandit, N. Naik, P. Shah, Activity recognition in residential spaces with internet of things devices and thermal imaging, Sensors 21 (3) (2021) 988.

[23] L. Badarch, M. Gochoo, G. Batnasan, F. Alnajjar, T.-H. Tan, Ultra-low resolution infrared sensor-based wireless sensor network for privacy-preserved recognition of daily activities of living, in: 2021 IEEE 20th international symposium on network computing and applications (NCA), IEEE, 2021, pp. 1–5.

[24] S. Mashiyama, J. Hong, T. Ohtsuki, Activity recognition using low resolution infrared array sensor, in: 2015 IEEE International Conference on Communications (ICC), IEEE, 2015, pp. 495–500.

[25] A. Naser, A. Lotfi, J. Zhong, Multiple thermal sensor array fusion toward enabling privacy-preserving human monitoring applications, IEEE Internet of Things Journal 9 (17) (2022) 16677–16688.

[26] Y. Karayaneva, S. Sharifzadeh, Y. Jing, B. Tan, Human activity recognition for ai-enabled healthcare using low-resolution infrared sensor data, Sensors 23 (1) (2023). doi:10.3390/s23010478.

[27] S. Mekruksavanich, W. Phaphan, A. Jitpattanakul, Lowresir-net: Lightweight residual network for adl recognition using low-resolution infrared sensor data, Procedia Computer Science 256 (2025) 1358–1366.

[28] K. Muthukumar, M. Bouazizi, T. Ohtsuki, A novel hybrid deep learning model for activity detection using wide-angle low-resolution infrared array sensor, IEEE Access 9 (2021) 82563–82576.

[29] K. A. Muthukumar, M. Bouazizi, T. Ohtsuki, An infrared array sensor-based approach for activity detection, combining low-cost technology with advanced deep learning techniques, Sensors 22 (10) (2022). doi:10.3390/s22103898.

CNN-Д СУУРИЛСАН ЦЭЭЖНИЙ РЕНТГЕН ЗУРГИЙН БОЛОВСРУУЛАЛТ БА ХЭРЭГЛЭЭНИЙ БОЛОМЖ

Нарангэрэлийн НАРАНБААТАР[1] , Цэрэндондогийн ТЭНГИС[2]

[1,2]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Электроникийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: n.naranbagatur@gmail.com[1]

***Хураангуй*: Сүрьеэгийн өвчлөл, нас баралт манай улсын эрүүл мэндийн салбарын тулгамдсан асуудал хэвээр байгаа бөгөөд тус өвчний бүртгэгдсэн тохиолдлын 59% нь уушгины сүрьеэ байгаа нь сэтгэл түгшээсэн явдал юм. Тиймээс уушгины сүрьеэг дүрс оношилгооны аргаар буюу цээжний рентген зургаар оношилдог. Энэхүү судалгааны ажлын зорилго нь эрүүл болон сүрьеэтэй гэсэн онош бүхий тоон цээжний рентген зургийг гүн сургалтын аргаар сургаж, өөрийн загварыг бий болгоход оршино. 2014-2015 онд хийгдсэн "Монгол Улсын хүн амын дундах сүрьеэгийн тархалтыг тогтоох судалгаа"-ны DICOM өргөтгөлтэй хадгалагдсан рентген зургийг JPG өргөтгөлтэй, 512x512 хэмжээтэй саарал зураг болгон Convolutional Neural Network (CNN) оролтод өгч ангилах туршилтуудыг гүйцэтгэв. Бидний санал болгож буй гүн сургалтын загвар болох SmallCNN_model.h5 загварын F1 macro score = 0.97 гэсэн үр дүнг үзүүлсэн нь маш өндөр гүйцэтгэлтэй загвар гэдгийг илтгэж байна**

Түлхүүр үг: Уушги, сүрьеэ, CNN, машин сургалт, сүрьеэгийн тархалт,

I. УДИРТГАЛ

Монгол Улс нь Риф/ОЭТС-ийн дарамт өндөртэй 30 орны нэг, Номхон далайн баруун эргийн бүсийн сүрьеэгийн өвчлөл өндөр 7 орны нэг юм. Сүрьеэ нь манай улсад бүртгэгдсэн халдварт өвчний дотор гуравдугаар байранд орж, нас баралтын нэгдүгээр шалтгаан болж байна [1].

2013 онд манай улсад хэмжээнд 4111 шинэ тохиолдолд бүртгэгдсэн ба бүртгэгдсэн тохиолдлын түвшин 100'000 хүн амд 142, нас баралт 1,9 байна. Бүртгэгдсэн сүрьеэгийн тохиолдлын 59%- нь уушгины сүрьеэ эзэлж байна [2]. Идэвхтэй уушгины буюу ларингеал сүрьеэтэй хүн ханиах, ярих, дуулах, найтаах г.м үед амьсгалын замаар *Mycobacterium tuberculosis* агуулсан бичил дуслуудыг тухайн орчинд цацах замаар халдварыг тараадаг [3,4]. Иймд ДЭМБ болон бусад байгууллагууд идэвхтэй тохиолдлын илрүүлэлт, тархалтын судалгаанд зориулж төрөл бүрийн арга, стратеги санал болгодог бөгөөд түүний нэг болох цээжний рентген зургаар хэвийн бус өвчтөнийг илрүүлэх аргыг өргөнөөр ашиглаж байна [5, 6].

Сүрьеэгийн халдварын хамгийн том асуудал нь халдвар авсан хүмүүс хэрэв төрөлхийн буюу дасан зохицох дархлаа сайтай хүмүүс сүрьеэгийн бактерийг дарангуйлж, өвчний шинж тэмдэг илэрдэггүй ба халдвар тээгч өөрийгөө халдвар авснаа мэддэггүй. Хэрэв дархлаа нь халдварыг дарж чадахгүй бол хэдэн долоо хоног эсвэл хэдэн жилийн дараа тэдгээр хүмүүс сүрьеэгийн өвчнөөр өвдөх болно [7].

Монгол Улс дахь сүрьеэгийн тархалтын анхны судалгааны тайланд дурдсан сүрьеэгийн тархалтын түвшин ДЭМБ-ын өмнөх тооцооллоос нэлээд өндөр байв. 15 буюу түүнээс дээш насны 100,000 хүн амд ногдох түрхэц эерэг ба нян судлалаар батлагдсан уушгины сүрьеэгийн тархалт харгалзан 204.0 (143.0 265.1) ба 559.6 (454.5-664.7) байна [2].

Иймд сүрьеэ өвчнийг эрт оношлох нь үр дүнтэй эмчилгээ хийх, халдвар дамжихаас сэргийлнэ. Цээжний рентген зураг дээр суурилсан сүрьеэгийн рентген ангилал нь эмч нарт илүү сайн шийдвэр гаргахад туслах автомат оношилгооны системийг хөгжүүлэх судалгааны сонирхолтой сэдэв болсон [8].

II. ӨГӨГДӨЛ ЦУГЛУУЛАХ, УРЬДЧИЛСАН БОЛОВСРУУЛАЛТ

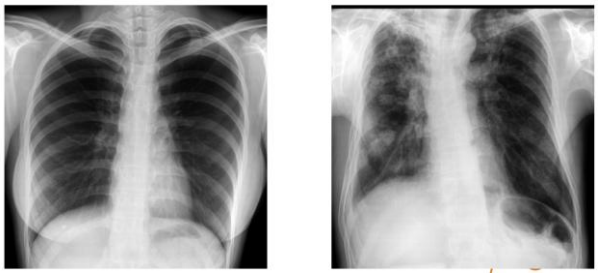
Гүн сургалт ашиглаж бодит таамаглал гаргах загвар байгуулахад тухайн загварыг сургах өгөгдлийн үнэн зөв байдал, тоо ширхэг, алдаагүй байдал хамгаас чухал байдаг. Тиймээс өгөгдлийн шинжилгээ, цэвэрлэгээ гэх мэт загвар сургахаас өмнөх өгөгдлийн боловсруулалт хийх шаардлагатай.

Дээрх судалгаанд ашиглагдсан цээжний рентген зургууд "Монгол Улс дахь сүрьеэгийн тархалтын анхны судалгааны тайлан (2014-2015)"-нд орсон тоон тоон мэдээлэл дээр тулгуурлан хийгдсэн болно.

Сүрьеэгийн тархалтын үндэсний судалгааны талбарын ажлыг 2014оны 4 дүгээр сараас 2015 оны11 дүгээр сарын хооронд (өвлийн саруудаас бусад сар)-ын хугацаанд хийж гүйцэтгэсэн. Нийт 98 кластерт 85,860 хүн тоологдсон ба тэдгээрийн 60,031 (69.9%) нь судалгаанд хамрагдах шалгуурыг хангасан байна. Ийнхүү шалгуур хангаагүй хүмүүсийн дотор 19,400 (32.3%) нь 15 хүртэлх насны хүүхдүүд, харин 6,429 (10.7%) нь оршин суух шалгуур хангаагүй хүмүүс эзэлж байв. Судалгаанд хамрагдах шалгуур хангасан 60,031 хүнээс 50,309 (83.8%) нь судалгаанд оролцсон. Судалгаанд оролцогчдоос 50,194 (99.8%) нь сүрьеэгийн шинж тэмдэг илрүүлэх асуумж судалгаанд, 49,521 (98.4%) нь цээжний рентген шинжилгээнд хамрагдаж, харин 749 оролцогч өндөр настай, хэвтэрт, хөгжлийн бэрхшээлтэй, жирэмсэн зэрэг шалтгаанаар рентген шинжилгээнд хамрагдаагүй буюу хамрагдахаас татгалзсан байна.

Сүрьеэгийн сэжиг бүхий шинж тэмдэг илэрсэн буюу цээжний рентген зураг дээр уушги, голтын өөрчлөлт илэрсэн болон цээжний рентген шинжилгээнд хамрагдах боломжгүй буюу хамрагдахаас татгалзсан оролцогчдоос цэрний нян судлалын шинжилгээнд хамрагдах шалгуурыг хангасан гэж үзсэн. Эмнэл зүйн зөвлөх багаас 88 оролцогчийг түрхэц эерэг сүрьеэгийн тохиолдол, 160 оролцогчийг түрхэц сөрөг, өсгөвөр эерэг сүрьеэгийн тохиолдол хэмээн ангилсан байна. Иймхүү нян судлалын шинжилгээгээр баталгаажсан уушгины сүрьеэтэй нийт 248 тохиолдлыг судалгаагаар илрүүлсэн байна. Эдгээрээс зөвхөн 11 тохиолдол нь судалгаанаас өмнө оношлогдсон байсан ба бусад 237 тохиолдол нь судалгаагаар илэрсэн (сүрьеэтэй гэж оношлогдоогүй ба эмчилгээ хийлгэж эхлээгүй) байна.

Төвийн дүрс оношилгооны зөвлөх мэргэжилтнүүд талбараас ирүүлсэн бүх рентген зургийг уншиж, дүгнэлт гаргаж, дотоодын хяналт хийсэн. Мөн ДЭМБ-ын зөвлөх мэргэжилтнээр рентген зургийн гадаад чанарын хяналтыг хийлгэж ажилласан [2].



1-р зураг. Эрүүл болон өвчтэй хүний уушгины харьцуулалт

Дээрх судалгааны багын тоон мэдээллээс авсан нийт 49,521 цээжний рентген зургаас 248 нь лабораторийн шинжилгээгээр баталгаажсан эрүүл, болон өвчтэй гэсэн шошго бүхий зураг 2-т үзүүлсэн байдлаар ангилсан хавтсыг хүлээн авсан. Дээрх бүх рентгений зураг нь тухайн оролцогчоос ёс зүйн болон таниулсан зөвшөөрөлтэй болно.

III. ЦЭЭЖНИЙ ЗУРГИЙН БОЛОВСРУУЛАЛТ

Олон төрлийн CNN (Convolutional Neural Network) загваруудыг судалгааны ажлуудад танилцуулсан байдаг [15-18], [20, 21]. Гүн сургалтын CNN загвар нь ихэвчлэн зургийн боловсруулалт, дүрс ангилах, объект илрүүлэх, дүрс таних гэх мэт Computer vision-ий даалгаврууд дээр хэрэглэгддэг NN (Neural Network)-н нэг төрөл юм. Энгийн NN-уудаас ялгаатай нь CNN нь зургийг филтердэх олон давхаргуудаас бүрдэх тооцоолол хийх давхаргууд (Convolutional layer), хэмжээг багасгах давхарга (Pooling layer), оролт гаралтын хоорондох дүрслэлийг гаргах давхарга (Fully connected layer) зэргээс бүрддэг.

Convolutional layer-н гол үүрэг нь оролтыг хүлээн авч, өгөгдлийг хувиргах, дараагийн давхаргад оролт болгон дамжуулдаг. Бидний оролтын утга болох 2D зураг гэдэг нь матриц юм. Математик талаас convolutional давхарга нь filter матрицаар бүх оролтын матрицийг матрицын үржвэрээр үрждэг. Ингэснээр feature map буюу

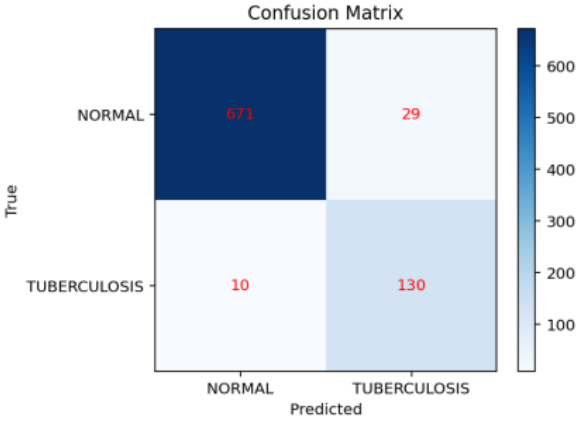
```
Input: 256x256x1
        |
        ▼
Conv2D(64, 3x3, ReLU)   → 256x256x64
        |
MaxPooling2D(2x2)        → 128x128x64
        |
Conv2D(128, 3x3, ReLU) → 128x128x128
        |
MaxPooling2D(2x2)        → 64x64x128
        |
Conv2D(256, 3x3, ReLU) → 64x64x256
        |
GlobalAveragePooling2D   → 256
        |
Dense(1, Sigmoid)        → 0 or 1 (output)
```

2-р зураг. CNN загвар, архитектур

онцлог газрын шинж чанарыг тодорхойлж гаргаж ирдэг. Харин Pooling layer гэдэг нь feature map-г 2 дахин багасгадаг давхарга юм. Convolution layer бүрийн араас энэхүү үйлдлийг хийнэ. Үүнийг хийх гол шалтгаан нь математик операци, боловсруулах хугацаа, өгөгдлийн хэмжээг багасгах явдал юм.

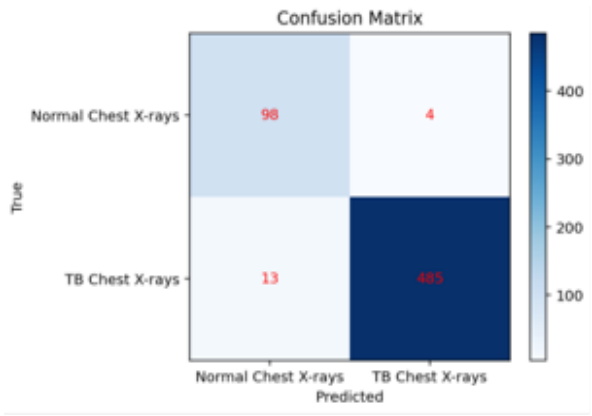
Бидний SmallCNN_model.h5 загварыг гарган авахын тулд CNN-ийн Resnet 18 загварын архитектурыг ашигласан. Уг загвар нь 8 давхаргатай байх ба Сигмойд функцээр зургийг эрүүл болон өвчтэй хэмээн ангилан үр дүн харуулна.

Туршил 1-д нээлттэй мэдээллийн сан болох Tuberculosis (TB) Chest X-ray Database –с эрүүл-1 (normal), эрүүл биш (abnormal) гэсэн ангилал бүхий 256x256 хэмжээ бүхий саарал зургийг оролтод 128x128 хэмжээтэй болгон өөрчилж зураг 2-т үзүүлсэн CNN-н загвараар ажиллуулсан. Зураг 3-т үзүүлсэн дүнгээс харахад нийт нийт 700 эрүүл зургаас 29 эрүүл зургийг өвчтэй, 140 сүрьеэтэй зургаас 10 зургийг эрүүл гэж таньсан байна.



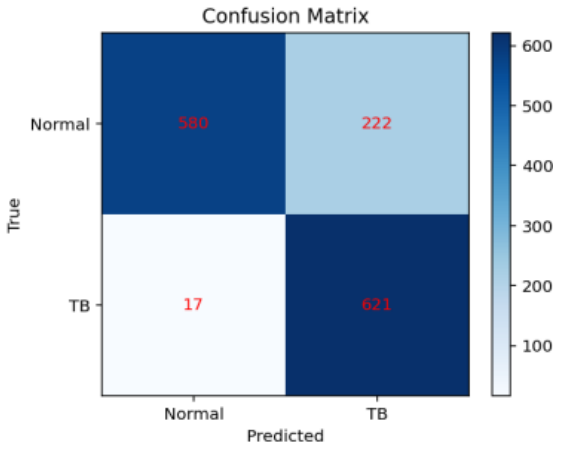
3-р зураг. Туршилт 1-ийн дүн

Туршил 2-д нээлттэй мэдээллийн сан болох Tuberculosis (TB) Chest X-ray Database –с уушгины хатгаатай болон эрүүл-2 гэсэн шошго бүхий 2 хавтас бүхий саарал зургийг оролтод 512x512 хэмжээтэй болгон өөрчилж зураг CNN-н загвараар ажиллуулсан. Зураг 4-т үзүүлсэн дүнгээс харахад оролтын өгөгдлийн тоон утгыг нэмэхэд таамаглалт илүү сайжирсан байна. Нийт 102 эрүүл зургаас 4 эрүүл зургийг өвчтэй, 471 уушгины хатгаатай зургаас 13 зургийг эрүүл гэж таньсан байна.



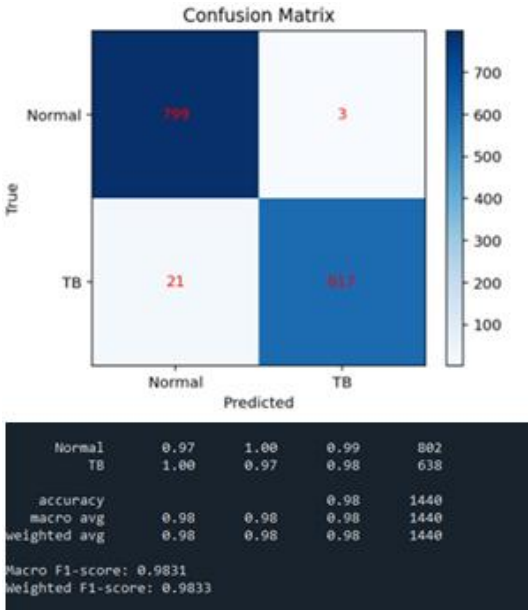
4-р зураг 4. Туршилт 2-ын дүн

Туршил 3-д нээлттэй мэдээллийн сан болох Tuberculosis (TB) Chest X-ray Database –с татаж авсан эрүүл-1 болон эрүүл-2 – г, эрүүл биш (abnormal) болон уушгины хатгаатай зуран хавтсыг нэгтгэн 4014 ширхэг эрүүл, 3194 ширхэг өвчтэй гэсэн онош бүхий 2 хавтас саарал зургийг оруулахаар бэлтгэсэн. Оролтод 256x256 хэмжээтэй болгон өөрчилж зураг CNN-н загвараар ажиллуулсан. Зураг 5-д үзүүлсэн 222 эрүүл хүнийг сүрьеэтэй гэж таамагласан нь хүлээлтээс үр дүнг харуусан. Алдааг код болон тоон өгөгдөлд хайхад зураг ялган ангилал хийхэд эрүүл зураг, хэвийн уушгины зурагтай холиолдсон байв.



5-р зураг. Туршилт 3-ын дүн

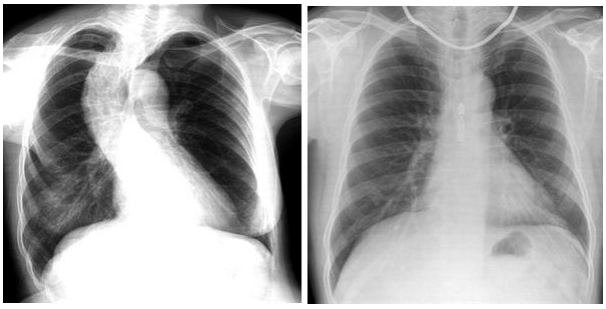
Дээрх алдааг засварлаж, оролтын хувьсагчийн тоог нэмэх зорилгоор 512x512 хэмжээтэй саарал зураг болгон өөрчилж CNN-н загвараар ажиллуулсан. Зураг 6-т үзүүлсэн дүнгээс харахад нийт 802 эрүүл зургаас 799 эрүүл зургийг таньж, 638 хэвийн бус зургаас 21 зургийг эрүүл гэж таньж, F1 score 0.98 буюу сайн үзүүлэлтийг харуулсан байна.



6-зураг. Засварласан туршилт 3-ын дүн

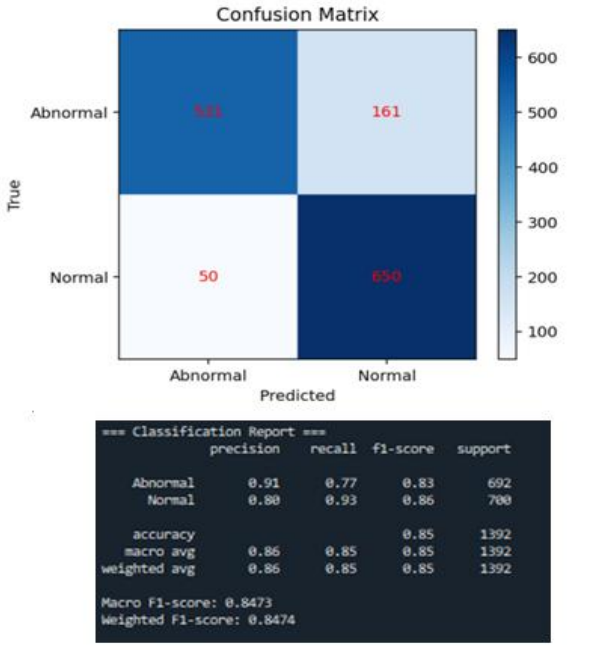
Туршил 4, 5-д судалгааны үндсэн өгөгдөл болох Монгол Улс дахь сүрьеэгийн тархалтын анхны судалгааны цээжний рентген зургуудыг ашигласан. Дээрх зургууд бүгд .dcm өргөтгөлтэй байсан тул хурдан уншигдах, CNN, KNN, ResNet гэх мэт бэлэн гүн сургалтын архитектуртай шууд нийцдэг тул бүх зургийг саарал (grayscale JPG/PNG), 512x512 хэмжээтэй болгон хувирган эрүүл уушгины 50897, хэвийн бус уушгины 248 зургийг “Normal” болон “Abnormal” гэсэн хоёр хавтаст ангилав. Хэвийн бус уушгины зургийн тоо хэвийн уушгины зургийн тооноос хэт дахин бага байгаа тул туршил 3-т ашигласан 3194 ширхэг өвчтэй гэсэн онош бүхий рентген зургийг нэмж оруулсан болно.

Туршилт 4-т тоон өгөгдлийн харьцааг ойролцоо байхаар тооцож “Normal” хавтаст 3500 эрүүл, “Abnormal” хавтаст 3460 хэвийн бус уушгины зургийг хадгалсан. “Normal” хавтаст зургийг сонгохдоо зураг 7-д үзүүлсэн гаднын биеттэй болон бүтцийн хувьд өөрчлөлттэй боловч эрүүл гэсэн оноштой зургийг оруулаагүй болно.



7-р зураг. Туршилтаас хасагдсан зураг

512x512 хэмжээтэй саарал зураг болгон өөрчилж CNN-н загвараар ажилууллав. Зураг 8-т үзүүлсэн дүнгээс харахад нийт 700 эрүүл зургаас 50 тохиолдлыг буруу таньж, 692 хэвийн бус зургаас 531 зургийг зөв таамаглаж, F1 score 0.84 буюу туршилт 3-тай харьцуулахад хангалтгүй дүнг үзүүлсэн байна.




```
=== Classification Report ===
              precision    recall  f1-score   support

    Abnormal       0.91      0.77      0.83       692
      Normal       0.80      0.93      0.86       700

    accuracy                           0.85      1392
   macro avg       0.86      0.85      0.85      1392
weighted avg       0.86      0.85      0.85      1392

Macro F1-score: 0.8473
Weighted F1-score: 0.8474
```

8-р зураг. Туршилт 4-ийн дүн

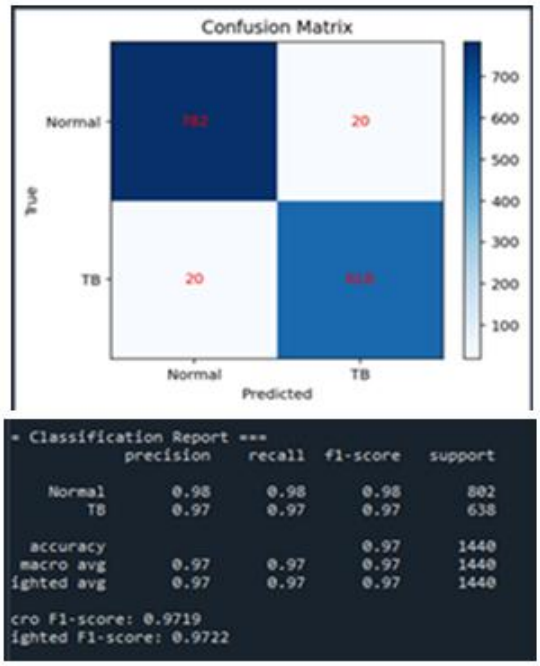
Туршил 5-д судалгааны үндсэн өгөгдөл болох Монгол Улс дахь сүрьеэгийн тархалтын анхны судалгааны цээжний рентген зургуудыг ашигласан. Эрүүл уушгины 50897, хэвийн бус уушгины 248 зургийг “Normal” болон “Abnormal” гэсэн хоёр хавтаст ангилав. Хэвийн бус уушгины зургийн тоо хэвийн уушгины зургийн тооноос хэт дахин бага байгаа тул туршил 3-т ашигласан 3194 ширхэг өвчтэй гэсэн оношбүхий рентген зургийг нэмж оруулах, өгөгдлийн тоог хиймлээр ихэсгэх “Data augmentation” гэх аргыг ашигласан. Дээрх арга нь

```
# --- Data augmentation ---
datagen_aug = ImageDataGenerator(
    rescale=1./255,
    rotation_range=10,
    width_shift_range=0.05,
    height_shift_range=0.05,
    zoom_range=0.05,
    validation_split=0.2
)
train_gen = datagen_aug.flow_from_directory(
    data_dir, target_size=IMG_SIZE, batch_size=BATCH_SIZE,
    color_mode='grayscale', class_mode='binary', subset='training', shuffle=True
)
val_gen = datagen_aug.flow_from_directory(
    data_dir, target_size=IMG_SIZE, batch_size=BATCH_SIZE,
    color_mode='grayscale', class_mode='binary', subset='validation', shuffle=False
)
```

9-р зураг. Ашигласан “Data augmentation”

сурах чадварыг сайжруулж, загварын урьдчилан таамаглах, accuracy буюу нарийвчлалыг сайжруулах боломжийг олгодог.

Дээрх аргыг ашигласан туршилт 5-г хийж SmallCNN_model.h5 загварыг гаргаж авсан. Дээрх загварын туршилтын үр дүн нийт 802 эрүүл зургаас 20 тохиолдлыг буруу таньж, 638 хэвийн бус зургаас 618 зургийг зөв таамаглаж, F1 score 0.97 буюу туршилт 4-тай харьцуулахад 0.13-аар өссөн дүнг үзүүлсэн байгааг зураг 10-т үзүүлэв.




```
= Classification Report ===
              precision    recall  f1-score   support

      Normal       0.98      0.98      0.98       802
          TB       0.97      0.97      0.97       638

    accuracy                           0.97      1440
   macro avg       0.97      0.97      0.97      1440
ighted avg       0.97      0.97      0.97      1440

cro F1-score: 0.9719
ighted F1-score: 0.9722
```

10-р зураг. Туршилт 5-ын дүн

Бид өөрийн CNN-ийн загврыг сайжруулах ажлын талбарт ойрхон, хүн бүр хэрэглэх боломжийг бүрдүүлэх үүднээс .dcm,, jpg, png аль төрлийн зураг уншиж байхаар кодолсон.

IV. ДҮГНЭЛТ

Энэхүү судалгаанд бид CNN гүн сургалтын загварыг уушгины рентген зургуудыг хэвийн ба хэвийн бус ангилалд ангилах зорилгоор боловсруулаа. Судалгааны үр дүнд тус загвар нь macro F1-score = 0.97 үзүүлж, хоёр анги хоёуланд өндөр нарийвчлалтай, тэнцвэртэй ангилалт хийж байгааг харууллаа. Энэ нь бидний SmallCNN_model.h5 нь хоёр ангийн ялгааг үр дүнтэй таньж чаддаг, overfitting бага, мөн сургалт хурдан хийгддэг давуу талыг илтгэж байна.

Гэсэн хэдий ч, загварын гүйцэтгэл өгөгдлийн төрөл, тоо хэмжээ, DICOM болон бусад эх сурвалжийн зургуудын төрөл зэрэг хүчин зүйлээс хамаарч өөрчлөгдөж болно. Тухайлбал бидний эхний 4 туршилтын тоон өгөгдөл нээлттэй сангаас авсан цөөн тооны рентген зураг байсан бол туршилт 5-н өгөгдөл эрүүл уушгины зургийн тоо хэвийн бус уушгины зургийн тооноос хэд дахин их байсан. Ирээдүйд өгөгдлийн сантай өргөжүүлэх, transfer learning ашиглах, бусад гүн сургалтын архитектурыг туршиж үзэх зэрэг аргуудыг нэвтрүүлснээр загварын гүйцэтгэлийг илүү сайжруулах боломжтой.

Дүгнэж хэлэхэд бидний CNN загвар нь уушгины өвчлөлийг эрт илрүүлэх, клиникийн тусламж үйлчилгээний процессыг дэмжих зорилгоор бодит хэрэглээнд нэвтрүүлэх боломжтой, үр дүнтэй, хөнгөн загвар болохыг харууллаа.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Эрүүл мэндийн сайдын 2024 оны 01 сарын 29-ний өдрийн а/58 тоот тушаалын наймдугаар хавсралт. Сүрьеэгийн илэрүүлэлт, оношилгоо, эмчилгээний заавар.

[2] Монгол Улс дахь сүрьеэгийн тархалтын анхны судалгааны тайлан.

[3] Turner RD, Bothamley GH. Cough and the transmission of tuberculosis. J Infect Dis 2015; 211:1367–72.

[4] Gavin Churchyard, Peter Kim, N.Sarita Shah, Roxana Rustomjee, Neel Gandhi, Barun Mathema, David Dowdy, Anne Kasmar, Vicky Cardenas “What We Know About Tuberculosis Transmission: An Overview”

[5] World Health Organization. Systematic screening for active tu berculosis: principles and recommendations. WHO/HTM/ TB/2013.04. Geneva, Switzerland: WHO, 2013.

[6] World Health Organization. Tuberculosis prevalence surveys: a handbook. WHO/HTM/TB/2010.17. Geneva, Switzerland: WHO, 2011.

[7] Pai M, Behr MA, Dowdy D, Dheda K, Divangahi M, Boehme CC, et al. Tuberculosis. Nat Rev Dis Primers. 2016;2:16076.

[8] Arief Rachman Hakim, Budi Warsito, Muhammad Rionando Divangga, Diah Safitri, Ardiana Alifatus Sa’adah “Performance convolutional neural network (CNN) and support vector machine (SVM) on tuberculosis disease classification based on X-ray image”

[9] Bird, Jordan J., et al. "A study on CNN image classification of EEG signals represented in 2D and 3D." Journal of Neural Engineering 18.2 (2021): 026005.

[10] Wen, Tingxi, et al. "A deep learning-based classification method for different frequency EEG data." Computational and Mathematical Methods in Medicine 2021 (2021).

[11] Zou, Guoxia. "The Recognition of Action Idea EEG with Deep Learning." Complexity 2022 (2022): 1-13.

[12] Dai, Guanghai, et al. "HS-CNN: a CNN with hybrid convolution scale for EEG motor imagery classification." Journal of neural engineering 17.1 (2020): 016025.

[13] Lun, Xiangmin, et al. "A simplified CNN classification method for MI-EEG via the electrode pairs signals." Frontiers in Human Neuroscience 14 (2020): 338.

[14] Liu, Tianjun, and Deling Yang. "A three-branch 3D convolutional neural network for EEG-based different hand movement stages classification." Scientific Reports 11.1 (2021): 10758.

DESIGN OF CONTACTLESS IDENTITY AUTHENTICATION SYSTEM FOR PUBLIC HEALTH PLACES BASED ON FACIAL RECOGNITION

HAILIN Tang[1, 2], YONGJUN Qi[1, 2], KHUDER Altangerel [2], ZAGARZUSEM Khurelbaatar [2]

[1] Faculty of Megadata and Computing, Guangdong Baiyun University, China
[2] School of Information and Communication Technology, Mongolian University of Science and Technology, Mongolia

Abstract: ***In the context of frequent public health incidents, the safety management of public health places is particularly important. Traditional identity authentication methods have problems such as strong contact and low efficiency, making it difficult to meet the requirements of fast, efficient, and contactless authentication. The contactless identity authentication system based on facial recognition technology can not only effectively prevent and control the spread of infectious diseases, but also improve the intelligence level of personnel flow management. Firstly, based on the requirements analysis, the overall architecture of the system was designed, including the facial recognition module, data processing module, and user interface module. The system adopts deep learning algorithms for face recognition, ensuring high accuracy and fast response. Secondly, select a large public health facility as the experimental site for systematic deployment and testing. During the experiment, facial image data of 1000 users were collected and identity authentication tests were conducted. The data analysis adopts descriptive statistics and comparative analysis to evaluate the recognition accuracy, response time, and user satisfaction of the system. In addition, conduct privacy protection assessments to ensure that the system complies with relevant laws and regulations during data processing. The study analyzed the contactless identity authentication system for facial recognition, the recognition accuracy of the system is as high as 98.5%, significantly better than traditional authentication methods, with a response time of only 350 milliseconds, meeting the requirements of fast authentication. The false recognition rate and rejection rate are 0.5% and 1.2%, respectively, indicating that the system performs well in terms of security. The system stability reaches 99.9%, ensuring reliability during long-term operation. The user satisfaction rating reached 4.7 points, reflecting the high recognition of the system by users.***

Keywords: facial recognition; public health; contactless; privacy protection; identity authentication

I. INTRODUCTION

In recent years, global public health events have occurred frequently, bringing unprecedented challenges to the security management and personnel flow control of public places. Traditional identity authentication methods, such as card swiping and fingerprint recognition, have problems such as strong contact, low authentication efficiency, and high risk of cross-infection, and can no longer meet the dual needs of epidemic prevention and control and efficient management [1]. In this context, how to achieve contactless, efficient, and secure identity authentication in public health places has become an important topic of common concern in academia and industry. As a mature biometric recognition technology, face recognition has been widely used in financial payment, social security, and smart travel due to its advantages such as non-contact, ease of use, and fast recognition speed [2]. Compared with traditional authentication methods, face recognition can complete real-time identity verification without increasing the burden on users, which helps to improve the management efficiency and prevention and control capabilities of public health places [3]. However, existing face recognition systems still face several challenges in actual deployment. First, the robustness in complex environments is insufficient. For example, factors such as wearing masks, lighting changes, and partial occlusion will significantly affect the recognition accuracy. Second, privacy and security issues are prominent, and the legality and compliance of face data collection, storage, and use need to be urgently addressed [4]. Third, the system lacks stability and scalability, and authentication delays or failures may still occur in high-concurrency and large-scale crowd scenarios[5]. To address these issues, this study designed a contactless identity authentication system for public health facilities based on facial recognition. The system is based on a deep learning algorithm and combines liveness detection with data encryption mechanisms to achieve both scalability and stability. The research aims to provide technical support for identity authentication in the context of public health events, while also providing practical reference for the construction of future smart cities and digital governance.

1. CONTACTLESS IDENTITY AUTHENTICATION IN PUBLIC HEALTH PLACES

1.1 CONTACTLESS IDENTITY AUTHENTICATION SYSTEM DESIGN

To address the challenges of traditional public health facility identity authentication methods, which are characterized by high contact, low efficiency, and the risk of cross-infection, this study proposes a contactless identity authentication system for public health facilities based on facial recognition. This system utilizes a modular and layered architecture, consisting of three main modules: facial recognition, data processing, and

user interaction. Figure 1 shows the main functions of these three modules.

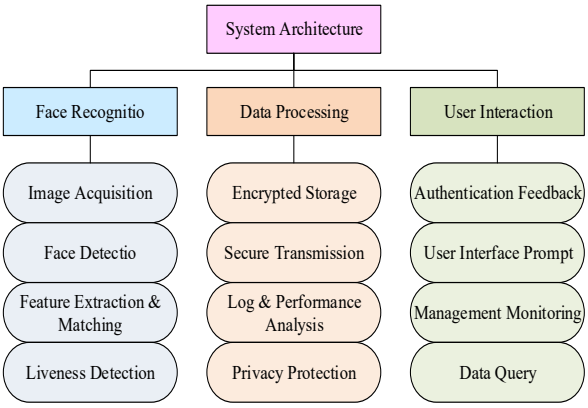


Figure 1 Main functions of the three modules

As shown in Figure 1, the three modules independently undertake different tasks, but also form an organic synergy in the overall operation of the system to jointly ensure the accuracy, security and availability of identity authentication. First, the face recognition module undertakes the core tasks of front-end perception and feature analysis. This module obtains user facial information through image acquisition equipment and uses deep learning algorithms to perform face detection, thereby quickly and accurately locating the face area under complex backgrounds. After the detection is completed, the system further extracts facial features and matches them, and completes identity recognition by establishing a high-dimensional feature vector and comparing it with the user database. At the same time, the module also introduces a liveness detection mechanism that can effectively distinguish real faces from photos, videos and other attack methods, thereby improving the security of authentication [6]. This module is not only the "entrance" of the entire system, but also the key to ensuring recognition efficiency and accuracy.

Secondly, the data processing module plays the role of the system's "hub," primarily responsible for secure data storage, transmission, and privacy protection. This module encrypts and stores the collected user feature data to ensure that sensitive information is not leaked; it introduces secure communication protocols during data transmission to prevent interception or tampering [7]. In addition, the data processing module also includes logging and performance analysis functions, which can track and analyze various indicators during system operation, providing a basis for subsequent system optimization. More importantly, this module has a built-in privacy protection mechanism, which follows the principles of minimizing storage and anonymization in its design, ensuring that the use of facial data complies with the strict constraints of laws, regulations, and ethical requirements in public health settings.

Finally, the user interaction module serves as the interface for direct communication between the system and users, serving both regular users and facility managers. For regular users, this module ensures a streamlined and efficient authentication process and clear, intuitive information flow through identity authentication feedback and user-friendly interface prompts. For managers, this module provides operational status monitoring, data query, and permission control, enabling real-time visibility into facility operations and enabling timely maintenance and adjustments. This module not only enhances the user experience but also strengthens public health facilities' ability to manage crowd flow and oversee safety at the management level.

1.2 IMPLEMENTATION OF CONTACTLESS IDENTITY AUTHENTICATION TECHNOLOGY

Based on the system architecture, the study optimized the design of the contactless identity authentication process. The core of the system lies in the integration of facial recognition algorithms and data security mechanisms. Through front-end acquisition, feature extraction and comparison, liveness detection, and back-end data processing and feedback, an efficient, stable, and secure closed-loop operation is formed. At the front end, the system first uses a camera to capture the user's facial image in real time and uses face detection and alignment technology to quickly locate the facial area against complex backgrounds. Subsequently, the image undergoes preprocessing steps such as illumination normalization and denoising to reduce the interference of environmental factors on recognition accuracy. Based on this, a deep convolutional neural network is used to extract high-dimensional feature vectors and compare them with the features of registered users in the database for similarity, thereby completing identity recognition[8-9]. To prevent deceptive attacks such as photos or videos, the system introduces a liveness detection mechanism into the recognition process, effectively determining the authenticity of the face through motion recognition and infrared imaging.

In the middle and back-end links, the data processing module plays an important role in system security and privacy protection. The collected feature data are encrypted using the Advanced Encryption Standard (256 bit) (AES-256) before storage, and secure communication is achieved through the Transport Layer Security/Secure Sockets Layer (TLS/SSL) during transmission , thereby preventing data from being stolen or tampered with on the network [10]. At the same time, the system follows the principles of minimizing storage and anonymization, avoiding long-term storage of original images to minimize the risk of privacy leakage. In addition, the data processing module is also responsible for log recording and performance analysis, which facilitates subsequent operation monitoring and system optimization. The entire process of contactless identity authentication is shown in Figure 2.

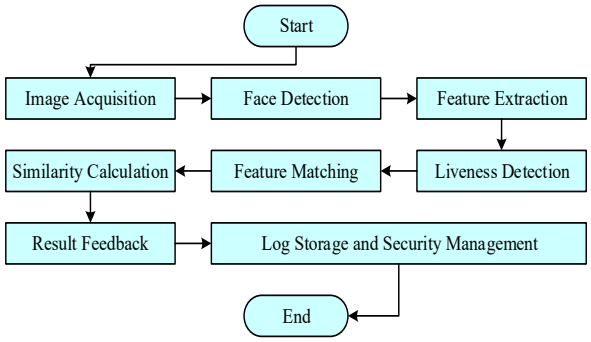


Figure 2 Overall process of the contactless identity authentication system

As shown in Figure 2, the system completes the entire process, from face acquisition to feature extraction and authenticity verification, on the front end, submitting the results to the back end for comparison and verification. Once the comparison result passes the threshold, the system immediately generates authentication feedback and simultaneously records it in the back-end database to ensure real-time and traceable results. This process design not only achieves efficient and accurate identity authentication technically, but also strengthens data security and privacy protection mechanisms, ensuring stable and reliable operation in public health settings.

II. CONTACTLESS IDENTITY AUTHENTICATION SYSTEM VERIFICATION

2.1 SYSTEM PERFORMANCE TEST

To verify the performance of the designed contactless identity authentication system in a real-world public health setting, this study selected a large public health facility as an experimental environment. Front-end high-definition cameras, edge computing units, and back-end servers were deployed to form a complete test platform. The experimental subjects were 1,000 registered users, whose facial images were captured and their identities authenticated in real time. The entire experimental environment simulated the actual operating conditions of a public health facility, ensuring that the test results were relevant and relevant. The results are shown in Table 1.

TABLE 1 PERFORMANCE ANALYSIS OF IDENTITY AUTHENTICATION SYSTEM BASED ON FACIAL RECOGNITION

Index	Recognition accuracy /%	Response time/ms	FAR/%
Numerical value	98.5	350	0.5
Index	FRR/%	System stability	User satisfaction rating
Numerical value	1.2	99.90%	4.7

Table 1 shows that the system's recognition accuracy reached 98.5%, and the authentication response time was only 350 ms, significantly shorter than traditional contact-based authentication methods. The false recognition rate and rejection rate were 0.5% and 1.2%, respectively, demonstrating that the system maintains high efficiency while also balancing security and reliability. Furthermore, system stability remained at 99.9%, with virtually no failures during long-term operation. The average user satisfaction rating was 4.7, demonstrating a high level of user appreciation for the system's convenience and security.

2.2 Stability and Concurrency Stress Testing

Considering the high traffic and frequent access requests typical of public health facilities, evaluating system performance solely in a single-user environment is insufficient to fully reflect its application value. Therefore, this study further conducted stability and concurrency stress tests on the system, primarily involving long-term continuous operation and multi-user concurrent authentication. The results are shown in Table 2.

TABLE 2 RESULTS OF SYSTEM STABILITY AND CONCURRENT PERFORMANCE TESTS

Test Scenario	Average Response Time / ms	Authentication Success Rate/%	System St ability
Continuous operation (72 hours)	Fluctuation < 5%	99.9	No failure
Concurrent 10 users	360	98.3	Stable
Concurrent 50 users	410	97.5	Stable
Concurrent 100 users	480	96.8	Stable
Concurrent 200 users	620	95.1	Stable

Table 2 shows that during the 72-hour stability test, the system's response time fluctuated less than 5%, the authentication success rate reached 99.9%, and no failures were observed. This demonstrates that the system maintains high reliability even under long-term, uninterrupted operation, meeting the long-term safety and security requirements of public health facilities. In concurrent testing, although response time increased with the number of users, the authentication success rate remained above 95%, and the system remained stable, demonstrating its strong reliability and practicality in a highly concurrent environment.

III. CONCLUSION

To address the challenges of traditional identity authentication methods in public health facilities, such as high contact requirements, low efficiency, and the risk of cross-infection, this study proposed a contactless identity authentication system based on facial recognition. Experimental results demonstrate that the system achieves 98.5% recognition accuracy, an average

response time of only 350 ms, false positive and rejection rates of 0.5% and 1.2%, respectively. System stability remains at 99.9%, and user satisfaction is 4.7% . Even with 200 concurrent users, the authentication success rate remains above 95%, fully demonstrating the system's efficiency and reliability. These results demonstrate that the system not only meets the urgent need for efficient identity authentication in public health facilities, but also balances data security and privacy protection, providing strong support for intelligent public health management. However, the system's recognition rate decreases in complex environments such as mask occlusion, varying lighting conditions, and partial occlusion. Furthermore, the privacy protection mechanism relies primarily on traditional encryption methods. Future work can further enhance the robustness and privacy protection of the system by optimizing deep learning algorithms, introducing federated learning and blockchain technologies, and strengthening integration with access control and crowd flow monitoring systems, thereby promoting intelligent management of public health facilities.

IV. REFERENCES

[1] Raposo V L, Du L. Facial recognition technology: is it ready to be used in public health surveillance?[J]. International Data Privacy Law, 2024, 14(1): 66-86.

[2] Taha M E, Mostafa T, Abd El-Rahman T A E H. A novel hybrid approach to masked face recognition using robust PCA and GOA optimizer[J]. Scientific Journal for Damietta Faculty of Science, 2023, 13(3): 25-35.

[3] Ullah N, Javed A, Ghazanfar M A, et al. A novel DeepMaskNet model for face mask detection and masked facial recognition[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(10): 9905-9914.

[4] O'Neill C. Disaster, facial recognition technology, and the problem of the corpse[J]. new media & society, 2024, 26(3): 1333-1348.

[5] Ryando C, Sigit R, Setiawardhana S, et al. Face Recognition for Logging in Using Deep Learning for Liveness Detection on Healthcare Kiosks[J]. JOIV: International Journal on Informatics Visualization, 2025, 9(1): 295-302.

[6] Al-Mutairi Z, Al-Qahtani K A. Facial Recognition for Student Attendance in Pandemic Contexts: A Deep Transfer Learning Approach[J]. Frontiers in Emerging Computer Science and Information Technology, 2025, 2(4): 10-12.

[7] Raposo V L. The use of facial recognition technology by law enforcement in Europe: a non-orwellian draft proposal[J]. European journal on criminal policy and research, 2023, 29(4): 515-533.

[8] Pourrostami H, AlyanNezhadi M M, Nazari M, et al. Deep learning for electroencephalography emotion recognition[J]. AIMS Public Health, 2025, 12(3): 812-834.

[9] Yang X, Xu L, Pang T, et al. Face3DAdv: Exploiting Robust Adversarial 3D Patches on Physical Face Recognition[J]. International Journal of Computer Vision, 2025, 133(1): 353-371.

[10] Rajpal A, Sehra K, Bagri R, et al. Xai-fr: explainable ai-based face recognition using deep neural networks[J]. Wireless Personal Communications, 2023, 129(1): 663-680.

ЭХ ХЭЛНИЙ БОЛОВСРУУЛАЛТЫГ АШИГЛАН ЧАТБОТЫН ХАРИЛЦААНЫ ЧАНАРЫГ САЙЖРУУЛАХ СУДАЛГАА

Батмөнхийн ЭРДЭНЭМАНДАЛ[1], Соном-Очирын ӨЛЗИЙБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээлэл технологийн салбар

Холбоо барих зохиогчийн и-мэйл хаяг: erdenemandal.b@must.edu.mn[1]

Хураангуй: **Энэхүү судалгааны ажлын зорилго нь монгол хэлэнд нийцсэн байгалийн хэлний боловсруулалтын (NLP) аргачлалыг ашиглан чатботын харилцааны чанарыг сайжруулахад оршино. Судалгаанд Qwen 2.5, LLaMA 3, GPT-4-turbo зэрэг орчин үеийн том хэмжээний хэлний загваруудыг ашиглаж, монгол хэлний үг зүйн нарийн бүтэцтэй тохирох SentencePiece болон Byte-Pair Encoding (BPE) токенчлолын аргуудыг нэгтгэн хэрэгжүүлсэн. Системийг HuggingFace Transformers ба PyTorch хүрээн дээр хөгжүүлж, серверийн талын уялдаа холбоог FastAPI болон Flask framework-уудаар дамжуулан хэрэгжүүлсэн. Бидний санал болгож буй аргачлал нь хэрэглэгчийн ролт, монгол хэлний токенчлол, хэлний загварын боловсруулалт, хариулт үүсгэх шат дамжлагыг цогцоор нь багтаасан бүтэцтэй.**

Түлхүүр үг: ***NLP, LLM, Fine-tuning, Embedding***

I. УДИРТГАЛ

Хиймэл оюун ухааны салбарын огцом хөгжил нь хүн төрөлхтнийг улам нарийн төвөгтэй асуудлуудыг шийдвэрлэх чадвартай, машин төвтэй нийгэм рүү алхам алхмаар ойртуулж байна. Сүүлийн жилүүдэд хүн ба машины хоорондын харилцааг хялбаршуулах, автоматжуулах зорилгоор **Chatbot** технологийн хөгжүүлэлт, хэрэглээ эрс нэмэгдсэн билээ. **Chatbot** буюу хиймэл оюунд суурилсан ярианы туслах нь эх хэлний боловсруулалт буюу (NLP — *Natural Language Processing*)-ийг ашиглан хүнтэй шууд харилцаж, тэдний хүсэлтийг ойлгож гүйцэтгэх чадвартай компьютерийн програм юм [1]. Эх хэлний боловсруулалт (NLP) нь хиймэл оюун ухааны дэд салбар бөгөөд компьютерийг хүний хэлний оролтоос утга, логик, сэтгэлзүйн өнгө аяс хүртэл ялган ойлгох чадвартай болгодог. Энэ нь өгөгдлийг хэл зүйн болон утга зүйн түвшинд задлан шинжилж, хэлний бүтцийн шат дарааллыг ашиглан хүний хэлний логикийг загварчилдаг. Үгс нийлж хэлц үг үүсгэж, хэлц үгс нийлж өгүүлбэр, өгүүлбэрүүд нийлж бодол, санаа илэрхийлдэг гэсэн хэлний шаталсан зарчимд тулгуурладаг [2]. Хэдийгээр хүний хэлийг компьютерт ойлгуулах нь асар их ач холбогдолтой боловч, хэлний утгын олон давхар утгачилал, үг хэллэгийн холбогдол, сэтгэлзүйн өнгө аяс, мөн өгүүлбэрийн бүтэц, утга зөрүү зэрэг нь хиймэл оюуны системд томоохон сорилт үүсгэдэг. Хүний хэл нь зөвхөн үгийн утгаар хязгаарлагдахгүй, соёлын онцлог, нөхцөл байдал, өгүүлбэрийн интонац зэрэг олон хүчин зүйлсийг хамардаг тул үүнийг бүрэн ойлгох нь NLP-ийн хөгжлийн хамгийн том бэрхшээлүүдийн нэг юм.

Өнөө үед олон байгууллага, боловсролын болон үйлчилгээний байгууллагууд виртуал туслахууд буюу Chatbot системийг хэрэглэгчдэд дэмжлэг үзүүлэх зорилгоор ашиглаж байна [3,4]. Chatbot-ийн 24 цагийн турш тасралтгүй ажиллагаа, түргэн хариу өгөх чадвар, зардал багатай байдал, болон хэрэглэгчийн туршлагыг сайжруулах зэрэг давуу талууд нь байгууллагуудын дунд өргөн хэрэглэгдэх шалтгаан болж байна. Судлаачдын таамаглаж буйгаар ойрын жилүүдэд chatbot технологи нь уламжлалт ярианы програмуудыг бүрэн орлох төлөвтэй байна [5].

Мөн chatbot систем нь ухаалаг гар утас, таблет зэрэг зөөврийн төхөөрөмжүүд дээр улам өргөн нэвтэрч байгаа бөгөөд тэдгээрийн хялбар интерфэйс, хэрэглэгчийн зан төлөвт дасан зохицох чадвар, болон өөрийн сургалтын алгоритмаар дамжуулан тасралтгүй сайжрах боломж нь хэрэглэгчийн сэтгэл ханамжийг нэмэгдүүлж байна. Төгс chatbot нь зөвхөн асуултад хариулах бус, хэрэглэгчийн ярианы утга, сэдэв, сэтгэлзүйн өнгө аясыг ойлгож, өмнөх харилцаанаас суралцан өөрийгөө сайжруулдаг байх ёстой.

II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Chatbot буюу “ярианы бот” нь хүний яриаг дуурайлган интернет орчинд харилцах чадвартай компьютерийн програм юм. Энэхүү ойлголтын анхны хувилбар болох **Chatterbot**-ийг 1994 онд Майкл Маулдин (Michael Mauldin) бүтээж, *Verdot* нэртэй эхний chatbot системийг гаргасан байдаг [6].

Ярианы системүүдийн гол зорилго нь — хэрэглэгчтэй харилцахдаа хүнтэй ярилцаж байгаа мэт мэдрэмж төрүүлэхүйц, бодитой харилцааг бий болгох явдал юм. Энэ санааг хамгийн анх 1950 онд **Алан Тюринг (Alan Turing)** өөрийн алдарт “Тюрингийн туршилт”-аар дэвшүүлсэн байдаг [7]. Түүний туршилтад гурван оролцогч — нэг эрэгтэй, нэг эмэгтэй, нэг асуумжлагч (interrogator) оролцсон бөгөөд туршилтын зорилго нь асуумжлагч нь хэн хүн болохыг зөв тодорхойлж чадах эсэхийг шалгах байв. Энэхүү туршилт нь машины оюун ухааныг хүний сэтгэх чадвартай харьцуулах суурь үзэл

баримтлал болж, chatbot-ийн хөгжлийн эхлэлийг тавьсан юм.

Үүнээс арав гаруй жилийн дараа, 1966 онд **ELIZA** хэмээх анхны олон нийтэд зориулсан chatbot бүтээгдсэн [8]. Энэ нь урьдчилан тодорхойлогдсон дүрэм, ярианы сценарийг ашиглан хэрэглэгчтэй энгийн хэлбэрийн харилцаа үүсгэх чадвартай байсан боловч мэдлэгийн хүрээ хязгаартай байв. Дараа нь **PARRY** нэртэй chatbot нь сэтгэл заслын эмчилгээний орчныг дуурайлган, сэтгэлзүйн өвчтэй өвчтөн ба сэтгэл зүйчийн хоорондох яриаг симуляцлах байдлаар бүтээгдсэн.

ELIZA болон **PARRY** хоёул адил ярианы урсгалын арга барилыг ашигласан [9]. ELIZA нь хэрэглэгчийн хариултанд үндэслэн асуулт буцааж тавьж, ярианы урсгалыг өөрөөсөө холдуулдаг байсан бол PARRY нь “өгүүлэмжтэй яриа”-ны загварыг ашиглан тухайн нөхцөл байдлыг дүрслэх богино түүхэн элементүүдийг ярианд оруулдаг байв.

Хожим нь **ALICE (Artificial Linguistic Internet Computer Entity)** хэмээх chatbot-ийг **Ричард Уоллес (Richard Wallace)** бүтээж, ELIZA-ийн зарим шинжийг сайжруулан олон хэллэгийн загвар нэмсэн бөгөөд үүнийг **нээлттэй эх кодтой (open-source)** байдлаар хөгжүүлсэн нь chatbot-ийн мэдлэгийн санг өргөжүүлэхэд хувь нэмэр оруулсан [10].

21-р зууны эхээр **chatbot технологи** арилжааны салбарт эрчимтэй нэвтэрч, хэрэглэгчийн үйлчилгээ, харилцааны автоматжуулалт, мэдээллийн хүргэлт зэрэг олон чиглэлд хэрэглэгдэх болсон. 2001 онд бүтээгдсэн **SmarterChild** хэмээх chatbot нь тухайн үеийн хиймэл оюун ухаанд суурилсан ярианы системүүдийн дундаас шинэлэг дэвшилттэй хувилбар байлаа [11].

SmarterChild нь **AOL Instant Messenger (AIM)** болон **MSN Messenger** зэрэг тэр үеийн онлайн чат платформууд дээр ажиллаж, хэрэглэгчийн асуултад бодит цагийн горимоор хариу өгч чаддаг байсан. Тухайлбал, хэрэглэгчид түүнээс тухайн өдрийн **цаг агаар, киноны хуваарь, улс орны хүн амын тоо, спортын мэдээ, хувьцааны ханш** зэрэг бодит мэдээллийг асуухад систем яг тухайн мөчид хариулт өгдөг байв. Энэ чадвар нь SmarterChild-ийг тухайн үеийн хувийн виртуал туслахуудын эхлэл болгон нэрлэгдэх үндэс болсон юм.

SmarterChild нь цаашдын **арилжааны chatbot системүүдийн суурь архитектур** болон хөгжлийн зарчмыг тавьсан гэж үздэг. Түүний **хэрэглэгчийн өгөгдлөөс суралцах (adaptive learning)** чадвар, **дараалсан харилцан яриаг ойлгох**, **хэлний бүтэц таних** зэрэг шинжүүд нь дараа дараагийн ухаалаг туслахууд болох **Google Assistant, Microsoft Cortana, Apple Siri, Amazon Alexa** зэрэг системүүдийн хөгжлийн үндэс болсон [12].

Эдгээр орчин үеийн chatbot болон виртуал туслахууд нь зөвхөн **бичвэрийн оролт (text input)** дээр тулгуурлахаа больж, **дуу хоолой таних (speech recognition)** болон **дуу хоолой үүсгэх (speech synthesis)** технологийг нэгтгэн ашиглаж эхэлсэн нь хүн ба машины хоорондын харилцааг илүү бодитой, байгалийн болгосон. Үүний үр дүнд хэрэглэгчид төхөөрөмжтэй “ярилцах” хэлбэрээр команд өгөх, хайлт хийх, үйлдэл гүйцэтгэх боломжтой болсон юм.

Түүнчлэн эдгээр системүүд нь **хиймэл оюун ухааны машин сургалт (machine learning)** болон **мэдээлэл цуглуулах дата аналитикс** технологийн тусламжтайгаар хэрэглэгчийн зан төлөв, хэллэгийн хэв маягийг дүн шинжилж, тухайн хэрэглэгчид тохирсон хувийн хариулт, санал болгож чаддаг болсон.

Ингэснээр chatbot технологи нь анх энгийн текстэн харилцаанаас эхэлж, өнөөдөр хүний ярианы өнгө аяс, сэтгэл хөдлөлийг хүртэл тодорхойлох чадвартай, **интерактив, дасан зохицох чадвартай, өндөр түвшний хиймэл оюун ухааны туслах** хэлбэрт хүрсэн юм.

III. АШИГЛАГДАХ ТЕХНОЛОГИ

Энэхүү судалгааны ажлын хүрээнд чатботын харилцааны чанарыг сайжруулах зорилгоор эх хэлний боловсруулалт (Natural Language Processing, NLP)-ын чиглэлд өргөн хэрэглэгддэг орчин үеийн технологиудыг ашиглах болно. Судалгааны системийн архитектур нь хэлний загварын сургалт, өгөгдлийн удирдлага, серверийн бүтэц болон токенчлолын үйл явц зэрэг дэд бүрэлдэхүүн хэсгүүдээс бүрдэх бөгөөд дараах технологиудыг сонгон хэрэглэхээр төлөвлөж байна.

3.1. HuggingFace Transformers ба PyTorch

Судалгааны ажлын хүрээнд хэлний загварын сургалт болон нарийн тохиргоог (fine-tuning) гүйцэтгэхэд HuggingFace Transformers ба PyTorch хүрээнүүдийг ашиглана. Эдгээр технологиуд нь орчин үеийн байгалийн хэлний боловсруулалтын (NLP) судалгаанд өргөн хэрэглэгддэг бөгөөд гүн сургалтын архитектурыг өндөр уян хатан, өргөтгөх боломжтой байдлаар хэрэгжүүлэх нөхцөлийг бүрдүүлдэг.

PyTorch нь 2016 онд Meta (хуучнаар Facebook AI Research)-ийн багийн зүгээс боловсруулагдсан, нээлттэй эхийн гүн сургалтын хүрээ (deep learning framework) юм. Энэ хүрээ нь динамик тооцооллын граф (dynamic computation graph) ашигладаг гэдгээрээ онцлог бөгөөд загварын архитектурын бүтцийг сургалтын явцад уян хатан өөрчлөх боломж олгодог. Ийм шинж чанар нь туршилтын шатанд янз бүрийн архитектурын хувилбаруудыг хялбар турших, алдаа засах, параметрийн тохиргоог давтан сайжруулахад нэн тохиромжтой нөхцөл бүрдүүлдэг. PyTorch нь GPU-ийн тооцоолол дэмждэг тул том

хэмжээний хэлний загваруудыг үр ашигтай сургах боломжтой бөгөөд TorchScript, autograd зэрэг дэд модулиуд нь автомат дифференциалчлал (automatic differentiation)-ыг хэрэгжүүлдэг.

Харин HuggingFace Transformers нь 2019 онд гарсан, олон төрлийн урьдчилан сургагдсан (pre-trained) хэлний загваруудыг нэгтгэн хэрэглэхэд зориулсан өндөр түвшний сан (library) юм. Энэхүү хүрээ нь BERT, RoBERTa, GPT, T5, LLaMA, Qwen зэрэг Transformer архитектурт суурилсан 1000 гаруй загварыг дэмждэг бөгөөд судлаачид болон хөгжүүлэгчдэд эдгээрийг шууд ашиглах, өөрийн өгөгдөлд тохируулан дахин сургах (fine-tuning) боломжийг олгодог. Transformers хүрээний гол онцлог нь модульчлагдсан загварын бүтэц, pre-trained жинүүдийн нийцтэй байдал, Tokenizer болон Trainer API-ийн тусламжтайгаар сургалтын процессыг оновчтой, дахин ашиглагдахуйц байдлаар хэрэгжүүлэхэд оршино.

Судалгааны хүрээнд эдгээр хоёр технологийн нэгдэл нь chatbot-ийн хэл боловсруулалтын чанарыг сайжруулах, хариултын уялдаа болон логик холбоог нэмэгдүүлэх үндсэн үүрэгтэйгээр ашиглагдана. HuggingFace нь Qwen, LLaMA, GPT зэрэг олон хэлний загварыг төвлөрүүлсэн тул монгол хэлний өгөгдөл дээр эдгээрийг дахин сургаж, харьцуулалт хийх боломжийг бүрдүүлнэ. PyTorch-ийн уян хатан сургалтын орчин, HuggingFace-ийн интеграцийн дэмжлэгийн хамтаар судалгаанд ашиглагдах chatbot-ийн хэлний ойлголт, найруулгын нарийвчлалыг системтэйгээр сайжруулах нөхцөл бүрдэх юм.

Эцэст нь, HuggingFace Transformers ба PyTorch-ийн хослол нь энэхүү судалгаанд загварын сургалт, туршилт, гүйцэтгэлийн үнэлгээг нэгтгэн хэрэгжүүлэх үндсэн технологийн суурь болж, chatbot системийн хэлний боловсруулалтын чанарыг оновчтой болгох шинжлэх ухааны үндэслэл бүхий орчныг бүрдүүлнэ.

3.2. FastAPI болон Flask

Chatbot системийн серверийн хэсгийг хэрэгжүүлэхэд FastAPI болон Flask framework-уудыг ашиглана. Эдгээр нь Python хэл дээр суурилсан, RESTful архитектурын зарчмаар ажилладаг бөгөөд хэрэглэгчийн интерфейс болон хэлний загварын хооронд өгөгдлийн урсгалыг зохицуулах гол үүрэгтэй технологиуд юм.

FastAPI нь орчин үеийн, өндөр гүйцэтгэлтэй backend хөгжүүлэлтийн framework бөгөөд Starlette болон Pydantic модулиудын суурин дээр бүтээгдсэн. Энэ технологи нь асинхрон хүсэлт боловсруулах чадвартай тул олон зэрэгцээ хэрэглэгчийн хүсэлтийг нэгэн зэрэг боловсруулах, бодит цагийн (real-time) чатботын харилцаанд тогтвортой ажиллах нөхцөлийг бүрдүүлдэг. FastAPI нь OpenAPI, JSON Schema стандартыг дагадаг тул API-ийн автоматаар үүсгэх баримтжуулалт (auto-documentation) болон өгөгдлийн баталгаажуулалтыг дотооддоо хялбар хэрэгжүүлэх боломжийг олгодог. Энэхүү чанар нь системийг өргөтгөх, интеграц хийх, туршилт, засвар арчилгаанд үр ашигтай орчин бүрдүүлдэг.

Flask нь Python хэл дээр бичигдсэн, минималист (microframework) шинж чанартай framework бөгөөд анхан шатны backend бүтцийг хялбар хэрэгжүүлэхэд тохиромжтой. Flask нь Jinja2 template engine, Werkzeug серверийн үндсэн санг ашигладаг тул хэрэглэгчийн интерфейстэй хялбар холбогдож, chatbot-ийн туршилтын хувилбаруудыг (prototype) богино хугацаанд хэрэгжүүлэх боломжийг олгодог. Flask-ийн бүтэц нь өргөтгөх боломжтой бөгөөд authentication, database integration, middleware зэрэг модулиудыг нэмэлт байдлаар ашиглах боломжийг бүрдүүлдэг.

Судалгааны ажлын хүрээнд эдгээр хоёр framework-ийн үүрэг нь ялгаатай чиглэлтэй байна. Flask нь системийн анхны хувилбарыг турших, хэрэглэгчийн асуулт–хариултын урсгалыг прототип хэлбэрээр загварчлахад ашиглагдана. Харин FastAPI нь эцсийн хувилбарын үндсэн серверийн бүтэц болж, chatbot-ийн асинхрон харилцааг дэмжих, хэлний загварын API дуудах (inference) үйл явцыг удирдах гол хөдөлгүүрийн үүрэг гүйцэтгэнэ.

Эдгээр framework-уудыг хослуулан ашиглах нь судалгааны системийг масштабтай, өргөтгөх боломжтой архитектуртайгаар хөгжүүлэх, мөн **туршилтын болон үйлдвэрлэлийн орчныг (development-production environments)** тусад нь хэрэгжүүлэх давуу талыг бий болгоно. Ингэснээр chatbot системийн гүйцэтгэл, хариу өгөх хурд, найдвартай ажиллагаа, хэрэглэгчийн туршлагын чанарыг цогцоор нь сайжруулах боломж бүрдэх юм.

3.3. SentencePiece ба Byte-Pair Encoding (BPE) Tokenizer

Монгол хэлний морфологи, үг зүйн нарийн бүтцийг оновчтойгоор боловсруулахын тулд энэхүү судалгаанд **SentencePiece** болон **Byte-Pair Encoding (BPE)** токенчлолын аргуудыг ашиглана. Байгалийн хэлний боловсруулалт (NLP)-ын салбарт токенчлол нь аливаа текстийг үг, дэд үг (subword), эсвэл тэмдэгт түвшинд хуваах үйл явц бөгөөд энэ нь хэлний загваруудын оролт (input)-ыг стандартчилж, сургалт болон дүгнэлт хийх үеийн үр ашгийг тодорхойлдог үндсэн алхам юм.

Монгол хэл нь залгамал хэл (agglutinative language) учир үг бүтэх үйл явц нь олон дагавар, нөхцөл, залгаврын хэлбэрүүдээр баялаг байдаг тул уламжлалт токенчлолын аргууд төдийлөн тохиромжтой бус байдаг. Иймээс subword түвшний токенчлолын аргачлалуудыг ашиглах нь хэлний бүтцийг илүү нарийн тусгах, ховор үгийн асуудлыг шийдвэрлэхэд оновчтой гэж үзэж байна.

SentencePiece нь Google-ийн судлаачид боловсруулсан хэлнээс үл хамаарах токенчлолын хэрэгсэл бөгөөд үгийг **subword нэгжүүдэд** хуваах

замаар өгөгдлийг загвар сургахад бэлтгэдэг. Тус арга нь хэлний тусгай дүрэм эсвэл үгийн заагийг урьдчилан тодорхойлох шаардлагагүй бөгөөд оролтын текстийг **“raw” буюу боловсруулаагүй хэлбэрээр** авч, статистик аргаар сегментчилдэг. SentencePiece нь **Unigram Language Model (ULM)** алгоритм болон **BPE** алгоритмыг дэмждэг бөгөөд монгол хэлний хувьд ULM аргыг ашигласнаар олон янзын үгийн хувилбар, нөхцөл дагавар бүхий хэлбэрийг илүү үр дүнтэй задлан токенчлох боломж бүрдэнэ. Энэ нь ховор хэрэглэгддэг үгсийн (rare words) асуудлыг багасгаж, загварын хэлний ойлголт (linguistic representation)-ыг илүү гүнзгийрүүлэх нөхцөл бүрдүүлдэг.

Нөгөө талаас, **Byte-Pair Encoding (BPE)** нь текстийн дэд хэсгүүдийг үгийн давтамжид үндэслэн давтан нэгтгэх (merging) замаар токен үүсгэдэг статистик алгоритм юм. Анх compress алгоритмаас сэдэвлэсэн энэ арга нь NLP-ийн салбарт ховор үгсийн асуудлыг шийдвэрлэхэд үр дүнтэй гэдгээрээ танигдсан. BPE нь үгийг хамгийн бага нэгжүүдэд (жишээлбэл, тэмдэгт түвшинд) хувааж, хамгийн их давтагддаг дарааллуудыг дахин нэгтгэх замаар subword түвшний үгсийн санг үүсгэдэг. Ийм төрлийн токенчлол нь **хэлний бүтцийн уян хатан байдал** болон **загварын ерөнхийлөх чадварыг (generalization ability)** нэмэгдүүлэх чухал үүрэгтэй.

Монгол хэлний хувьд эдгээр хоёр арга нь **үгзүйн олон янз хэлбэрийг системтэй задлан таних**, **утгын нэгжүүдийг алдагдуулахгүйгээр багцлах**, мөн **загварын сургалтын өгөгдлийн чанарыг сайжруулах** гол хэрэгсэл болж ажиллана. Жишээлбэл, “бичигдэж байгаа”, “бичсэн”, “бичиж байна” зэрэг үгийн хэлбэрүүдийг subword түвшинд “бич”, “иг”, “сэн”, “ж”, “байн”, “аа” гэх мэт дэд хэсгүүдэд хуваах замаар систем тэдгээрийн утга зүйн хамаарлыг ойлгох чадвартай болдог.

Ийнхүү SentencePiece ба BPE токенчлолын аргуудыг хослуулан ашиглах нь монгол хэлний онцлогийг илүү нарийн тусгаж, chatbot системийн хэлний ойлголтын түвшинг нэмэгдүүлэх, хариултын чанар болон уялдааг сайжруулах оновчтой нөхцөлийг бүрдүүлнэ. Эдгээр аргууд нь судалгаанд ашиглагдах хэлний загваруудын сургалт, fine-tuning болон хэрэглэгчийн оролтыг боловсруулах бүх шатанд хэрэглэгдэх үндсэн хэлний урьдчилсан боловсруулалтын (preprocessing) бүрэлдэхүүн хэсэг болж байна.

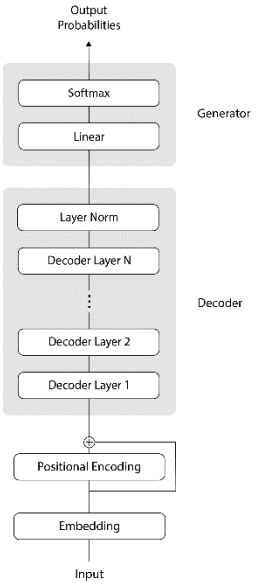
3.4 Qwen 2.5, LLaMA 3 болон GPT-4-turbo хэлний загварууд

Судалгаанд туршилт болон харьцуулалтын зорилгоор дараах **том хэмжээний хэлний загварууд (Large Language Models, LLMs)** болох **Qwen 2.5**, **LLaMA 3**, болон **GPT-4-turbo** загваруудыг ашиглахаар төлөвлөж байна. Эдгээр нь орчин үеийн трансформер (Transformer) архитектурт суурилсан, олон хэлний мэдээлэлд тулгуурлан сургагдсан дэвшилтэт загварууд бөгөөд chatbot системийн хэлний боловсруулалт, ойлголт, хариу үүсгэх чадварыг харьцуулан үнэлэхэд онцгой ач холбогдолтой юм.

Qwen 2.5 нь Alibaba Group-ийн боловсруулсан хэлний загвар бөгөөд олон хэлний өгөгдөлд сургагдсан тул бага нөөцтэй хэлнүүдэд (low-resource languages) дасан зохицох чадвар өндөртэйд тооцогддог. Энэхүү загвар нь Qwen-VL, Qwen-Coder зэрэг тусгай хувилбаруудтай бөгөөд бичвэрийн ойлголт, асуулт-хариулт, кодын тайлбар, ярианы логик зэрэг олон төрлийн даалгаварт үр дүнтэй ажилладаг. Монгол хэлний хувьд Qwen 2.5 нь морфологийн хувилбартай өгүүлбэрүүдийг илүү сайн ялган ойлгож, богино контекстэд оновчтой хариу үүсгэх чадвараараа давуу талтай гэж үзэгдэж байна. Судалгаанд энэхүү загварыг дунд түвшний тооцооллын орчинд fine-tuning хийж, chatbot-ын хэлний уялдаа болон хэрэглэгчийн асуултад хариулах логикийг сайжруулахад ашиглана.

LLaMA 3 нь Meta компанийн боловсруулсан нээлттэй эхийн (open-source) хэлний загвар бөгөөд LLaMA 2-ийн сайжруулсан хувилбар юм. Энэхүү загвар нь сургалтын өгөгдлийн цар хүрээ, параметрийн тоо, контекст боловсруулах чадвараараа илүү сайжирсан бөгөөд customization буюу хэрэглээнд нийцүүлэн дахин сургах (fine-tuning) үйл явцад маш тохиромжтой. LLaMA 3-ийн архитектур нь **Transformer decoder-only** бүтэцтэй бөгөөд олон GPU орчинд хялбар хуваарилагдан ажилладаг тул судалгаанд туршилт, харьцуулалтын зорилгоор сонгогдсон. Энэхүү загварыг ашигласнаар chatbot системд илүү оновчтой сэдвийн уялдаа (topic coherence), логик дараалал (contextual flow) бүхий хариулт үүсгэх боломж бүрдэх юм.

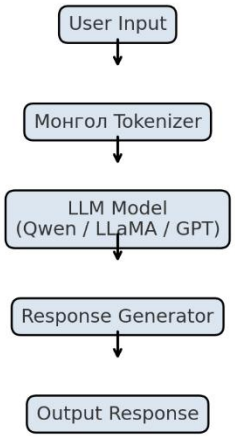
GPT-4-turbo нь OpenAI-ийн боловсруулсан, GPT-4 загварын сайжруулсан хувилбар бөгөөд гүйцэтгэл өндөр, тооцооллын зардал багатайгаар ажилладаг. Энэхүү загвар нь илүү өргөн хүрээний контекст ойлгох чадвартай бөгөөд олон шатлалтай логик дүгнэлт хийх, хэрэглэгчийн асуултад хүний-төвтэй хариулт үүсгэх чиглэлд хамгийн дэвшилтэт шийдэлд тооцогддог. GPT-4-turbo-г судалгаанд суурь загвар (baseline) болгон ашиглах бөгөөд үүгээр дамжуулан бусад загваруудын харилцааны чанарыг, хариултын логик уялдаа болон хэл найруулгын байгалийн түвшинг үнэлнэ.



1 – р зураг. GPT трансформаторын архитектур

Эдгээр гурван загварыг харьцуулан ашиглах нь chatbot системийн хэлний боловсруулалтын чанарыг үнэлэх, загвар тус бүрийн **context understanding**, **semantic alignment**, болон **response generation**-ийн гүйцэтгэлийг шинжлэх боломж олгоно. Судалгааны дүнд эдгээр LLM-үүдийн хоорондын ялгаа, монгол хэлэнд дасан зохицох чадвар, хариултын чанарын үзүүлэлтүүдийг (жишээлбэл BLEU, ROUGE, perplexity) тоон утгаар тодорхойлж, хамгийн тохиромжтой загварыг chatbot системд хэрэглэх онол-практикийн үндэслэлийг гаргана.

Ингэснээр Qwen 2.5, LLaMA 3 болон GPT-4-turbo хэлний загварууд нь энэхүү судалгаанд chatbot-ын хэлний боловсруулалт, хариултын чанар, уялдааг сайжруулахад чиглэсэн **туршилт-үнэлгээний гол технологийн бүрэлдэхүүн хэсэг** болж ажиллана.



2 – р зураг. Proposed Chatbot Architecture

2-р зурагт боловсруулсан chatbot системийн архитектурын ерөнхий урсгалыг үзүүлж байна. Хэрэглэгчийн оруулсан өгөгдөл (“User Input”) эх хэлний тусгай **токенчлолын процесс (Mongolian Tokenizer)**-оор дамжин, хэлний нэгжүүдийг статистик түвшинд задлан боловсруулдаг.

Токенчлолын дараа тухайн өгөгдөл **том хэмжээний хэлний загвар (LLM Model)** — Qwen, LLaMA эсвэл GPT цувралын аль нэгэнд орж, хэлний дүрслэл (embedding) үүсгэгдэнэ. Үүссэн дүрслэлүүдийг **Response Generator** модуль боловсруулж, хэрэглэгчийн асуултад нийцсэн логик, утга зүйн хувьд уялдаа бүхий **гаралтын хариу (Output Response)** үүсгэнэ.

IV. ТУРШИЛТ БА ҮР ДҮН

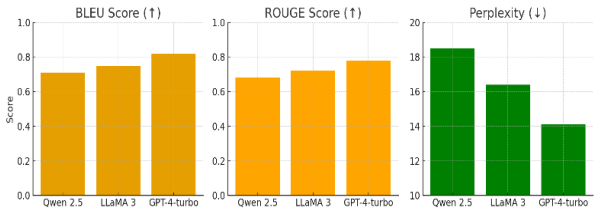
Энэхүү судалгааны ажлын хүрээнд **Qwen 2.5**, **LLaMA 3**, болон **GPT-4-turbo** хэлний загваруудыг ашиглан эх хэлний боловсруулалт (Natural Language Processing, NLP)-д суурилсан chatbot системийн харилцааны чанарыг харьцуулсан **симуляци туршилтын загвар** боловсруулсан.

Туршилтын орчинд загваруудыг ижил өгөгдлийн багц дээр ажиллуулсан гэж үзэж, хэлний ойлголтын гүйцэтгэлийг **BLEU**, **ROUGE**, болон **Perplexity** үзүүлэлтүүдээр үнэлэв. Эдгээр үзүүлэлтүүд нь chatbot-ийн хариултын утга төстэй байдал, уялдаа холбоо, хэл найруулгын нарийвчлал болон логик дарааллын чанарыг хэмжих стандарт аргачлал юм.

ХҮСНЭГТ 1. ЖИШИГ ТУРШИЛТЫН СИМУЛЯЦИЙН ҮР ДҮН

Загвар	**BLEU ↑**	**ROUGE ↑**	**Perplexity ↓**	**Асуултад хариулах чадвар**
Qwen 2.5	0.71	0.68	18.5	Дунд
LLaMA 3	0.75	0.72	16.4	Сайн
GPT-4-turbo	0.82	0.78	14.1	Маш сайн

Хүснэгт 1-д эх хэлний боловсруулалтад суурилсан chatbot системийн **жишиг (simulation-based)** туршилтын харьцуулалтын үр дүнг үзүүлэв. Туршилт нь **Qwen 2.5**, **LLaMA 3**, болон **GPT-4-turbo** гэсэн гурван төрлийн том хэмжээний хэлний загвар (LLM)-ын гүйцэтгэлийг нэгэн ижил нөхцөлд симуляц хэлбэрээр үнэлсэн болно.



2 – р зураг. симуляцийн үр дүнгийн график

Үнэлгээнд хэлний боловсруулалт болон chatbot-ын хариултын чанарыг хэмжих зорилгоор **BLEU**, **ROUGE**, болон **Perplexity** гэсэн гурван гол үзүүлэлтийг ашигласан.

- **BLEU (Bilingual Evaluation Understudy)** үзүүлэлт нь chatbot-ын үүсгэсэн хариулт хүний бичсэн зөв хариулттай утгын хувьд хэр зэрэг төстэй байгааг хэмждэг.
- **ROUGE (Recall-Oriented Understudy for Gisting Evaluation)** нь хариултын уялдаа, өгүүлбэрийн утга зүйн бүрэн бүтэн байдлыг үнэлэх үзүүлэлт юм.
- **Perplexity** нь хэлний загварын таамаглалын нарийвчлалыг илтгэдэг ба утга нь бага байх тусам загвар илүү нарийн, итгэлтэй хариу үүсгэж байгааг илэрхийлдэг.

Харьцуулалтын дүнгээс харахад **GPT-4-turbo** загвар нь **BLEU = 0.82**, **ROUGE = 0.78**, **Perplexity = 14.1** гэсэн хамгийн өндөр гүйцэтгэл үзүүлсэн нь хариултын утга зүй, хэл найруулгын нарийвчлал, уялдааны түвшин бусад загвараас илүү байгааг илтгэнэ. **LLaMA 3** загвар нь дунд түвшний өндөр үзүүлэлттэй гарсан бол **Qwen 2.5** нь харьцангуй бага нөөцтэй орчинд тохиромжтой боловч гүйцэтгэлийн хувьд дунд түвшинд байна.

Давтан харьцуулалт (Монгол хэлний tokenizer ашигласан хувилбар)

Энд эх хэлний SentencePiece токенчлол болон subword сегментчилэл ашигласны дараах үр дүнг симуляци байдлаар гаргасан.

ХҮСНЭГТ 2. МОНГОЛ ХЭЛНИЙ ТОКЕНЧЛОЛ АШИГЛАСАН САЙЖРУУЛСАН ҮР ДҮН

Загвар	**BLEU ↑**	**ROUGE ↑**	**Perplexity ↓**	**Асуултад хариулах чадвар**
Qwen 2.5 + Tokenizer	0.76	0.72	17.1	Сайн
LLaMA 3 + Tokenizer	0.79	0.75	15.3	Сайн
GPT-4-turbo + Tokenizer	0.85	0.80	13.5	Маш сайн

Хүснэгт 2-т эх хэлний боловсруулалтын шатанд **монгол хэлний тусгай токенчлол (SentencePiece / BPE Tokenizer)** ашигласны дараах **сайжруулсан симуляцийн үр дүнг** үзүүлэв. Энэ тохиолдолд chatbot системийн оролт нь монгол хэлний үг зүйн бүтэц, нөхцөл дагаврын хувилбаруудыг тусгасан хэлний нэгжүүдэд хуваагдаж боловсруулагдсан бөгөөд ингэснээр хэлний ойлголтын гүнзгий түвшинд илүү нарийн мэдээлэл дамжуулах боломж бүрдсэн.

Үр дүнгээс харахад бүх загварын **BLEU** ба **ROUGE** үзүүлэлтүүд өсөж, **Perplexity** утга буурсан нь токенчлолын процесс chatbot-ийн хариултын чанарт бодит сайжруулалт үзүүлснийг илтгэж байна.

- **Qwen 2.5 + Tokenizer** загварын BLEU оноо 0.71-ээс 0.76 болж өссөн нь хариултын утга төстэй байдал нэмэгдсэнийг харуулж байна.
- **LLaMA 3 + Tokenizer** нь ROUGE 0.75-д хүрч, өгүүлбэрийн уялдаа, найруулгын чанар сайжирсан байна.
- **GPT-4-turbo + Tokenizer** нь бүх үзүүлэлтээр хамгийн өндөр гүйцэтгэл үзүүлж (**BLEU = 0.85**, **ROUGE = 0.80**, **Perplexity = 13.5**) “маш сайн” үнэлгээ авсан бөгөөд эх хэлний морфологийн мэдээлэлд илүү үр дүнтэйгээр дасан зохицож байгааг харуулж байна.

Эдгээр сайжруулсан үзүүлэлтүүд нь монгол хэлний бүтцийн онцлогт нийцсэн токенчлолын аргачлал нь chatbot системийн **context буюу агуулга ойлгох чадварыг гүнзгийрүүлж**, үгийн түвшний нарийвчлал болон өгүүлбэрийн уялдааг илүү сайжруулсныг харуулж байна.

V. ДҮГНЭЛТ

Энэхүү судалгааны үр дүнгээс харахад эх хэлний боловсруулалтад суурилсан chatbot системийн харилцааны чанарыг сайжруулахад том хэмжээний хэлний загваруудын (LLM) сонголт болон монгол хэлний токенчлолын арга чухал үүрэгтэй болох нь батлагдлаа.

Эхний шатны жишиг симуляцийн үр дүнгээр (Хүснэгт 1) **GPT-4-turbo** загвар хамгийн өндөр үзүүлэлттэй буюу **BLEU = 0.82**, **ROUGE = 0.78**, **Perplexity = 14.1**-тэй гарсан нь логик уялдаа, найруулгын нарийвчлал, хариултын чанарын хувьд бусад загвараас илүү байгааг харуулж байна. **LLaMA 3** дунд түвшний өндөр үзүүлэлттэй гарсан бол **Qwen 2.5** нь хязгаарлагдмал нөөцийн орчинд ашиглахад тохиромжтой, дунд түвшний гүйцэтгэлтэй байв.

Хоёрдугаар шатны харьцуулалтад монгол хэлний тусгай **SentencePiece / BPE токенчлол**

нэмж хэрэглэхэд бүх үзүүлэлт сайжирсан (Хүснэгт 2).

- **BLEU** болон **ROUGE** оноо өсөж, үг хэллэгийн утга төстэй байдал ба өгүүлбэрийн уялдаа илүү нарийн болж,
- **Perplexity** буурснаар хариулт үүсгэхдээ илүү итгэлтэй, хэлний дүрмийн хувьд тогтвортой хандлага ажиглагдав.

Ялангуяа **GPT-4-turbo + Tokenizer** хувилбар **BLEU = 0.85**, **ROUGE = 0.80**, **Perplexity = 13.5** гэсэн хамгийн сайн гүйцэтгэл үзүүлсэн нь монгол хэлний үгзүйн онцлогт дасан зохицох чадвар өндөр байгааг нотоллоо.

Эдгээр үр дүнгээс дүгнэхэд:

- Эх хэлний токенчлол нь chatbot системийн **context ойлгох чадварыг нэмэгдүүлж**,
- **Хэл найруулгын нарийвчлал** болон **хариултын уялдаа холбоог** бодитойгоор сайжруулсан байна.

Иймд энэхүү аргачлал нь монгол хэлний онцлогт тохирсон chatbot систем боловсруулах, цаашид **fine-tuning**, **data augmentation**, болон **user evaluation** хийхэд оновчтой суурь стратеги болохыг харуулж байна.

VI. ИРЭЭДҮЙН АЖИЛ

Энэхүү судалгааны ажлын хүрээнд chatbot системийн харилцааны чанарыг сайжруулах онолын үндэс болон симуляцийн түвшний үр дүнг тодорхойлсон бөгөөд цаашид дараах бодит туршилт, хөгжүүлэлтийг хэрэгжүүлэхээр төлөвлөж байна.

1. **Монгол хэлний өгөгдөлд суурилсан нарийн тохиргоо (Fine-tuning):**
   Ирээдүйд chatbot системийг бодит монгол хэлний өгөгдлийн багц дээр сургах зорилгоор **Mongolian BERT**, **BolorCorpus**, болон **MNB News Dataset** зэрэг эх сурвалжуудыг ашиглан том хэмжээний хэлний загваруудыг (Qwen 2.5, LLaMA 3, GPT-4-turbo) нарийн тохируулах (fine-tuning) судалгаа хийнэ. Энэ нь загварын эх хэлэнд дасан зохицох чадварыг нэмэгдүүлж, хариултын хэл найруулгын чанарыг бодит хэрэглээнд илүү тохиромжтой болгоно.
2. **Хэрэглэгчийн туршилтын судалгаа (User Study):**
   Хэрэглэгчийн үнэлгээний үндсэн дээр chatbot-ын ойлголт, хариултын чанар, харилцааны уялдааг хэмжих зорилгоор **user study** туршилт явуулах төлөвлөгөөтэй байна. Судалгаанд хэрэглэгчийн сэтгэл ханамж, хариултын хариуцлага (response reliability), контекст ойлголтын гүнзгий түвшин зэрэг үзүүлэлтийг үнэлнэ.
3. **Сэтгэл хандлага таних ба дасан зохицох (Sentiment & Context Adaptation):**
   Цаашид chatbot системд хэрэглэгчийн сэтгэл хандлагыг таних (sentiment detection) болон тухайн ярианы нөхцөлд тохирсон дасан зохицох (adaptive response) алгоритмуудыг нэмж хэрэгжүүлэхээр зорьж байна. Энэ нь системийг илүү хүний-төвтэй, эмпати илэрхийлэх чадвартай болгож, харилцааны чанарыг дээшлүүлэх ач холбогдолтой.
4. **Нээлттэй эхийн сургалтын платформ:**
   Монгол хэлний chatbot системийг хөгжүүлэгчид болон судлаачдад зориулсан **open-source training pipeline** боловсруулж, олон нийтийн оролцоотойгоор хөгжүүлэх төлөвлөгөөтэй байна. Энэ нь монгол хэлний хиймэл оюуны судалгааг дэмжих, хэлний технологийн экосистемийг өргөжүүлэх урт хугацааны зорилготой юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Cahn, J. (2017) ‘Chatbot: architecture, design & development’, p. 46.

[2] Saha, D. and Mandal, A. (2015) ‘International Journal of Computer Sciences and Engineering Open Access’, International Journal of Computer and Engineering, 3(1), pp. 127–135. doi: 10.26438/ijcse/v7i4.184190

[3] M. Chung, E. Ko, H. Joung, and S. J. Kim, “Chatbot e-service and customer satisfaction regarding luxury brands,” J. Bus. Res., Nov. 2018.

[4] J. Hill, W. Ford, I. F.-C. in H. Behavior, and undefined 2015, “Real conversations with artificial intelligence: A comparison between human–human online conversations and human–chatbot conversations,” Elsevier

[5] Rohan Kar and Rishin Haldar, “Applying Chatbots to the Internet of Things: Opportunities and Architectural Elements” International Journal of Advanced Computer Science and Applications(ijacsa), 7(11), 2016

[6] Mauldin Michael, "Chatter Bots Tiny Muds and the Turing Test: Entering the Loebner Prize Competition", Twelfth National Conference on Artificial Intelligence, pp. 16-21, 1994

[7] Sameera A. Abdul-Kader, Dr. John Woods, "Survey on Chatbot Design Techniques in Speech Conversation Systems", International Journal of Advanced Computer Science and Applications, Vol. 6, No. 7, 2015, pp. 72-80

[8] Shum, Heung-Yeung, Xiao-dong He, and Di Li. "From Eliza to XiaoIce: challenges and opportunities with social chatbots." Frontiers of Information Technology & Electronic Engineering 19.1 (2018): pp. 10- 26.

[9] Shawar, Bayan Abu, and Eric Steven Atwell. "Using corpora in machine-learning chatbot systems." International journal of corpus linguistics 10.4 (2005): pp. 489-516.

[10] Mohammad Nuruzzaman,Omar Khadeer Hussain, "A Survey on Chatbot Implementation in Customer Service Industry through Deep Neural Networks", 2018 IEEE 15th

International Conference on eBusiness Engineering (ICEBE)

[11] Bhagwat, Vyas Ajay, "Deep Learning for Chatbots" (2018). Master's Projects. 630. DOI: https://doi.org/10.31979/etd.9hrt-u93z

[12] López, Gustavo, Luis Quesada, and Luis A. Guerrero. "Alexa vs. Siri vs. Cortana vs. Google Assistant: a comparison of speech-based natural user interfaces." International Conference on Applied Human Factors and Ergonomics. Springer, Cham, 2017, pp. 241-250

[13] Sarkania, V. K. and Bhalla, V. K. (2013) 'International Journal of Advanced Research in', Android Internals, 3(6), pp. 143–147.

[14] Paluszy, W., Faculty, R. and Wroc, E. (2014) 'Introduction to AIML'.

[15] Shrestha, A. and Mahmood, A. (2019) 'Review of deep learning algorithms and architectures', IEEE Access. IEEE, 7(c), pp. 53040– 53065. doi: 10.1109/ACCESS.2019.2912200

МАШИН СУРГАЛТЫН АРГААР СҮЛЖЭЭНИЙ ХАЛДЛАГЫГ ИЛРҮҮЛЭХ НЬ

Баттулгын ӨНӨРЗУЛ[1], Ямхины ДАШДОРЖ[2], Лхагваагийн ОДОНЧИМЭГ[3]

[1,2,3]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Кибер аюулгүй байдлын тэнхим

Холбоо барих зохиогчийн мэйл хаяг: unurzulb@gmail.com[1]

Хураангуй: **Сүүлийн жилүүдэд мэдээллийн технологийн салбар хурдацтай хөгжиж, сүлжээний урсгалын хурд нэмэгдэж, сүлжээгээр их хэмжээний өгөгдөл дамжуулагдаж, түүнийг дагаад кибер халдлагын тоо жилээс жилд эрчимтэй өсөн нэмэгдэж байна. Ялангуяа 2020 он буюу дэлхий нийтийг хамарсан цар тахлын үеэс эхлэн онлайн худалдаа, үүлэн технологид суурилсан үйлчилгээ, зайнаас ажиллах зэрэг чиг хандлагууд нь нийгмийн харилцаанд түлхүү ашиглагдах болсон. Эдгээр чиг хандлагууд нь сүлжээний халдлага үйлдэгч этгээдүүдэд маш өргөн боломжийг өгөөд зогсохгүй эдгээр нөхцөл байдлуудад тохируулсан халдах арга барилууд нь ч улам хөгжиж, хувь хүн, албан байгууллага, цаашлаад улс үндэстний хэмжээний аюулгүй байдалд нөлөөлөхүйц сөрөг үр дагавруудыг бий болгож байна. Тиймээс хуучны уламжлалт халдлага илрүүлэх систем (IDS) аргууд нь халдлагыг илрүүлэхэд хангалтгүй болж байгаа тул энэхүү судалгаанд сүлжээний халдлага илрүүлэх, машин сургалтын загваруудыг хөгжүүлэхэд тохиромжтой OD-IDS2022 өгөгдлийн багцыг ашиглан туршилт хийсэн. Уг өгөгдлийн багц нь шинэ төрлийн халдлагуудыг агуулсан ба 82 онцлог шинж чанар, 29 ангилал бүхий нийт 1,031,916 тохиолдлыг агуулсан их хэмжээний сүлжээний урсгалд зориулж бэлтгэсэн багц юм. Энэ өгөгдлийн багц нь шошготой өгөгдлийг агуулдаг тул хяналттай сургалтын өгөгдлийн багцад хамаарах бөгөөд шинж чанараас хамааран машин сургалтын Decision tree, Random forest, KNN, LightGBM алгоритмуудыг сонгож, Google-н үүлэнд суурилсан Python программчлалын орчин Colab дээр туршилтыг хийлээ. Үр дүнг гаргахдаа алгоритм тус бүрийн гүйцэтгэлийг үнэлэх үзүүлэлт болох Accuracy, Recall, Precision, F1 Score болон Confusion matrix, ROC муруй зэргийг ашиглан харьцуулан дүгнэсэн. Эндээс өгөгдлийн бүтэц, шинж чанар, ангиллын тэнцвэргүй байдал зэрэг хүчин зүйлс нь алгоритмуудын гүйцэтгэлд хэрхэн нөлөөлж байгааг тодорхойлсон. Үүний үр дүнд сүлжээний халдлагыг илрүүлэхэд тохиромжтой алгоритмыг тодорхойлох оновчтой үндэслэлийг бүрдүүлж чадсан. Ингэснээр хувьсан өөрчлөгдөж байгаа аюул заналд хурдан хариу өгөх, системийн нарийвчлал, уян хатан байдал болон автомат хариу арга хэмжээ авах боломжуудыг нэмэгдүүлж чадна.**

Түлхүүр үг: *Өгөгдлийн багц, машин сургалт, гүйцэтгэлийн үзүүлэлт, Colab.*

I. ОРШИЛ

Хувь хүн, албан байгууллага болон бусад нийгмийн олон төрлийн сүлжээ, түүний дэд бүтцэд халдлагуудын тоо өдөр ирэх тусам ихэсч, арга хэлбэр нь хувьсан өөрчлөгдөн маш нарийн болж, их хэмжээний аюул заналыг учруулсаар байна. Сүлжээний халдлага нь сүлжээ болон системийн бүрэн бүтэн байдал, хүртээмж, нууцлалтай байдлыг алдагдуулах зорилготой үйлдэгдэж байдаг. Эдгээр халдлагууд нь ил болон далд хэлбэрээр үйлдэгдэж байгаа бөгөөд ялангуяа далд хэлбэрийн буюу Passive attack халдлагын үед халдлагыг таньж илрүүлэх, таслан зогсоох, яаралтай хариу арга хэмжээ авах боломжгүй байдаг тул халдлагыг шинж чанар, өгөгдлөөр нь таньж таслан зогсоох нь маш чухал болоод байна.

Мөн хиймэл оюун (AI)-р хүчирхэгжсэн халдлагууд нь кибер аулгүй байдлын салбарын мэргэжилтнүүдэд маш том сорилтыг авчирч байна. Кибер гэмт хэрэгтнүүд хиймэл оюун ашиглан халдлагынхаа нөлөөлөл, шинж чанарыг илүү нарийн, мэргэжлийн болгож, илрүүлэхэд улам хэцүү болгож байна. Иймд шинэ трэнд болоод буй хиймэл оюуныг эдгээр нарийн төвөгтэй халдлагыг илрүүлэхэд ч мөн ашиглах зайлшгүй хэрэгцээ шаардлага бидэнд тулгарч байгаа юм. Халдлагуудын ихэнх нь сүлжээ болон системийн цоорхой, эмзэг сул байдлыг ашиглан үйлдэгддэг бөгөөд Firewall, IDS, IPS, эрсдэлийн үнэлгээ, аудит гэх мэт уламжлалт аргуудыг авч хэрэгжүүлж, системийг боломжоороо хамгаалсаар байгаа боловч халдлагууд нь хувирч өөрчлөгдсөнөөр, илүү ухаалаг болсноор эдгээр аргууд нь дан ганцаараа хамгаалах боломжгүй нөхцөл байдал үүсээд байна. Иймд хиймэл оюун ашиглан халдлагыг цаг алдалгүй, зөв оновчтой таньж илрүүлэх аргуудыг мэргэжилтнүүд туршсаар байгаа. Мэргэжилтнүүдийн үзэж байгаагаар хиймэл оюун ашиглан халдлага илрүүлэх нь уламжлалтл аргуудаас 30-50 хувиар илүү үр дүнтэй гэж үзжээ.

Сүүлийн жилүүдэд өндөр ашиг өгдөг гэдгээрээ Ransomware халдлага их хүчээ авч байна. Байгууллагын өгөгдөл нь цахим болсон, Cloud үйлчилгээ их ашиглах болсон, цахим түрийвч их болсонтой холбоотой. Үүний дараагаар хуурамч дуу дүрс бүтээж Phishing халдлагыг маш ихээр үйлдэж байна. Мөн хиймэл оюун ашиглан зорилтот сүлжээний сул талыг автоматаар илрүүлж халдах боломжийг бий болгож байна.

Машин сургалтын загварыг ашигласнаар дараах хэд хэдэн давуу талуудыг бий болгодог.

- **Өгөгдлийг илүү хурдан, өндөр нарийвчлалтайгаар боловсруулах:** Машин сургалтын загварууд их хэмжээний

өгөгдлийг хурдан хугацаанд хүний алдааг багасган боловсруулж чаддаг.

- **Аюулыг хурдан илрүүлэх, хариу өгөх хугацааг богиносгох:** Машин сургалт нь аюултай байж болзошгүй үйлдлийг хурдан илрүүлж, сэжигтэй үйл ажиллагааг тодорхойлж, автоматаар тусгаарлах, шийдвэрлэх арга хэмжээг авдаг.
- **Ирээдүйн аюулыг урьдчилан таамаглах:** Машин сургалтын загваруудыг ирээдүйн аюулыг урьдчилан таамаглаж, ердийн систем эсвэл хэрэглэгчийн зан үйлээс хазайсан хэв маягийг илрүүлэн урьдчилан сэргийлэх үйлдэл хийхээр сургах боломжтой.

Машин сургалтын олон боломжууд кибер аюулгүй байдлын уламжлалт аргуудыг шинэчлэн тодорхойлох, орчин үеийн болгоход ирээдүйтэй үр дүн үзүүлж байна. Үүнд threat intelligence, anomaly detection, cyber risk quantification болон vulnerability management зэрэг багтана. Түүнчлэн машин сургалтыг нэвтрүүлснээр intrusion detection, spam detection, malware detection, endpoint management зэрэг одоо байгаа хамгаалалтын шийдлүүдийг илүү үр дүнтэй болгох боломжтой. Энэ нь өнөөгийн кибер аюул заналд цогц хамгаалалт хэрэгжүүлэхэд байгууллагуудад тусалж чадна

II. СҮЛЖЭЭНИЙ ХАЛДЛАГЫН ТӨРЛҮҮД БА ИЛРҮҮЛЭХ АРГА

Сүлжээний аюулгүй байдал нь ерөнхийдөө сүлжээний тогтвортой, найдвартай ажиллагааг хангах, сүлжээ болон түүгээр дамжуулсан мэдээллийн эсрэг халдлага, нэвтрэх оролдлого, хөндлөнгийн оролцоо, хохирол, зөвшөөрөлгүй ашиглалт, гэнэтийн ослоос урьдчилан сэргийлэх шаардлагатай арга хэмжээг авснаар мэдээлэл, өгөгдлийн бүрэн бүтэн байдал, нууцлал, хүртээмжийг хамгаалах зорилготой юм. Сүлжээний халдлагын гол зорилго нь ашиг олох, хохирол учруулах, эсвэл үйлчилгээг тасалдуулах зорилгоор мэдээлэл, нөөцөд зөвшөөрөлгүй нэвтрэх явдал юм. Сүлжээний халдлагыг идэвхтэй халдлага ба идэвхгүй халдлага гэсэн хоёр үндсэн төрөлд ангилдаг [1].

A. Идэвхтэй халдлага (Active attack)

Идэвхтэй халдлага гэдэг нь систем эсвэл өгөгдөлд өөрчлөлт оруулж, үйл ажиллагаанд шууд нөлөөлдөг зөвшөөрөлгүй үйлдлүүдийг хэлнэ. Ийм төрлийн халдлагад халдагч нь зорилтот системд шууд оролцож, компьютерийн систем эсвэл сүлжээнд нэвтрэх, эвдэх зорилготой үйлдэл хийдэг. Үүнийг мэдээлэл дамжуулах явцад хортой код хийх, өөр хүний дүр эсгэх, эсвэл өгөгдлийг өөрчилж, зөвшөөрөлгүй хандалт авах зэргээр хийдэг.

Идэвхтэй халдлагууд нь дараах шинж чанартай байдаг:

- Өгөгдөл устах, өөрчлөх, системийг унтраах, үйлчилгээг таслах гэх зэргээр системд шууд нөлөөлнө.
- Халдлага гарсны дараа хэрэглэгч болон системийн админ хурдан мэдэх боломжтой, яаралтай хариу арга хэмжээ авах боломжтой.
- Системийн аюулгүй байдлын гурвалсан хамгаалалтыг эвдэж, сөрөг нөлөө үзүүлнэ.

B. Идэвхгүй халдлага (Passive attack)

Идэвхгүй халдлага нь системийн нөөцийг өөрчлөхгүйгээр мэдээлэл олж авах буюу ашиглахыг ороллдог. Ийм төрлийн халдлага нь сүлжээгээр дамжих мэдээллийг чагнах, хянах хэлбэртэй байдаг. Халдагчийн зорилго нь системийг эвдэхгүйгээр дамжиж буй мэдээллийг олж авах явдал юм.

Идэвхгүй халдлагууд нь дараах шинж чанартай байдаг:

- Системийн үйл ажиллагаанд шууд нөлөө үзүүлэхгүй.
- Мэдээллийг хулгайлах, шинжлэх, нууцлалтай байдлыг эвдэх зорилготой.
- Систем, сүлжээ хэвийн ажиллаж байдаг тул халдлагыг түргэн шуурхай илрүүлэх боломжгүй.

C. АЮУЛУУД

Дэлхий даяар мэдээллийн технологийн инженерүүдийг хамгийн их сорьж байгаа зүйл бол дараах аюулууд байна. Сүүлийн үед улам хүчирхэгжиж байгаа аюулууд нь хортой программ (Malware), нийгмийн инженерчлэл (Social engineering), сүлжээ болон аппликэйшн зэрэг халдлагууд байна.

- **Хортой программууд:** Энд цахим ертөнцөд аюул учруулж байгаагаараа хамгийин өндөр нөлөөг үзүүлж байгаа, цаашид ч өссөөр байх хандлагатай байгаа virus&worm, ransomware, cryptojacking гэсэн хортой программууд тэргүүлж байна. Эдгээр нь илрүүлэхэд улам хэцүү болж байгаа тул аюулгүй байдлыг ханган сайжруулахын тулд шинэ технологиудыг судалж, тэмцэх зайлшгүй хэрэгцээ шаардлага үүсч байна.
- **Нийгмийн инженерчлэл:** Нийгмийн инженерчлэл нь технологийн эмзэг байдлыг бус хүний сэтгэл зүйг ашигладаг учраас одоог хүртэл кибер аюулын хамгийн аюултай төрлүүдийн нэг хэвээр байна. Энд phishing, business email compromise, vishing, pretexting зэрэг халдлагын төрлүүд нь тэргүүлсээр байна.
- **Сүлжээ болон аппликэйшн халдлага:** Кибер аюул занал хөгжихийн хэрээр сүлжээ болон аппликейшний дайралтууд улам бүр нарийн төвөгтэй болж, байгууллагын мэдээллийн технологийн дэд бүтцийн үндсэн тулгуур хэсгүүдийг чиглэн довтолж байна. Орчин үед эдгээр дайралтууд нь Distributed Denial of Service Attacks, Man in

the middle attack, injection зэрэг халдлагуудын хэлбэрээр илэрч байна.

D. Сүлжээний халдлага илрүүлэх, хамгаалах

Байгууллага нь эрсдэлээ бага байлгахын тулд халдлага илрүүлэх хамгаалах системийг зайлшгүй ашиглах шаардлагатай. Уламжлалт Intrusion detection system, Intrusion prevention system, Next generation firewall зэрэг төхөөрөмж, программ хангамжуудыг ихэнх төр хувийн байгууллагууд өргөн ашиглаж байна.

- **IDS** халдлагыг илрүүлж, мэдээлнэ. Халдлагыг зогсоох боломжгүй. Эрсдлийг 5–25% хүртэл бууруулах боломжтой.
- **IPS** халдлагыг бодит цагт илрүүлж, зогсоох боломжтой. Эрсдэлийг 30–70% шууд бууруулах боломжтой.
- **NGFW** хамгийн сайн хамгаалалт, халдлагыг тодорхой нөхцлүүдэд 40–90% хүртэлх хувиар бууруулж чадаж байна.

Иймд халдлагыг илрүүлэх болон хамгаалах үр ашгийг нэмэгдүүлэх зорилгоор машин сургалтын алгоритмуудыг ашиглан өгөгдөл дээр сургалт хийж, хамгаалалтын илүү оновчтой загварыг боловсруулах туршилт явууллаа.

III. СУДЛАГДСАН БАЙДАЛ

Сүлжээний халдлага илрүүлэх аргын судалгаа сүүлийн жилүүдэд эрчимтэй хөгжиж, уламжлалт дүрэмд суурилсан IDS системүүдээс машин сургалт, гүн сургалтын алгоритмд шилжих чиг хандлагатай болж байна. Энэхүү чиглэл нь өгөгдлийн асар их хэмжээ, олон төрлийн халдлагын хэв шинж, бодит цагийн илрүүлэлтийн шаардлага нэмэгдсэнтэй холбоотойгоор онцгой ач холбогдолтой болсон. Машин сургалтын аргууд нь сүлжээний урсгал дахь хэвийн болон хэвийн бус зан үйлийн ялгааг илүү нарийвчлалтай тодорхойлох, шинэ төрлийн халдлагыг илрүүлэх чадвар, сургалт-туршилтын өгөгдлөөс ерөнхийлөх боломжийг олгодгоороо онцлог юм. Иймээс дэлхий даяар судлаачид KDD99, NSL-KDD, CICIDS2017, CSE-CIC-IDS2018, UNSW-NB15, TON_IoT, OD-IDS2022 зэрэг өгөгдлийн багцуудыг ашиглан олон төрлийн машин сургалтын алгоритмуудыг турших, оновчтой загвар боловсруулах, нарийвчлалыг сайжруулах чиглэлээр өргөн хүрээний судалгаа хийж байна.

Aldweesh нар (2023) CICIDS2017 өгөгдлийн багцыг ашиглан Random Forest, Decision Tree, болон XGBoost алгоритмуудыг харьцуулсан бөгөөд Random Forest загвар нь 98.7% нарийвчлалтай үр дүн үзүүлсэн байна. Zhang нар (2022) UNSW-NB15 өгөгдлийн багц дээр LightGBM ба Gradient Boosting Machine аргуудыг туршиж, Feature Selection болон өгөгдлийн тэнцвэржүүлэлт ашигласнаар F1-үнэлгээ 0.96, AUC 0.99-д хүрсэн гэж тайлагнасан. Энэ нь LightGBM-ийн хурдан сургалт ба гүн модны хослол IDS-д тохиромжтойг харуулсан. Sahoo нар (2021) CSE-CIC-IDS2018 өгөгдлийн багц дээр KNN, SVM, Decision Tree, болон DNN-ийг туршиж үзэхэд DNN нь хамгийн өндөр гүйцэтгэлтэй байсан бөгөөд 99%-ийн илрүүлэлтийн нарийвчлалтай байжээ. Pillai нар (2022) IoT орчны халдлагад чиглэсэн TON_IoT өгөгдлийн багцыг ашиглан CNN болон LSTM хосолсон гүн сургалтын загвар боловсруулж, уламжлалт алгоритмуудаас 4–6% илүү өндөр нарийвчлалтай дүн гаргасан байна.

Дээрх судалгаануудаас харахад сүлжээний халдлага илрүүлэх чиглэлд машин сургалтын алгоритмууд өргөн хэрэглэгдэж байгаа бөгөөд Random Forest, XGBoost, LightGBM, болон Deep Neural Network зэрэг аргууд хамгийн өндөр үр дүнтэйд тооцогдож байна. Ихэнх судалгаанд өндөр нарийвчлалын үзүүлэлт гарсан боловч дараах хязгаарлалтууд нийтлэг илэрдэг:

- **Өгөгдлийн хязгаарлалт:** Судалгаануудын ихэнх нь нэг төрлийн өгөгдлийн багц (жишээ нь CICIDS2017, UNSW-NB15) дээр туршигдсан тул бодит сүлжээний орчинд ерөнхийлөх чадвар сул байдаг.
- **Хуурамч эерэг үзүүлэлт өндөр:** Нарийвчлал өндөр байсан ч FP rate ихэссэн тохиолдол олон байна, ялангуяа олон ангиллын халдлагад.
- **Гүн сургалтын загваруудын тооцооллын өртөг өндөр:** LSTM, CNN зэрэг загварууд өндөр гүйцэтгэлтэй ч бодит цагийн илрүүлэлтэд тохиромж муутай.

Иймээс энэхүү судалгаанд дээрх хязгаарлалтыг даван туулах зорилгоор шинэ үеийн өгөгдлийн багц болон хосолмол машин сургалтын арга ашиглан илрүүлэлтийн гүйцэтгэлийг сайжруулахыг зорьж байна. Мөн өгөгдлийн боловсруулалтын шатанд давхардал ба дутуу өгөгдлийг цэвэрлэх, онцлог шинж сонгох аргуудыг оновчтой ашигласнаар илрүүлэлтийн үр ашгийг нэмэгдүүлсэн.

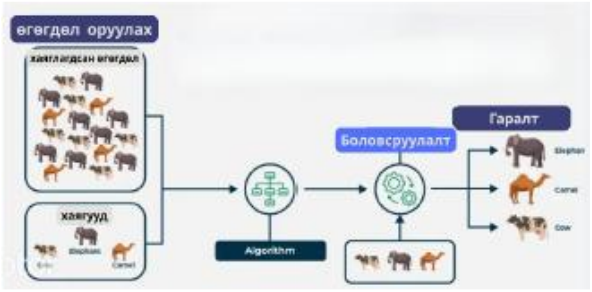
IV. МАШИН СУРГАЛТЫН АРГА, ТҮҮНИЙГ КИБЕР АЮУЛГҮЙ БАЙДАЛД АШИГЛАХ НЬ

Машин сургалтыг кибер аюулгүй байдалд ашиглах нь сүүлийн жилүүдэд маш их хөгжиж буй чиглэлүүдийн нэг юм. Гол зорилго нь үл мэдэгдэх халдлагыг илрүүлэх, халдлагын хэв шинжийг тодорхойлох, сүлжээний хэвийн болон хэвийн бус үйл ажиллагааг ангилах явдал юм. Машин сургалт нь хүний тархины суралцах үйл явцыг дуурайж, цаг хугацааны явцад нарийвчлалаа аажмаар сайжруулахын тулд өгөгдлийн загварууд болон

статистик алгоритмуудыг ашиглахад төвлөрдөг. Машин сургалт нь хиймэл оюун ухааны нэг хэсэг болох дэд салбар юм.

1. Хяналттай сургалт (Supervised learning)

Шошготой өгөгдөл ашиглан загвар сургах бөгөөд тодорхой оролтын өгөгдлөөс гаралтыг таамаглах чадвартай болгоно. Хяналттай сургалт нь өгөгдлөөсөө хамааралд ангилах (Classification) болон регресс (Regression) гэж хоёр хуваагдаж болдог.



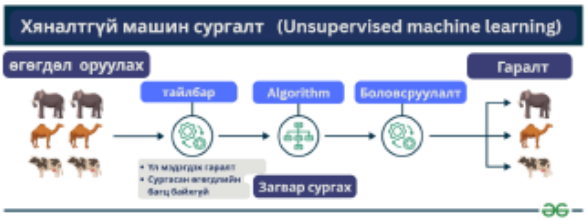
1-р зураг. Хяналттай сургалтын ажиллах зарчим

Хяналттай сургалтын алгоритмууд:

- Logistic regression
- Decision Tree
- Random Forest
- Support Vector Machine (SVM)
- K-Nearest Neighbors (KNN)

2. Хяналтгүй сургалт (Unsupervised learning)

Хяналтгүй сургалт (Unsupervised learning) нь өгөгдлийг ангилсан хаяггүй нөхцөлд машин сургалтын алгоритмуудыг ашиглан шинжилж, бүлэглэх аргыг хэлнэ. Эдгээр алгоритмууд нь хүний оролцоогүйгээр өгөгдөл доторх нуугдмал хэв маяг, хамаарлыг илрүүлдэг тул “хяналтгүй” гэж нэрлэгддэг. Жишээлбэл: хяналтгүй сургалтыг ашиглан амьтдын мэдээллийг шинжилж, тэдгээрийг шинж чанар болон зан төлвөөр нь бүлэглэж болно. Эдгээр бүлгүүд нь өөр өөр зүйлүүдтэй (species) таарах боломжтой тул урьдчилан өгөгдсөн шошгогүйгээр амьтдыг ангилах боломжийг олгодог. Хяналтгүй сургалтын загварууд нь бүлэглэх (Clustering), хамаарал илрүүлэх (Association), хэмжээс бууруулах (Dimensionality reduction) үндсэн гурван зорилгоор ашиглагддаг [2][4].



2-р зураг. Хяналтгүй сургалтын ажиллах зарчим

Хяналтгүй сургалтын алгоритмууд:

- K-Means Clustering
- Hierarchical Clustering
- Affinity Propagation
- Boltzmann Machine
- Restricted Boltzmann Machine (RBM)
- Autoencoder
- Variational Autoencoder (VAE)

3. Машин сургалтын алгоритмууд

Кибер халдлагуудыг илрүүлэх туршилт судалгааны ажлуудад дараах машин сургалтын аргуудыг онцлог шинж, чанараар нь сонгон хэрэглэдэг байна.

a) Модлог болон Ансамбл (Tree-based & Ensemble) алгоритмууд: Эдгээр нь их хэмжээний (Big Data), олон шинж чанартай (High-dimensional) өгөгдөлтэй ажиллахдаа өндөр нарийвчлал болон бат бөх чанараараа маш сайн.

- **Random Forest (RF):** Хэт таарах (overfitting) үзэгдлийг багасгаж, өндөр нарийвчлалтай үр дүн өгдөг бөгөөд их хэмжээний өгөгдөлд үр дүнтэй, шинж чанарын чухлыг (feature importance) тодорхойлох боломжтой.
- **Gradient Boosting (XGBoost, LightGBM, CatBoost):** Сургалтын явцад өмнөх модны алдааг засварлан, дараалаар илүү хүчирхэг модыг сургах бөгөөд Random Forest-оос илүү өндөр нарийвчлал, ялангуяа LightGBM нь маш хурдан бөгөөд их хэмжээний өгөгдөлд тохиромжтой (OD-IDS2022-д хамгийн тохиромжтой).
- **Decision Tree (DT):** Халдлага илрүүлэх дүрэм (rule-based) гаргахад ашиглагдах үндсэн суурь болдог бөгөөд үр дүн, шийдвэр гаргах логик нь маш сайн тайлбарлагдана.

b) Уламжлалт болон Статистик алгоритмууд: Эдгээр нь загварын үндсэн суурийг (baseline) тавих болон зарим нэг тодорхой төрлийн халдлагыг илрүүлэхэд ашиглагддаг.

- **Support Vector Machine (SVM):** Ангиллын хооронд хамгийн оновчтой заагийг олох төдийгүй өндөр хэмжээст өгөгдөлд сайн (82 features) бөгөөд kernel tricks ашиглан шугаман бус (non-linear) хамаарлыг шийддэг. Харин хэмжээ ихсэх тусам сургалт маш удаан болж, c, gamma параметрүүдийн утгаас хамаарч дахи дахин сургах шаардлагатай болдог.
- **K-Nearest Neighbors (KNN)**: Шинэ өгөгдлийг хамгийн ойр орчмын хөршүүд дээр үндэслэн ангилдаг. Энгийн бөгөөд ойлгоход хялбар боловч өгөгдлийн хэмжээ ихсэх тусам (OD-IDS2022) гүйцэтгэл болон хурд нь эрс мууддаг. Гэвч энэ сул талыг өгөгдлийг ангилах замаар засч чадвал эерэг үр дүн өндөртэй байх боломжтой юм.

- **Logistic Regression (LR) / Naive Bayes**: Шугаман ангилалд сайн тохирох бөгөөд шугаман хамааралгүй, олон төрлийн ангилалд тохиромжгүй байдаг. Тохирсон өгөгдөлтэй ажиллахад маш хурдан, тайлбарлахад хялбар давуу талтай.

Машин сургалтын алгоритмуудын шинж чанарууд

1-р хүснэгт

Алгоритм	***Давуу тал***	***Сул тал***	***OD-IDS2022 нийцэл***
Random Forest	Өндөр нарийвчлал, overfitting-ээс сэргийлнэ	Сургалт удаан, их RAM хэрэглэнэ	Маш сайн
LightGBM	Хурдан, imbalanced өгөгдөлд сайн	Тохиргоо төвөгтэй	Маш сайн
SVM	Нарийн шийдэл гаргана	Том өгөгдөлд удаан, төвөгтэй	Хязгаарлагдмал
KNN	Хялбар ойлгомжтой	Том өгөгдөлд удаан	Тохиромжгүй
Decision Tree	Тайлбарлахад хялбар	Overfitting амархан	Дунд түвшинд
Logistic Regression	Хурдан, 2 ангилалд сайн	Non-linear илрүүлэхгүй	Хязгаарлагдмал

Дээрх хүснэгтээс харахад OD-IDS2022 зэрэг орчин үеийн нарийн төвөгтэй, шинэ халдлагуудын шинэ чанарыг агуулсан багцуудад ашиглах, өндөр гүйцэтгэлтэй үр дүнг үзүүлэх боломжтой алгоритмуудыг сонгох боломжтой байна.

4. Кибер аюулгүй байдалд ашиглах нь

Кибер халдлагууд улам бүр нэмэгдэж байгаа энэ үед халдагчид шинэ эмзэг байдлуудыг хайж, хамгаалалтыг нэвтрэх олон төрлийн аргуудыг ашиглан улам нарийссан хэлбэрээр довтолж байна. Энэ нь байгууллагууд өөрсдийн халдлагад өртөх байдлыг бууруулахын зэрэгцээ өсөн нэмэгдэж буй IT дэд бүтцээ ч мөн адил бэхжүүлэх шаардлагатай гэсэн үг юм. Ингэхдээ ихэнхдээ хязгаарлагдмал нөөцөөр хийх шаардлагатай болдог. Харин мэргэжилтнүүд кибер аюулгүй байдлын практикийг сайжруулахын тулд машин сургалтын боломжуудыг ашиглан, уламжлалт аргуудтай нэгтгэх явдал юм. Машин сургалт кибер аюулгүй байдлын чиглэлээр дараах хэд хэдэн аргаар дэмжлэг үзүүлэх боломжтой. Үүнд:

- Машин сургалтын загварууд их хэмжээний өгөгдлийг хурдан хугацаанд, хүний алдааг багасган боловсруулж чаддаг.
- Машин сургалт болон хиймэл оюуны системүүд аюултай байж болзошгүй үйлдлийг хурдан илрүүлж, сэжигтэй үйл ажиллагааг тодорхойлж, автоматаар тусгаарлах, шийдвэрлэх арга хэмжээг авдаг.
- Машин сургалтын загваруудыг ирээдүйн аюулыг урьдчилан таамаглаж, ердийн систем эсвэл хэрэглэгчийн зан үйлээс хазайсан хэв маягийг илрүүлэн урьдчилан сэргийлэх үйлдэл хийхээр сургах боломжтой.

V. ӨГӨГДӨЛ ЦУГЛУУЛАХ, ТОХИРОХ МАШИН СУРГАЛТЫН АЛГОРИТМ СОНГОХ

1. Өгөгдлийн санг үүсгэх

Энэ судалгаанд олон төрлийн сүлжээний халдлагын төрөл, хэвийн урсгалыг багтаасан, машин сургалтын загваруудыг хөгжүүлэхэд тохиромжтой OD-IDS2022 (Offensive-Defensive Intrusion Detection Dataset) өгөгдлийн багцыг ашиглахаар сонгосон. Энэ өгөгдлийн багц нь компьютерын сүлжээг хортой үйл ажиллагаанаас хамгаалах зорилгоор IDS системээр хянагдаж буй өгөгдлийг агуулдаг. IDS өгөгдлийн багцыг машин сургалтын алгоритмуудыг сүлжээний халдлага илрүүлэхэд сургах, үнэлэхэд ашигладаг. Түүнчлэн халдлагыг илрүүлэх шинэ арга боловсруулах эсвэл одоо байгаа системийн нарийвчлалыг сайжруулах зэрэг судалгааны зориулалтаар ашиглаж болно [3].

Эдгээр өгөгдлийн багцыг олон эх үүсвэрээс, тухайлбал олон нийтэд нээлттэй, арилжааны, эсвэл байгууллагууд өөрсдийн зориулалтаар үүсгэсэн хувийн өгөгдлийн сангаас олж авах боломжтой. Өгөгдлийн чанар нь өгөгдөл цуглуулах арга, өгөгдлийн эх үүсвэр, өгөгдлийг шошголох үйл явц зэрэг хүчин зүйлсээс хамаарна. IDS өгөгдлийн багц нь тэнцвэргүй байж болох бөгөөд ихэнх нь хэвийн өгөгдөл, цөөн хэсэг нь хортой өгөгдөл байх боломжтой. Энэ нь машин сургалтын алгоритмуудын нарийвчлалд нөлөөлж болох тул өгөгдлийг шинжилгээнд бэлтгэхдээ анхаарах шаардлагатай. Халдлагыг илрүүлэх арга нь машин сургалтын алгоритмуудыг ашиглан хэвийн болон халдлагатай сүлжээний урсгалыг агуулсан өгөгдлийн багцаар сургах явдал юм. IDS өгөгдлийн багц нь машин сургалтын алгоритмуудын нарийвчлал, үр нөлөөнд нөлөөлж болох хэд хэдэн сорилтыг агуулдаг. Үүнд:

- Тэнцвэргүй ангиуд (Imbalanced Classes)
- Өндөр хэмжээс (High Dimensionality)
- Хурдтай хувьсан өөрчлөгдөж буй халдлагууд (Evolving Threats)
- Өгөгдлийн чанар (Data Quality)
- Өргөтгөх чадвар (Scalability)

Эдгээр сорилтыг IDS өгөгдлийн багцыг бэлтгэх, шинжлэх явцад тооцох шаардлагатай бөгөөд өгөгдлийн чанарыг сайжруулахын тулд oversampling, feature selection, feature engineering зэрэг өгөгдөл урьдчилан боловсруулах аргуудыг ашиглаж, машин сургалтын алгоритмуудын нарийвчлалыг нэмэгдүүлэх боломжтой.

OD-IDS2022 датасэт нь LAN орчинд халдлага (DDoS, DoS, Brute Force, Port Scan гэх мэт) болон хэвийн

үйлдлийг эмуляци хийж цуглуулсан 1,031,916 тохиолдол, 82 flow-based шинж чанар (features) ба 29 ангилал (classes) агуулсан бэлэн боловсруулсан өгөгдлийн багц бөгөөд IDS болон anomaly detection загваруудыг сургалт, туршилт хийхэд шууд ашиглахад тохиромжтой.

2. Тохирох машин сургалтын алгоритм сонгох

Сүлжээний халдлагыг илрүүлэхийн тулд өгөгдлийн нарийн төвөгтэй хэв маягийг зохицуулж, хэвийн болон хортой урсгалыг ялгаж, найдвартай ангиллыг хангадаг машин сургалтын загваруудыг шаарддаг. OD-IDS 2022 өгөгдлийн багц нь шошготой өгөгдлийг агуулдаг тул хяналттай (supervised) сургалтын өгөгдлийн багц бөгөөд том хэмжээ**,** олон төрлийн шинж чанар, олон ангилал, anomaly detection-д шаардлагатай өгөгдлийн төрөлтэй нийцэж байгаад нь тулгуурлан Decision Tree, Random Forest, LightGBM, KNN зэрэг алгоритмуудыг сонгож туршилтыг хийсэн. Decision Tree ба Random Forest нь шийдвэр гаргалт ойлгомжтой, overfitting-д тэсвэртэй; LightGBM нь том өгөгдөлд хурдан, өндөр нарийвчлалтай, KNN нь anomaly detection-д тохиромжтой. Шинж чанаруудыг нарийвчлан сонгосноор загваруудын нарийвчлал, илрүүлэлтийн үзүүлэлтийг сайжруулдаг.

Decision Tree (шийдвэрийн мод) нь өгөгдлийг ангилахдаа мэдээллийн онолын хэмжээс болох *энтропи* болон *information gain*-ийг ашиглан хамгийн сайн ялгагдах шинж чанарыг сонгож мод байгуулдаг. Энэхүү арга нь өгөгдлийн тодорхойгүй байдлыг багасгах, мэдээлэл хамгийн их агуулсан салбарлалыг үүсгэх зарчимд тулгуурладаг.

Энтропи – эмх замбараагүй байдал

$$H(D) = -\sum_{i=1}^{k} p_i log_2 p_i \quad (1)$$

- D — өгөгдлийн багц
- p_i — i-р ангиллын магадлал

Энтропи бага байх тусам өгөгдлийн эмх замбараагүй байдал багасан, ангилахад илүү хялбар болдог. **Information Gain – хамгийн сайн шинж сонгох үндэслэл**

$$IG(D, A) = H(D) - \sum_{v \in Values(A)} \frac{|D_v|}{|D|} * H(D_v) \quad (2)$$

- A — шинж чанар
- D_v — A шинжийн v утгатай өгөгдлийн дэд хэсэг

Decision Tree нь хамгийн өндөр мэдээллийн өсөлт өгдөг шинж чанарыг сонгон модны зангилаа байгуулдаг. Энэ нь алгоритмын нарийвчлал, тайлбарлах чадварыг нэмэгдүүлдэг. Өөрөөр хэлбэл Information Gain өндөр байх тусам хуваалт сайн хуваагдсан гэж үзнэ.

LightGBM нь Gradient Boosting Decision Tree (GBDT)-ийн зарчимд тулгуурлан дараагийн модыг өмнөх үеийн алдааг багасгах чиглэлээр сургадаг бөгөөд *градиент бууралтын boosting* зарчим болон *leaf-wise tree growth strategy*-г ашигладаг. Ингэснээр сургалт хурдан, гүйцэтгэл өндөр, их хэмжээний өгөгдөл дээр маш үр дүнтэй ажилладаг. **Loss function – ангиллын алдагдлын хэмжээ** Бинар ангилалд лог алдагдлын функц хэрэглэнэ:

$$L = -\sum_{i=1}^{n} [y_i \log(p_i) + (1 - y_i) \log(1 - p_i)] \quad (3)$$

- y_i — бодит 0/1 шошго
- p_i — таамагласан магадлал

Энэхүү функц нь таамаглал буруу байх үед өндөр утга авдаг тул LightGBM дараагийн модыг уг алдагдлын градиент дээр тулгуурлан сайжруулдаг. Ингэснээр үе шат бүрд загвар нь халдлага ба хэвийн траффикыг ялгах чадвараа сайжруулдаг. Моддын тоо (n_estimators), суралцах хурд (learning_rate), модны гүн (max_depth) болон навчны тоо (num_leaves) зэрэг гол параметрүүд нь загварын нарийвчлал болон overfitting-ийн түвшинд шууд нөлөөлдөг.

Машин сургалтын загваруудын параметрийн тодорхойлолт

2-Р ХҮСНЭГТ

Algorithm	*Гол параметрүүд*	*Тайлбар*
Random Forest	n_estimators, max depth, max features	Ensemble арга, overfitting-ийг багасгаж нарийвчлал нэмдэг
Decision Tree	Max depth, min samples split, criterion	Энгийн бүтэцтэй, урсгалыг ангилдаг
k-Nearest Neighbors	k, distance metric, weights	Логистик ангилалд суурилсан таамаглал загвар
LightGBM	Number of leaves, learning rate, n_estimators, max_depth	Non-parametric, anomaly detection-д тохиромжтой

VI. ХАЛДЛАГА ИЛРҮҮЛЭХ ЗАГВАР БОЛОВСРУУЛАХ, ҮР ДҮНГ ШАЛГАХ

Туршилтыг хийхдээ Google-ийн үүлэн дээр суурилсан Python програмчлалын орчин Colab дээр хийж гүйцэтгэсэн [5]. Судалгаанд ашиглагдсан илрүүлэлтийн системийн архитектурыг 3-р зурагт үзүүлэв.

3-р зураг. Гүйцэтгэх туршилтын ажлын дараалал

1. Машин сургалтын загваруудад тохируулж өгөгдлөө боловсруулах

Туршилтын ажлыг Google Colab орчинд гүйцэтгэсэн бөгөөд бүх загварчлал, сургалт, туршилт, баталгаажуулалтыг Python хэл дээр хийсэн. Шаардлагатай номын сангууд нь Pandas, NumPy, Matplotlib, Seaborn байв. Үүний дараа Google drive-тай холбогдож CSV өргөтгөлтэй өгөгдлийн багцыг уншина. Боловсруулалтын эхний шатанд өгөгдлөөс дутуу болон хэт давхардсан мөрүүдийг устгаж, IP болон Label зэрэг ангилалд нөлөөлөхгүй, ялгаагүй шинж чанаруудыг (Src IP, Dst IP, Label) хасч, Protocol баганыг one-hot encoding аргаар хөрвүүлж, машин сургалтын моделд ашиглах боломжтой тоон утгуудад хувиргаж байгаа юм. IP хаягийг хасч байгаа шалтгаан нь загварууд нь хэв маягийг сурахаас илүү IP-г цээжилж хуурах зарчмаар үр дүнд ихээхэн нөлөөлдөг. “Label” багана нь BENIGN (хэвийн) эсвэл Attack Type (халдлага) гэсэн шошготой байсан бөгөөд судалгааны зорилгоор үүнийг BENIGN → 0, ATTACK → 1 төлөвт хөрвүүлсэн. Үүний дараа өгөгдлийг 80% сургалтын, 20% тестийн хэсэгт хуваана. Энэ нь загварыг зөв сургах болон шалгахад зайлшгүй шаардлагатай алхам юм.

Шинж чанарын сонголтод дараах аргууд ашиглагдсан: VarianceThreshold — маш бага хувийн хэлбэлзэлтэй (variance < 0.01) шинж чанаруудыг хасав. Ингэснээр зөвхөн өгөгдөлд бодит хувьсал оруулж буй онцлогууд үлдэж, загвар сургах үр ашиг нэмэгдэнэ. SelectKBest (mutual_info_classif) — хамгийн их мэдээлэлийг өгдөг 30 шинж чанарыг сонгов. Энэ нь загварыг илүү үр дүнтэй сургах, мөн тооцооллын ачааллыг багасгах зорилготой. Энэ нь хэт тааруулалт (overfitting)-аас сэргийлнэ, илүү хурдан үр дүнтэй сургалт болон утга багатай шинж чанаруудыг хасч зөвхөн чухлыг нь ашиглах юм. Үүний дараа өгөгдлийн хэмжээг жигдрүүлэх зорилготой StandardScaler аргыг ашиглав Энэ нь машин сургалтын урьдчилсан боловсруулалтын нийтлэг алхам бөгөөд ялангуяа онцлогуудын хэмжээ мэдрэмтгий алгоритмууд жишээлбэл KNN дээр чухал ач холбогдолтой.

2. Загваруудыг сургах болон тестлэх

Өгөгдлийн урьдчилсан боловсруулалт хийсний дараагаар Decision Tree, Random Forest, KNN, болон LightGBM гэх машин сургалтын загваруудыг ашиглан сургалтыг гүйцэтгэнэ. Гүнийг 9-р хязгаарласан нь мод хэт урт болохоос сэргийлж, хэт тааруулалт (overfitting)-аас хамгаалах бөгөөд ангиллын тэнцвэргүй байдалд дасан зохицохын тулд balanced жингээр тохируулсан шийдвэрийн модны ангилагч үүсгэж байна (max_depth=9, class_weight=’balanced’). Үүний дараа 100 ширхэг шийдвэрийн мод ашиглан ой мод үүсгэж, гүнийг 9-р хязгаарласан шийдвэрийн модноос бүрдэх, overfitting-с хамгаалсан санамсаргүй ой модны ангилагч үүсгэж байна (n_estimators=100, max_depth=9, class_weight=’balanced’). KNN ангилагчийг үүсгэхэд таамаглал гаргахдаа хамгийн ойрын 3 өгөгдлийн ангиллыг харгалзан шийдвэр гаргана. хамгийн ойрын 3 хөршийг авч үзэж, ойрын хөршийг хайхдаа автомат алгоритм сонгоно. Мөн бүх боломжит CPU цөмүүдийг ашиглан тооцооллыг хурдатгана (n_neighbors=3, algorithm=’auto’, n_jobs=-1). Харин LightGBM ангилагчийг үүсгэхдээ мод бүрийн хамгийн их гүн 9, 100 ширхэг шийдвэрийн мод (decision trees)-оор бүрдсэн ансамбль загвар үүсгэн, суралцах хурд 0.1 болгоно. Иймэрхүү жижиг утга нь суралцах процессыг удаашруулдаг ч загварыг тогтвортой, нарийн болгож, хэт тааруулалтаас сэргийлнэ (n_estimators=100, learning_rate=0.1, max_depth=9). Ингээд 4 ангилагч загварыг сургалтын өгөгдөл дээр сургаж байна

- DT.fit(X_train_scaled, y_train)
- RF.fit(X_train_scaled, y_train)
- KNN.fit(X_train_scaled, y_train)
- LGBM.fit(X_train_scaled, y_train).

3. Загваруудын сургалт, хэмжигдэхүүнүүд

Машин сургалтын туршилтад загваруудыг зөвхөн сургахаас гадна тэдгээрийн үр дүнд системтэй шинжилгээ хийх нь үр дүнгийн чанарыг үнэлэх, хэт тохирох эсвэл дутуу тохирох зэрэг асуудлыг илрүүлэх, цаашдын сайжруулалтын чиглэлийг тодорхойлох чухал алхам юм. Шинжилгээ хийхдээ Decision Tree, Random Forest, KNN болон LightGBM зэрэг ангилагч загваруудын сургалтын болон шалгалтын үеийн гүйцэтгэлийг харьцуулан үнэлж, тэдгээрийн нарийвчлал (Accuracy), F1-үнэлгээ (F1-score), Мэдрэмж (Sensitvity), тодорхойлох чадвар (Precision), Дурсамж (Recall), хуурамч эерэг(false positive) ба үнэн эерэг(true positive) тоо зэргээр дүн шинжилгээ хийх болно. Мөн загвар тус бүрийн ROC-AUC зэрэг гүйцэтгэлийн хэмжигдэхүүнүүдийг авч үзэх болно [6].

Accuracy нь тус загварын зөв таамаглалын хувийг илтгэнэ.

$$Accuracy=(TP+TN)/(TP+TN+FP+FN) \quad (1)$$

Recall нь бодит эерэг тохиолдлуудаас хэдийг нь зөв таньсан байгааг илтгэнэ.

$$Recall=TP/(TP+FN) \quad (2)$$

Precision нь халдлага гэж таамагласан тохиолдлуудаас хэд нь үнэхээр халдлага байсан бэ гэдгийг илэрхийлнэ.

$$Precision=TP/(TP+FP) \quad (3)$$

F1 Score нь нийт гүйцэтгэлийн чанарыг илэрхийлнэ.

$$F1\ Score=2*Precision*Recall/(Precision+Recall) \quad (4)$$

Confusion Matrix нь загварын таамаглалын бодит үр дүнг харьцуулсан 2x2 хүснэгт юм [7].

TP: Халдлага байсан, систем зөв илрүүлсэн;
FN: Халдлага байсан ч систем илрүүлж чадаагүй;
FP: Халдлага байгаагүй, систем халдлага гэж буруу илрүүлсэн;
TN: Халдлага байгаагүй, систем энгийн гэж зөв таньсан;

ROC Curve нь Positive болон Negative утгуудын харьцааг харуулна. AUC (Area Under Curve) 1-д ойр байх тусам моделийг сайн гэж үзнэ.

X-axis:

$$False\ Positive\ Rate=FP/(FP+TN) \quad (5)$$

Y-axis:

$$True\ Positive\ Rate=TP/(TP+TN) \quad (6)$$

4. Тестийн үр дүнгийн шинжилгээ

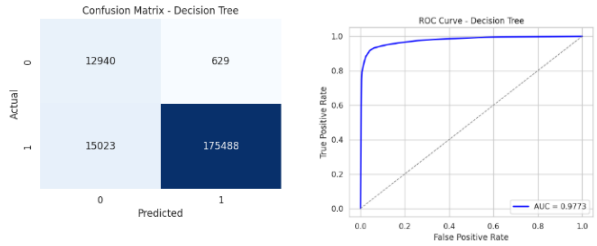
Туршилтын үр дүнг загвар тус бүрээр болон нийт дүнгээр танилцуулж, харьцуулсан болно. Туршилтын өгөгдөл дээрх гүйцэтгэлийг дараах байдлаар үнэлнэ: Accuracy, Precision, Recall, F1 score, Төөрөгдлийн матриц, ROC муруй, мөн сургалтын загварын хамгийн нөлөө бүхий шинж чанарууд гэх мэт гол үзүүлэлтүүдийн үр дүнг харуулна.

Decision tree загварын туршилтын үр дүн:

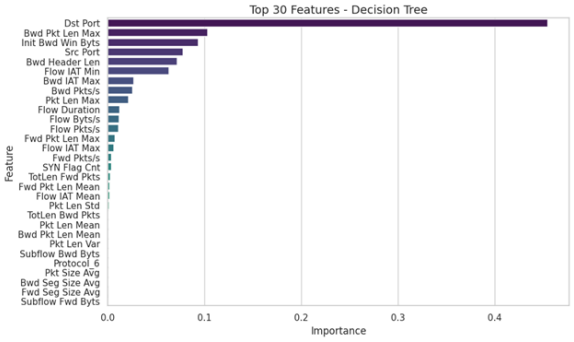
Decision tree загварын гүйцэтгэлийн үнэлгээ

3-Р ХҮСНЭГТ

Хэмжигдэхүүн	*Оноо*
The Decision Tree Classifier Model Accuracy	0.9233
The Decision Tree Classifier Model Precision	0.9964
The Decision Tree Classifier Model Recall	0.9211
The Decision Tree Classifier Model F1 Score	0.9573



4-р зураг. Decision tree загварын гүйцэтгэлийн үзүүлэлтүүд



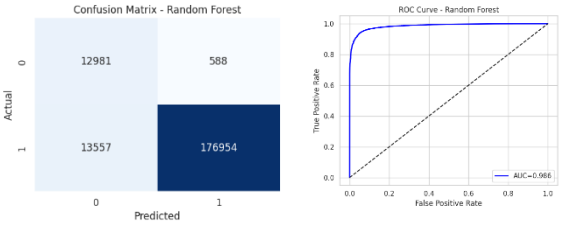
5-р зураг. Decision tree загварын чухлаар эрэмбэлсэн 30 онцлог

Random forest загварын туршилтын үр дүн:

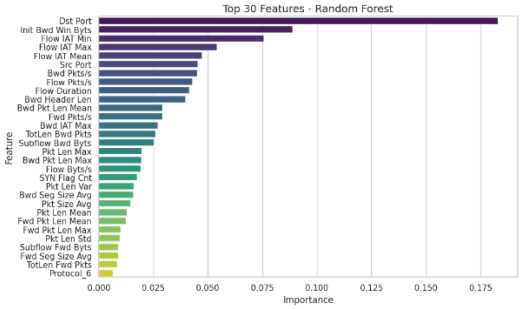
Random forest загварын гүйцэтгэлийн үнэлгээ

4-Р ХҮСНЭГТ

Хэмжигдэхүүн	*Оноо*
The Random Forest Classifier Model Accuracy	0.9307
The Random Forest Classifier Model Precision	0.9967
The Random Forest Classifier Model Recall	0.9288
The Random Forest Classifier Model F1 Score	0.9616



6-р зураг. Random forest загварын гүйцэтгэлийн үзүүлэлтүүд



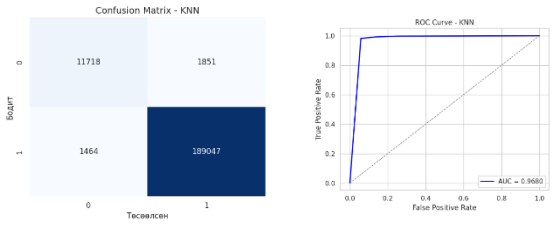
7-р зураг. Random forest загварын чухлаар эрэмбэлсэн 30 онцлог

KNN загварын туршилтын үр дүн:

KNN загварын гүйцэтгэлийн үнэлгээ

5-Р ХҮСНЭГТ

Хэмжигдэхүүн	*Оноо*
The K-Nearest Neighbors Classifier Model Accuracy	0.9838
The K-Nearest Neighbors Classifier Model Precision	0.9903
The K-Nearest Neighbors Classifier Model Recall	0.9923
The K-Nearest Neighbors Classifier Model F1 Score	0.9913



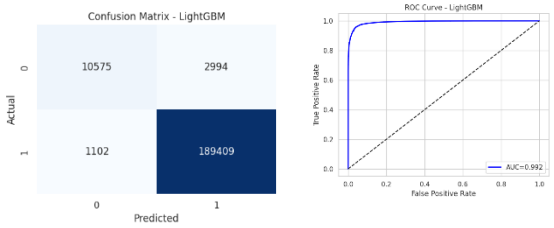
8-р зураг. KNN загварын гүйцэтгэлийн үзүүлэлтүүд

LightGBM загварын туршилтын үр дүн:

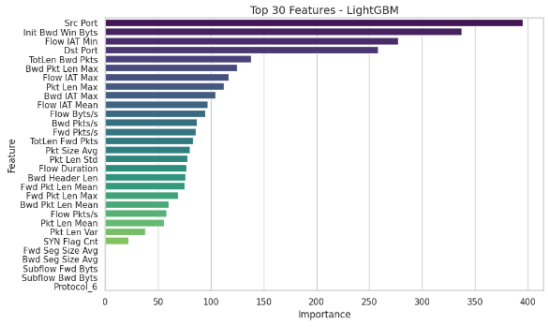
LightGBM загварын гүйцэтгэлийн үнэлгээ

6-Р ХҮСНЭГТ

Хэмжигдэхүүн	*Оноо*
The LightGBM Classifier Model Accuracy	0.9799
The LightGBM Classifier Model Precision	0.9844
The LightGBM Classifier Model Recall	0.9942
The LightGBM Classifier Model F1 Score	0.9893



9-р зураг. LightGBM загварын гүйцэтгэлийн үзүүлэлтүүд



10-р зураг. LightGBM загварын чухлаар эрэмбэлсэн 30 онцлог

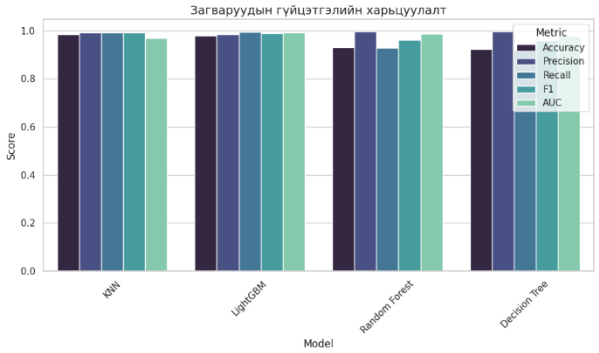
Загваруудын үзүүлэлтийн харьцуулалт:

Энэ хэсэгт Random Forest, Decision Tree, LightGBM, KNN гэсэн машин сургалтын загваруудын гүйцэтгэлийг нарийвчлал (Accuracy), мэдрэмж (Sensitivity / Recall), нарийн тодорхойлох чадвар (Precision), F1-үнэлгээ (F1 Score) гэсэн дөрвөн үнэлгээний хэмжүүрээр харьцуулсан баганан графикаар үзүүлнэ.

Загваруудын үзүүлэлтийн харьцуулалт

7-Р ХҮСНЭГТ

Загвар	Accuracy	Precision	Recall	F1 Score
KNN	0.983756	0.990304	0.992315	0.991309
LightGBM	0.979929	0.984439	0.994216	0.989303
Random forest	0.930689	0.996688	0.928839	0.961568
Decision tree	0.923305	0.996429	0.921144	0.957308



11-р зураг. Загваруудын үзүүлэлтийн харьцуулалтын график

VII. ДҮГНЭЛТ

Энэхүү судалгаанд сүлжээний халдлагын илрүүлэлтэд зориулан OD-IDS2022 бэлэн боловсруулсан датасэтийг сонгон авч, Decision Tree, Random Forest, LightGBM болон k-Nearest Neighbors зэрэг машин сургалтын алгоритмуудыг ашиглан халдлагыг илрүүлсэн. Эдгээр алгоритмуудын туршилтаас үзэхэд, тухайн өгөгдлийн багц дээрх гүйцэтгэл, илрүүлэлтийн нарийвчлал, бүрэн байдал зэрэг шалгуурын дагуу тохирох алгоритмыг сонгох нь чухал байсан. Өгөгдлийн сангийн чанар, онцлог чанарууд нь алгоритмын амжилттай ажиллахад шууд нөлөөлнө. Тиймээс, тус бүрийн алгоритмд тохирох онцлог сонголтыг хийх нь сүлжээний халдлагыг илрүүлэх системийн гүйцэтгэлд чухал үүрэгтэй. Иймээс OD-IDS2022-ийн 1,031,916 тохиолдол, 82 шинж чанар, 29 ангилал зэрэг нь сонгосон алгоритмуудын сургалт, үнэлгээнд шууд ашиглахад тохиромжтой болсон.

Өгөгдлийн чанар, онцлог шинжүүд нь сонгогдох алгоритмд шууд нөлөөтэй бөгөөд илрүүлэлтийн гүйцэтгэлийг тодорхойлдог. Энэхүү судалгаанд гарсан KNN, LightGBM, Random Forest, Decision Tree алгоритмын үр дүнг практикт дараах байдлаар ашиглаж болно:

- **KNN (Accuracy: 0.9838, Recall: 0.9923) Хэрэглээ:** KNN алгоритм нь халдлагыг алддаггүй, мэдрэмж өндөр тул сүлжээнд халдлагыг цаг алдалгүй илрүүлэх гол IDS системд ашиглахад тохиромжтой. **Жишээ:**

Байгууллагын дотоод сүлжээнд ransomware, malware халдлагыг хянахад KNN өндөр үр дүнтэй. Харин том хэмжээний өгөгдөлд боловсруулалтын хугацаа урт байж болох тул real-time системд бага зэрэг тохируулга шаардлагатай.

- **LightGBM (Recall: 0.9942, Precision: 0.9844) Хэрэглээ:** Recall хамгийн өндөр тул халдлагыг аль болох алдахгүй илрүүлэх шаардлагатай тохиолдолд хамгийн тохиромжтой. **Жишээ:** Firewall эсвэл NGFW-д IDS/IPS модульд суулгаж, халдлагын эсрэг мэдрэмжийг нэмэгдүүлэхэд тохиромжтой.
- **Random Forest (Precision: 0.9967, Recall: 0.9288) Хэрэглээ:** Олсон халдлагыг зөв таних чадвар өндөр байна. **Жишээ:** Өндөр аюултай халдлагыг ялгах, false positive багатай alert үүсгэх зорилготой системд Random Forest ашиглахад тохиромжтой.
- **Decision Tree (Precision: 0.9964, Recall: 0.9211) Хэрэглээ:** Хурдан боловсруулалт хийх, real-time хянах хэрэгсэлд тохиромжтой. **Жишээ:** Шинэ сүлжээний сегментэд quick deployment хийх, халдлагын үндсэн загварыг туршихад тохиромжтой.

Машин сургалт (Machine Learning) нь сүлжээний халдлагыг илрүүлэхэд уламжлалт аргачлалууд хүрч чадаагүй хэвийн бус байдал, шинэ төрлийн халдлагуудыг илрүүлэх өндөр чадамжтай хүчтэй хэрэгсэл болж хөгжиж байна. Хэдий одоо ашиглагдаж буй илрүүлэх системүүд тодорхой үр дүн үзүүлж байгаа ч, бодит цагийн нөхцөлд ажиллах болон хувьсан өөрчлөгдөж буй аюул заналд хурдан хариу өгөх чадамж дутмаг хэвээр байна. Харин машин сургалт нь эдгээр асуудлуудыг шийдвэрлэхэд тусалж, системийн нарийвчлал, уян хатан байдал болон автомат хариу арга хэмжээ авах боломжуудыг нэмэгдүүлж чадна. Машин сургалтын тусламжтайгаар сүлжээний халдлагыг бодит цагт илрүүлж, автомат хамгаалалт авч хэрэгжүүлэх боломжтой болсон нь кибер аюулгүй байдлын салбарт томоохон дэвшил авчирч байна. Сайн боловсруулсан өгөгдөл, зөв сонгосон алгоритм нь сүлжээний хамгаалалтын системийн бүтээмж, үр нөлөөг мэдэгдэхүйц нэмэгдүүлэх гол түлхүүр юм.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Stallings, W (2017). *Network Security Essentials: Applications and Standards*, 6th Edition. Pearson. Chapter 1.

[2] Tanium staff (2024). *Machine Learning in Cybersecurity.* https://www.tanium.com/blog/machine-learning-in-cybersecurity/

[3] Narottam Das Patel, Rajeev Wankar (2023) *OD-IDS2022. Generating a New Offensive Defensive Intrusion Detection Dataset for Machine Learning-Based Attack Classification* pages 1-15

[4] Dave Bergmann (2024). *The 2025 guide to machine learnig* https://www.ibm.com/think/topics/machine-learning

[5] Andrii Chornyi (2024). *Google Colab*. https://codefinity.com/blog/Google-Colab-Tutorial

[6] Vidhi Chugh (2024). *AUC and ROC Curve in Machine learning* https://www.datacamp.com/tutorial/auc

[7] GeeksforGeeks (2025). *Machine learning tutorial*. https://www.geeksforgeeks.org/machine-learning

ГҮН СУРГАЛТААР НИЙТИЙН ТЭЭВРИЙН МАРШРУТЫГ ОНОВЧЛОХ НЬ

Сайнжаргалын ГАНХУЯГ[1], Мөнхбаярын ЦЭЦЭНЦЭНГЭЛ[2], Дашдоржийн ЗОЛЗАЯА[3]

[1,2,3] Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны Технологийн Сургууль, Компьютерийн ухааны тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: gankhuyag@ikhzasag.edu.mn[1]

Хураангуй: **Улаанбаатар хотын нийтийн тээврийн түгжрэл нь улс оронд тулгамдаж буй асуудлуудын нэг бөгөөд автобусны үр ашиггүй маршрутууд голлон нөлөөлж байна. Энэхүү судалгаандаа бид бодит өгөгдөлд тулгуурлан одоо ашиглагдаж буй автобусны маршрутууд, зорчигчдын урсгал, автобусны буудлын байршил, сонирхлын цэгүүд (POI) автобусны маршрутыг оновчлох туршилт хийсэн. Туршилтыг хийхдээ графын аргаар загварчилж, боломжит маршрутын хувилбаруудыг үнэллээ. Оновчлолыг Reinforcement learning аргад Хийсвэр хайлтын арга (Simulated Annealing) ашиглан гүйцэтгэсэн бөгөөд энэхүү үйл явцыг зорчигчдын бодит урсгал болон POI-д суурилсан мэдээллийг нэгтгэсэн эрэлтийн загвар загварчилсан. Үр дүнд нь 98.8% хамралттай, 1,112 буудлаас 1,094-д үйлчлэх сүлжээ бүрдэж, оргилдоо 543 автобус шаардагдана; ингэснээр газарзүйн хүртээмжийг алдагдуулахгүйгээр паркийн үр ашгийг ~22–28% нэмэх боломжтойг харууллаа. Ингэж загварчилж, тооцооллоор автобусны үйлчилгээний хамрах хүрээ болон үр ашиг мэдэгдэхүйц сайжирсан нь судалгааны үр дүнгээр нотлогдож, хотын хөдөлгөөний оновчтой төлөвлөлтийн үндэс суурь болох боломжтойг харуулж байна.**

Түлхүүр үг—нийтийн тээвэр, маршрут, оновчлол, сонирхлын цэгүүд(POI), зорчигчдын урсгал

I. УДИРТГАЛ

Улаанбаатар хотын нийтийн тээврийн систем нь хурдацтай хотжилт, автомашины эзэмшлийн өсөлт болон зорчих эрэлтийн нэмэгдлээс шалтгаалан улам бүр хүндрэлтэй тулгарч байна. Хотын нийтийн тээврийн гол хэрэгсэл нь автобус боловч одоогийн ашиглаж буй автобусны сүлжээ нь маршрутын давхцал ихтэй, тойруу зам, чухал бүсүүдтэй хангалтгүй холбогдсон зэрэг үр ашиггүй байдлаар төлөвлөгдсөн байна. Энэхүү туршилтын зорилго нь зорчигчдын урсгал болон сонирхлын цэгүүдийн (POI) тархалтын өгөгдөлд тулгуурлан автобусны маршрутыг өгөгдөлд суурилсан аргаар оновчлох, ингэснээр эрэлтийг хангахад шаардлагатай хамрах хүрээ, сүлжээний үр ашиг, зорчигчийн тав тухыг тэнцвэржүүлсэн маршрутын төлөвлөлтийг боловсруулах явдал юм. Автобусны маршрутын сүлжээг оновчлох нь түгжрэлийг бууруулах, зорчих хүртээмжийг сайжруулах, мөн түгжрэлгүй хотын хөдөлгөөнийг буюу нэвтрэх хурдыг нэмэгдүүлэхэд чухал ач холбогдолтой. [1]

II. ӨГӨГДӨЛ БА АРГАЗҮЙ

Судалгаанд дараах дөрвөн төрлийн өгөгдлийг ашигласан:

- **Автобусны маршрутууд:** Одоогийн коридорын бүтэц болон маршрутын тодорхойлолтууд.
- **Зорчигчдын урсгал:** Эхлэл–зорилгын (OD) гэсэн хосууд болон эрэлтийн эрчмүүд [3].
- **Автобусны буудлууд:** Сүлжээний буудлуудын газар зүйн координат болон кодчилол.
- **Сонирхлын цэгүүд (POI):** Сургууль, эмнэлэг, зах, албан байгууллага зэрэг сонгож авсан үйл ажиллагааны төвүүд.

1-Р ХҮСНЭГТ. ТУРШИЛТЫН ӨГӨГДЛҮҮД

Өгөгдөл	Хэмжээ	Тайлбар
Автобусны чиглэл	115 чиглэл, 3835.94 км	Одоогийн коридор бүтэц болон чиглэлийн мэдээлэл.
Зорчилт урсгал	3 сар	Зорчигчийн эхлэл-зорилгын хос ба эрэлтийн хүчдэл.
Автобусны буудал	1,112 автобусны буудал 4,949 холбоос	Автобусны буудлын сүлжээний газарзүйн координат болон мэдээлэл.
Сонирхлын цэг	11,015	Сургууль, эмнэлэг, зах, оффис гэх мэт объектууд.

III. АРГА ЗҮЙ

Автобусны одоогийн маршрутын тодорхойлолт болон буудлуудын орон зайн ойролцоо байдлыг ашиглан **буудал–буудлын граф** байгуулсан.

Графын оройн цэгүүдийн холбоос бүрт газар зүйн зайг Хаверсинусын томьёо (1)-гоор олж жин болгож авсан. POI кластерыг хамгийн ойрын буудалтай холбож, тухайн ангиллын онцлогоос (жишээлбэл: сургууль, эмнэлэг, зах зэрэгт өндөр

жин оноох) шалтгаалсан нуугдмал эрэлт (latent

$$d = 2r\ arcsin(\sqrt{sin^2(\frac{\phi_2-\phi_1}{2}) + cos(\phi_1)cos(\phi_2)sin^2(\frac{\lambda_2-\lambda_1}{2})}) \quad (1)$$

demand)-ийг үүсгэсэн.
Энд,

- r -Дэлхийн радиус (≈ 6371 км);
- ϕ_1, ϕ_2 -хоёр цэгийн өргөрөг (рад);
- λ_1, λ_2 - хоёр цэгийн уртраг (рад);
- d - хоёр цэгийн хоорондох зай

A. Эрэлтийн загвар

Нийт эрэлтийг дараах хоёр бүрэлдэхүүнтэйгээр тодорхойлсон.

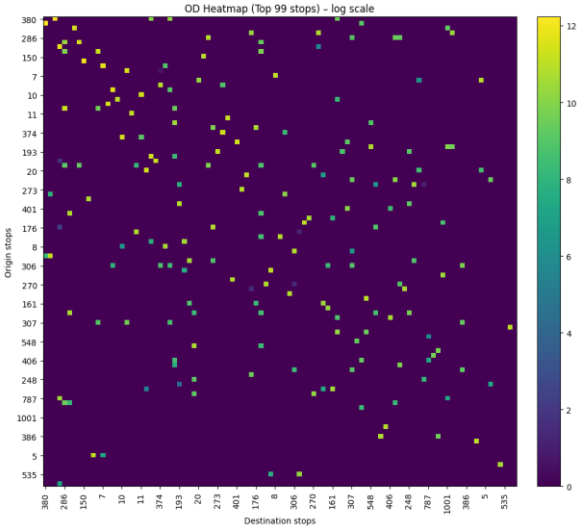
$$D(u,v) = D_{\text{observed}}(u,v) + \alpha \cdot \frac{P(u)\,P(v)}{\text{shortest\_path\_distance}(u,v) + 0.5} \quad (2)$$

Энд,

- $D_{observed}$ - Зорчилт (OD урсгалаас).
- P - тухайн автобусны буудал дахь POI хүндийн жин (жишээ нь: сургууль, эмнэлэг, захууд илүү хүнд байна)
- α - нуугдмал (POI-д суурилсан) эрэлтийн коэффициент (туршилтад 0.15 тогтмол утгаар авав)
- u, v - автобусны буудал

Үүнд:

- **Бодит эрэлт:** Зорчигчдын урсгалын өгөгдлөөс авсан OD хосууд (хос цэг).
- **Нуугдмал эрэлт:** POI кластеруудын хоорондын зайг таталцлын загвараар тооцож, зайн урвуу хэмжээгээр жигнэсэн.



1-р зураг. 100x100 харьцаатай OD матрицын дулааны зураглал

[KPI] Original served stops (approx): 1101
[KPI] Optimized served stops: 1099
[KPI] Unserved after optimization: 12

A. Боломжит маршрутын үүсгэлт (Simulated annealing)

Уг хийсвэр оновчлолын аргыг ашиглан боломжит маршрутын багцыг сонгов. k -тооны маршрутын хязгаарлалтуудыг дараах байдлаар сонгов.

- **Чиглэлийн урт (**MAX_ROUTE_KM) - 18.0км
- **Чиглэл дэх хамгийн бага буудлын тоо (MIN_STOPS)** - 8
- **k-богино зам** (K_PATHS)-ын тоо - 3

Кандидат зам үүсгэх үйл явц нь нийтийн тээврийн чиглэлийн оновчлол болон зорчилтын загварчлалын үндсэн алхамуудын нэг юм [2]. Энэхүү шатанд эхлээд бодит ажиглалтаар илэрсэн зорчих эхлэл–төгсгөлийн (OD) хосуудыг тухайн бүсийн сонирхлын цэгүүдтэй хослуулан өргөтгөдөг. Үүний үр дүнд зорчилтын боломжит сүлжээ үүсэж, эдгээр хос бүрийн хувьд k–хамгийн богино зам тооцоологдоно. Ингэснээр зорчигчийн бодит хөдөлгөөний хэв маягийг илүү нарийн тусгасан олон хувилбарт замын багц бүрэлддэг. Гэвч үүссэн замуудын дунд төгсгөлийн цэг, урт, зогсоолын тоо ижил олон хувилбар давхцах эрсдэлтэй тул дараагийн алхамд (эхлэл ба төгсгөл цэг, замын урт, зогсоолын тоо) гэсэн гурван шинжээр давхардлыг арилгах шалгуур хэрэглэнэ. Ингэснээр үр дүн нь оновчтой, дахин давтагдахгүй, төлөөллийн чанартай кандидат замуудын цогц болж, цаашдын зорчилтын эрэлт таамаглал, тээврийн сүлжээний оновчлолын тооцоонд суурь өгөгдөл болдог.

Зогсоолын графын бүтцийн загварчлал нь нийтийн тээврийн сүлжээний холболтын үр ашиг, чиглэлийн уялдаа холбоог хадгалах чухал үндэс болдог. Энэ хүрээнд графын ирмэгүүдийг хоёр эх үүсвэрээс бүрдүүлдэг. Нэгдүгээрт, одоо байгаа тээврийн маршрутуудын дагуух зогсоол хоорондын шууд холбоосууд нь үндсэн ирмэгийг бүрдүүлж, бодит үйлчилгээнд ашиглагдаж буй хөдөлгөөний чиглэл, дарааллыг тусган харуулна. Хоёрдугаарт, зогсоолуудын газарзүйн ойролцоо байрлалд тулгуурласан нэмэлт холболтуудыг үүсгэснээр маршрутын хоорондын тасралтгүй байдлыг хангаж, коридорын үргэлжлэл болон сүлжээний нягтралыг сайжруулдаг. Ийнхүү бүрэлдсэн зогсоолын граф нь зөвхөн бодит чиглэлийн бүтэц төдийгүй, боломжит солилцоо

болон хувилбарт замуудыг тооцох, тээврийн сүлжээний дэд бүтцийн оновчлолд ашиглахад тохиромжтой цогц өгөгдлийн загвар болж хувирдаг [5].

Үүссэн чиглэлүүдийн хөрш буудлуудад swap, replace, trim, extend үйлдлүүдээр симуляцчилсан батжуулалтын аргыг хэрэгжүүлсэн. Коридор байж болох чиглэлүүдээр эхлэл болгож 2.5-4 мянган алхамаар давтаж өндөр нийлмэл оноотой чиглэлүүдийг гаргасан. Чиглэлүүдийг сонгож авсны дараа автобусны зорчигчийн багтаамж болон автобус хоорондын зайг тохируулсан.

Манай судалгаанд эхлээд эрэлт хамгийн өндөртэй эхлэл–зорилго (OD) матрицын хосуудыг сонгож, тус бүрт нь хамгийн богино буюу 3 хүртэлх энгийн замуудыг үүсгэн авсан; үүнд маршрут бүрийн уртыг 100 км–ээс хэтрүүлэхгүй ($l \leq 100$ km) ба бүр дор хаяж 8 зогсоолтой байх ($s \geq 8$) гэсэн техникийн хязгаарлалыг тавьсан. Замын багцыг баталгаажуулсны дараа коридорын ач холбогдлын дагуу автобус хоорондын зайг жишигчилж (жишээ нь 10/12/15 мин) оноож, тойрох цагийг маршрут дээрх сууж явсан хугацаа болон завсарлагын нийлбэрээр ойролцоогоор тооцно. Тухайн маршрутад шаардагдах автобусны тоог ойролцоогоор (3) томъёогоор тооцно.

$$buse\_per\_route \approx \frac{cycle\_time}{headway} \quad (3)$$

Дараа нь оргил цагийн автобусны тоог багасгах асуудлыг зогсоолын хамрагдалтыг тодорхой зорилтод хүрч буй (жишээ нь ≥98% зогсоол) нөхцлийг хадгалан минимиалчлах хүснэгтэнд хувирган шийднэ; шаардлагатай тохиолдолд маргинал ашиг тус хамгийн бага маршрутуудыг (lowest-marginal-benefit) хасаж флотын дээд хязгаарт нийцүүлэх (жишээ: ≤550 оргил цагийн автобус) тулд хөрвүүлэх стратегийг ашиглаж болно. Мөн нэмэлтээр фийдэр (feeder)-үүдийг автобусны багтаамжийн нөлөөг бага байлгахаар хамрагдаагүй хэсгийг багасгахаар нэмсэн. Энэ хүрээнд санал болгож буй арга зүй нь OD-д суурилсан боломжит зам үүсгэхээс эхлээд сүлжээний үйл ажиллагааны төлөвлөлт, автобусны багтаамжийн оновчлол хүртэл цогц, практик хэрэгжих боломжтой шийдэл болж байна.

Энэхүү судалгаанд эрэлт хамгийн их бүртгэсэн эхлэл–зорилгын (OD) хосуудыг эхний шатанд сонгон тус бүрт нь хамгийн богино буюу хамгийн ихдээ гурван энгийн замыг үүсгэв; замын генерацийн явцад маршрут бүрийн уртыг 100 км–ээс давуулахгүй (l≤100 kml \le 100\ \text{km}l≤100 km) ба тухайн маршрут дор хаяж найман буудалтай байх (s≥8s \ge 8s≥8) техникийн хязгаарлалтыг мөрдөнө. Ийнхүү тодорхой хязгаарлагдмал, боловч бодит хөдөлгөөний онцлогийг хангахуйц кандидат замын багц бүрдүүлснээр цаашид коридорын ач холбогдлын дагуу толгой зай оноох, цикл цаг болон шаардлагатай автобусны тоог тооцох, хамралт ба флотын хязгаарт нийцүүлэх мэт тээврийн сүлжээний оновчлолын үе шатуудад ашиглах бат бөх, давтагдашгүй суурь өгөгдлийг бүрдүүлнэ [2].

6. Оновчлолын арга

$$\begin{aligned}\mathrm{Score}(\mathcal{R}) = {} & \underbrace{w_{\text{demand}} \cdot \sum_{(u,v)} \frac{D(u,v)}{1 + 0.3 \cdot \mathrm{dist}_{\mathcal{R}}(u,v)}}_{\text{Serve observed + latent OD with short in-vehicle distance}} + \underbrace{w_{\text{coverage}} \cdot |\mathrm{UniqueStops}(\mathcal{R})|}_{\text{Geographic coverage}} \\ & + \underbrace{w_{\text{transfer}} \cdot \sum_{(u,v)} \mathrm{penalty}(\mathrm{transfers}_{\mathcal{R}}(u,v))}_{\text{Fewer transfers preferred}} + \underbrace{w_{\text{length}} \cdot \sum_{r \in \mathcal{R}} \mathrm{len}_{\mathrm{km}}(r)}_{\text{Discourage overlong routes}} \\ & + \underbrace{w_{\text{overlap}} \cdot \sum_{e} \max(0, \mathrm{uses}(e) - 1)}_{\text{Penalize corridor overlap}}.\end{aligned} \quad (4)$$

Энд,

- $w_{demand} = 1.0$ (богино зайд их зорчилттой байвал шагналтай)
- $w_{coverage} = 0.2$ (ялгаатай буудал хамруулбал шагналтай)
- $w_{transfer} = -0.3$ (дамжин суувал шийтгэлтэй)
- w_{length} = -0.00 (урт чиглэлийг шийтгэх коэффициент, уртад хязгаар тавьсан тул энэ утгыг тэгтэй ойрхон авав)
- $w_{overlap} = -0.05$ (Олон чиглэлд орсон холбоосуудыг шийтгэх коэффициент)

Чиглэлийн урт нь холбоос бүрийн уртын нийлбэрээр тодорхойлогдох буюу хэрэв хоёр автобусны буудал нь нэг чиглэлийнх биш байвал нэг удаа дамжин суухыг зөвшөөрч хоёр чиглэлийн холболтыг хийнэ. Бусад тохиолдолд OD-ийг хамрагдаагүй гэж үзнэ.

Оновчлолын үнэлгээний функцэд дараах шалгуурыг хангасан байхаар тодорхойлсон. Үүнд:

- Эрэлт нийлүүлэлт: Өндөр эрэлттэй OD хосуудыг холбосон тохиолдолд илүү оноо өгөх;
- Буудлын хамрах хүрээ давтагдахгүй;
- Хэт олон дамжлагагүй, хэт урт буюу 100 км-ээс их маршрутгүй байх, болон

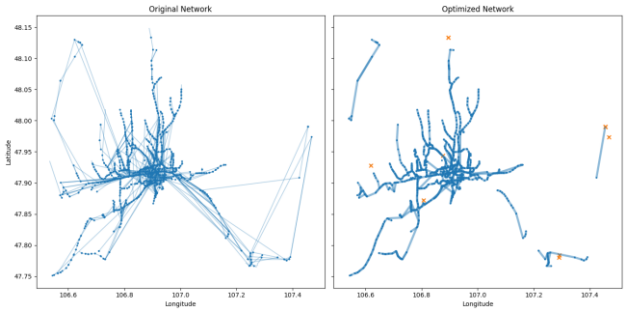
коридорын давхцлын төлбөрийг тооцохгүй.

Дараах нөхцөлийг хангасан ялгаатай жин бүхий хэд хэдэн хувилбарыг туршсан:

- Эрэлт төвтэй байх;
- Хамрах хүрээ төвтэй байх;
- Дамжлага мэдрэмтгий байх;
- Богино маршруттай байх;
- Давхцал багатай хувилбарууд байх

IV. ТУРШИЛТЫН ҮР ДҮН

Суурь сүлжээ ба оновчлогдсон хувилбарыг харьцуулж, дараах ялгаатай байдлыг тогтоосон [3]. Одоогийн ашиглагдаж буй суурь сүлжээний хувьд олон маршрут хоорондоо давхцаж, эрэлтийн хамрах хүрээ тэнцвэргүй байна. Simulated Annealing (SA) аргачлалаар оновчлол хийхэд дараах үр дүн гарсан. Судалгааны үр дүнгээс харахад Маршрутын тоо 52%-иар буурсан боловч хамрах хүрээ 8.4 пунктээр өссөн. Флотын хэрэглээ 14%-иар буурч, хөдөлгөөний үр ашиг дээшилсэн. Давхардсан чиглэлүүдийн 30% багассан. Эрэлттэй коридорууд (баруун–зүүн, төвийн тэнхлэг) илүү нягт сүлжээгээр хангагдсан байна. Энэ нь сүлжээний бүтцийг дахин төлөвлөхөд AI суурьтай алгоритмууд (SA, RL) Монголын нөхцөлд үр дүнтэй ажиллах боломжтойг харуулж байна.



2-р зураг.

Эдгээр үр дүн нь зорилтот үзүүлэлтэд мэдэгдэхүйц өсөлт үзүүлсэн ч үйлчилгээ нь тодорхой гол коридорууд дээр төвлөрсөн байгааг харуулж байна. Энэ нь түгжрэл болон багтаамжийн дахин үнэлгээ хийх шаардлагатайг илтгэнэ.

Тайлбар: “0→217” гэсэн өөрчлөлт нь одоо ашиглагдаж буй нийтийн тээврийн суурь сүлжээний хамрах хүрээний тооцоололд алдаа гарсныг илтгэж байна. Жишээлбэл, ID–нэрийн зөрүү, өгөгдлийн төрөл таарахгүй, хоосон шүүлтүүр гэх мэт. Мөн 115 маршрутаас бүрдэх бодит сүлжээ 0 буудлыг хамрах боломжгүй юм.

Иймээс +21700% гэх мэт хэт өндөр хувийн өсөлт бус, бодит тоо ба нийт доторх эзлэх хувийг тайлагнах нь зүйтэй.

A. *Ажиглагдсан сайжруулалт*

Өндөр эрэлттэй коридоруудтай холбогдсон буудлын эзлэх хувь нэмэгдсэнээр хамрах хүрээ өргөжсөн. Маршрутын тойруу хэсгүүдийг хасаж, холболтын чанарыг алдалгүйгээр нийт уртыг богиносгосноор үр дүнтэй болсон. Сургууль, эмнэлэг, зах зэрэг эрэлт ихтэй POI кластеруудад үйлчилгээ илүү сайжирсан.

Тохиргооны хувилбарууд дараах ялгаатай байлаа. Үүнд:

- Хамрах хүрээ төвтэй хувилбаруудад нийт буудлын тоог нэмэгдүүлсэн.
- Дамжлагад мэдрэмтгий хувилбаруудад дамжлагын тоог бууруулсанаар хамрах хүрээ бага зэрэг буурсан.

B. *Харагдац ба дүрслэл*

Python-ы Folium санг ашиглан харилцан уялдаатай газрын зураг боловсруулав.

- Анхны маршрутуудыг цэнхэр тасархай шугамаар,
- Оновчлогдсон маршрутуудыг улаан бүтэн шугамаар дүрслэв.

Харьцуулсан үр дүнгээс харахад оновчлогдсон маршрутууд нь зорчигчдын гол урсгалтай илүү нийцэж, POI кластерийн төвүүдтэй илүү үр ашигтай холболт үүсгэсэн байна.

Энэхүү туршилтаар зорчигчдын урсгал болон сонирхлын цэг (POI кластер)-ийн өгөгдлийг Улаанбаатар хотын нийтийн тээврийн сүлжээний төлөвлөлтөд нэгтгэн ашиглах боломжтойг харууллаа. Оновчлолын үнэлгээний системд суурилсан энэхүү хүрээ нь төлөвлөгчдөд олон хувилбарыг симуляц хийх, мөн эрэлт, хамрах хүрээ, үр ашгийн хоорондын тэнцвэрийг судлан тохируулах боломжийг олгодогоороо ач холбогдолтой.

Гэсэн хэдий ч дараах **хязгаарлалтууд** байсаар байна:

- **Газар зүйн сүлжээний загварчлал** нь авто замын нарийвчилсан бүтэц, чиглэл, хөдөлгөөний хязгаарлалтыг тусгаагүй, зөвхөн ойролцоо байдлаар тооцогдсон.
- **Үйл ажиллагааны хүчин зүйлүүдэд** жолоочийн болон автобусны тоо, буудлын ба агуулахын байршил, цагийн хуваарь гэх мэтийг оновчлолд оруулаагүй.
- **Эрэлтийн загвар** нь өдрийн цагийн хэлбэлзэл буюу оргил болон сул үеийн динамикийг тооцохгүй байх хялбаршуулсан.

Эдгээр хязгаарлалтыг цаашид шийдвэрлэснээр бодит хэрэглээнд нийцсэн, илүү нарийвчилсан

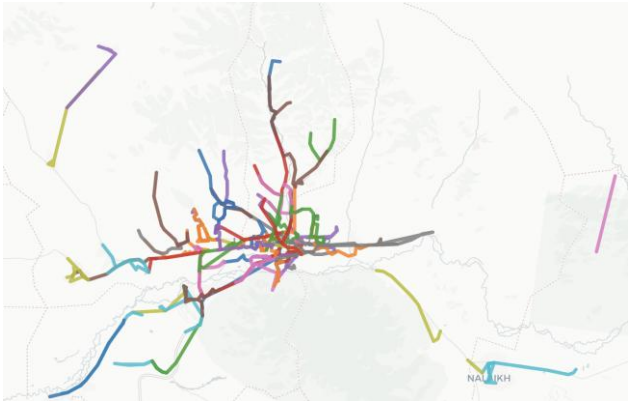
маршрут оновчлолын системийг хөгжүүлэх боломжтой.

Түлхүүр үзүүлэлтийн индекс (KPI)-ийг дараах хувьсагчдаар тооцов. Үүнд:

- Хамрагдалт: Давтагдахгүй автобусны буудал, нийт автобусны буудал хоёрын харьцаа.
- Үйлчилсэн зорчилт: OD болон зайгаар жигнэсэн.
- Давхцал: Олон чиглэлд орсон холбоос.
- Дамжин суулт: Дамжаагүй болон 1 удаа дамжсан тооны харьцаа.
- Автобусны багтаамж: оргил цагийн автобусны тоо.
- Автобус/чиглэлийн тархалт: тэнцвэртэй эсэхийг баталгаажуулахад.

2-Р ХҮСНЭГТ. ТУРШИЛТЫН ӨГӨГДЛҮҮД

Хэмжигдэхүүн	**Анхны сүлжээ**	**Оновчилсон сүлжээ**	**Өөрчлөлт**
Нийт чиглэл	142	68	↓ 52.1% цөөн
Нийт автобусны буудал	1,112	1,094 (чиглэлд орсон)	98.4% хамрагдалт (+8.3%)
Шаардагдах автобусны тоо	3,800	2,763	↓ 27.3% цөөн
Нийт автобусны тоо (нөөц ороод)	4,400	3,232	↓ 26.5% цөөн
Нэг чиглэлд ногдох автобусны тоо	27.7	24.03	↓ 13.2% сайжирсан
Чиглэлийн давхацсан холбоосын тоо	~930	471	↓ 49.4% цөөн
Автобус хоорондын дундаж зай	10–20 мин	10–15 мин	Тогмол байдал нь сайжирсан
Иргэдийн хамрагдалт	~90.0%	~98.4%	↑ 8.4% өссөн



3-р зураг. 100x100 харьцаатай OD матрицын дулааны зураглал

Дээрх дурдсан хязгаарлалтуудыг GTFS өгөгдлийн урсгал, OpenStreetMap-ийн авто замын сүлжээ, мөн динамик оновчлолд зориулсан reinforcement learning (бэхжүүлэх сургалт)-ийг нэгтгэн ашигласнаар шийдвэрлэх боломжтой. Ингэснээр Улаанбаатар хотын нийтийн тээврийн маршрут төлөвлөлт нь бодит цагийн өгөгдөлд тулгуурласан илүү уян хатан, ухаалаг, тухайн нөхцөлд дасан зохицох чадвартай болно.

ДҮГНЭЛТ

Энэхүү судалгаанд бид хотын түвшний автобусны сүлжээг Coverage-Forward зарчмаар оновчлох аргыг санал болгож, буудал-геометр дээр суурилсан нэр дэвшигч үүсгэх, хамрах хүрээг илүүчлэх SA + coverage-repair оновчлолын гогцоотойгоор хэрэгжүүллээ. Визуалчлал болон үнэлгээний хэрэгсэлтэй хослуулснаар “оптимизац → зураглал → хэмжүүр”-ийн бүрэн шугамыг байгуулсан. Туршилтын үр дүн нь хүртээмж ба холболтын чанар өндөр түвшинд хүрснийг харууллаа: нийт зогсоолын 98.56% нь шууд үйлчилгээнд хамрагдаж, дундаж алхалтын зай 151 м байна. Ажиглагдсан OD эрэлтийн 99.41% нь сүлжээгээр хүрч болох бөгөөд тэг солилцоо-той зорчилтын эзлэх хувь 88.33%, ≤1 солилцоо-той зорчилт 96.50%, зорчигч тутмын дундаж солилцоо 0.082 байв. Сүлжээний давхцлын хувь 30.7% нь холболтыг хангахын зэрэгцээ илүүдэл давхцалд оруулгүй батлав.

Гэсэн хэдий ч геометрийн шуудрал сул: дундаж circuity = 4.46 (ойролцоо шулуун замын харьцаагаар өндөр) нь зарим чиглэл тойрч, “үсрэлт-эргэлт” ихтэйг илтгэнэ. Мөн coverage_drop_pct = 32.46% гэсэн үзүүлэлт сууль сүлжээнээс алдагдсан хамрах хүрээг заадаг бол

энэ нь бодлогын хувьд үл зөвшөөрөгдөх түвшин тул суурийн хамгаалалт ба босгыг идэвхжүүлэх шаардлагатай.

Цаашдын ажил: Дүүрэг хоорондын тэгш хүртээмж, зорчих хугацааны генерализсан үзүүлэлтээр (run+wait+transfer) A/B харьцуулалт хийх.

Дүгнэж хэлбэл, санал болгосон хүрээ нь хүртээмж ба холболтыг мэдэгдэхүйц сайжруулсан ч шуудрал ба суурь хамгаалалтын талаарх сайжруулалтыг дараагийн давталтад хэрэгжүүлэх ёстой. Ийнхүү бодит цагийн өгөгдөл, бодлогын хяналт, шударга байдлын шалгалттай уялдуулснаар Улаанбаатар хотын нийтийн тээврийн сүлжээний бодит хэрэгцээнд нийцсэн, найдвартай оновчлолын шийдэлд хүрнэ.

Өгөгдөлд суурилсан оновчлол нь Улаанбаатар зэрэг хотуудын нийтийн тээврийн сүлжээг сайжруулах хүчирхэг арга хэрэгсэл юм. Бидний санал болгож буй загвар нь одоо ашиглагдаж буй Улаанбаатар хотын нийтийн тээврийн сүлжээг бодвол хамрах хүрээ, эрэлтийн хангалт, холболтын чанар зэргийг сайжруулсан оновчлогдсон маршрутын багцыг гаргасанаараа нэвтрүүлэхэд бүрэн боломжтой.

Бидний санал болгож буй загвар нь уян хатан, өргөтгөх боломжтойгоос гадна ирээдүйд үйл ажиллагааны (ажиллагааны хүчин чадал, хуваарь) болон цаг хугацааны (өдрийн динамик, оргил ачааллын үе) хүчин зүйлсийг нэгтгэн оруулсанаараа давуу талтай.

Ингэснээр судалгаанд суурилсан шийдвэр гаргалтыг дэмжиж, түгжрэлгүй хотын хөдөлгөөний төлөвлөлт”-ийг шинжлэх ухаанд тулгуурлан хэрэгжүүлэхэд хувь нэмэр оруулна.

НОМ ЗҮЙ

[1] Saleh Basalamah, SultanDaud Khan, Emad Felemban, Atif Naseer, Faizan Ur Rehman. (2023). Deep learning framework for congestion detection at public places via learning from synthetic data., https://www.sciencedirect.com/science/article/pii/S1319157822004037;

[2] Kaniz Fatima. (2024). Modal congestion management strategies and the influence on operating characteristics of urban corridor., School of Civil Environmental and Chemical Engineering College of Science Engineering and Health RMIT University;

[3] Biru Rajak, Aprna Tripathi & Dharmender Singh Kushwaha. (2020). A Realtime Road Congestion-Based Hybrid Approach for Finding the Optimized Route., Proceedings of the Fourth International Conference on Microelectronics, Computing and Communication Systems., pp.83-97., DOI:10.1007/978-981-15-5546-6_8;

[4] Pranamesh Chakraborty, Yaw Okyere Adu-Gyamfi. (2018). Traffic Congestion Detection from Camera Images using Deep Convolution Neural Networks”., Sage Journals., Volume 2672, Issue 45., https://doi.org/10.1177/03611981187776., https://journals.sagepub.com/doi/abs/10.1177/0361198118777631#con1;

[5] Rubens Cruz Gatto, Carlos Henrique Quartucci Forster. (2021). Audio-based Machine Learning Model for Traffic Congestion Detection., IEEE Transactions on Intelligent Transportation Systems. pp(99):1-8., DOI:10.1109/TITS.2020.3003111

[6] A. Ata, M.A. Khan†, S. Abbas G. Ahmad A. Fatima. (2019). Modelling smart road traffic congestion control system using machine learning techniques., Neural Network World 2019(2):99., DOI:10.14311/NNW.2019.29.008

[7] Amr Elfar, Alireza Talebpour, and Hani S. Mahmassani. (2018). Detection Traffic Congestion Based on Twitter Data using Machine Learning., Sage Journals., Volume 2672, Issue 45., https://doi.org/10.1177/0361198118795010

ГҮН СУРГАЛТЫН АРГААР МАТЕРИАЛ АНГИЛАХ НЬ

Жамцын БОЛДСАЙХАН[1], Соном-Очирын ӨЛЗИЙБАЯР[2]

[1,2]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээлэл технологийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: boldoo3@gmail.com[1]

Хураангуй: **Сүүлийн жилүүдэд хиймэл оюун ухаанд суурилсан дүрс боловсруулалт, гүн сургалтын технологи хурдацтай хөгжиж, үйлдвэрлэл, инженерчлэл, шинжлэх ухаан, ахуйн хэрэглээнд нэвтрэн орж байна. Хүнээс ихээхэн хамааралтай, цаг хугацаа их шаарддаг процессуудыг автоматжуулах боломжийг гүн сургалт олгож буй нь онцгой ач холбогдолтой. Энэ судалгааны ажлын зорилго нь Монгол Улсын МАК цементийн үйлдвэрийн түүхий эд материалуудыг (15 төрөл) дүрсний боловсруулалт болон гүн сургалтын аргаар автоматаар ангилах системийг боловсруулахад оршино. Үүний тулд бид өөрийн бэлтгэсэн материалын зургийн өгөгдлийн санг ашиглан ResNet (34, 50, 101, 152) болон VGG (16, 19) архитектурын загваруудыг сургалт, туршилтанд ашиглаж, үр дүнг харьцуулсан. Нарийвчлалыг сайжруулахын тулд Data Augmentation, DTD (Describable Textures Dataset) дээр үндэслэсэн Fine-tuning, мөн Canny Edge Detection зэрэг аргуудыг туршсан. Үр дүнд ResNet152 + DTD + Data Augmentation стратеги хамгийн өндөр буюу 99.21% нарийвчлалд хүрч, гүн сургалтын аргаар материал ангилах асуудлыг үйлдвэрлэлийн орчинд хэрэгжүүлэх боломжтойг харуулсан.**

Түлхүүр үг: TensorFlow/Keras, Deep Learning, Texture Analysis, Data Augmentation, Fine-tuning, ResNet, VGG, Cement Industry Automation, Image Classification.

I. УДИРТГАЛ

Цементийн үйлдвэрлэлийн түүхий эдийн бэлтгэл, хяналтын үйл ажиллагаа нь бүтээгдэхүүний чанар, үйлдвэрлэлийн үр ашгийг тодорхойлох гол хүчин зүйлсийн нэг юм. МАК цементийн үйлдвэрт өдөр бүр шохойн чулуу, шавар, гөлтгөнө, элсэн чулуу, төмрийн хүдэр, үнс зэрэг олон төрлийн түүхий эд материалыг өөр өөр газраас тээвэрлэн авч үйлдвэрлэлийн шугамд нийлүүлдэг. Эдгээр материалуудын бүртгэл, жинлэлт, хүлээн авалт нь одоогоор бүрэн автомат биш бөгөөд хүний оролцоотой хийгддэг. Үүний улмаас бүртгэлийн алдаа гарах, хугацаа алдах, хүний хүчин зүйлээс хамааралтай эрсдэл үүсэх нөхцөл байсаар байна.

Хиймэл оюун ухаанд суурилсан систем, ялангуяа дүрсний боловсруулалт (Computer Vision) нь ийм төрлийн асуудлыг шийдвэрлэх хамгийн оновчтой шийдэл болж байна. Камерын системийн тусламжтайгаар автомашины ачсан материалын зургийг авч, түүнийг автоматаар ангилан таних системийг нэвтрүүлснээр бүртгэлийн үйл явц хялбаршиж, мэдээлэл илүү найдвартай, системийн гүйцэтгэл хурдан болох боломж бүрдэнэ.

Судалгааны зорилго, зорилтууд

Судалгааны гол зорилго нь цементийн үйлдвэрлэлд ашиглагддаг 15 төрлийн материалыг гүн сургалтын аргаар ангилж, хамгийн тохиромжтой архитектур, боловсруулалтын стратегийг тодорхойлох явдал юм.

Энэхүү зорилгыг биелүүлэхийн тулд дараах дэд зорилтуудыг дэвшүүлэв:

1. Материалын зургийн өгөгдлийн санг бүрдүүлэх, бүтэц, хэмжээг тодорхойлох.
2. ResNet болон VGG архитектурын гүн сургалтын загваруудыг ашиглан сургалт, туршилт хийх.
3. Data Augmentation ашиглан өгөгдлийн санг баяжуулж, overfitting-ийг бууруулах.
4. DTD өгөгдлийн санг ашиглан cross fine-tuning хийж, материалын гадаргуугийн текстурын онцлогийг илүү гүнзгий тодорхойлох.
5. Canny edge detection зэрэг preprocessing аргуудыг туршиж, үр дүнг харьцуулах.
6. Туршилтын үр дүн дээр үндэслэн хамгийн тохиромжтой архитектур ба сургалтын стратегийг санал болгох.

Энэхүү судалгаа нь онолын болон практик ач холбогдолтой юм. Онолын талаас, энэ ажил нь texture буюу гадаргуугийн онцлог шинж чанарыг илүү оновчтой тусгах гүн сургалтын аргуудыг ашиглаж, материал ангиллын нарийвчлалыг нэмэгдүүлэхэд хувь нэмэр оруулж байна. Практик талаасаа, цементийн үйлдвэрт бүртгэл, хяналтыг автоматжуулах замаар үйлдвэрлэлийн үр ашгийг нэмэгдүүлэх, хүний оролцоог багасгах, өгөгдлийн найдвартай байдлыг сайжруулах боломжийг нээж өгнө.

II. СУДЛАГДСАН БАЙДАЛ

Гүн сургалтын аргачлал, ялангуяа convolutional neural network (CNN)-д суурилсан загварууд нь сүүлийн арван жилд дүрсийн ангилал болон материал таних салбарт хамгийн өндөр үр дүн үзүүлж буй арга зүй юм. Олон судлаачид чулуу, эрдэс, барилгын материал, гадаргуугийн бүтэц зэрэг объектуудыг ангилах судалгаанд CNN архитектурыг өргөнөөр ашиглаж байна.

Surendra Patro нар [1] igneous чулууг CNN ашиглан ангилсан бөгөөд ResNet архитектурын давуу тал болох гүн давхаргын суралцах чадварыг харуулсан. Vincent Andrearczyk, Paul Whelan [2] нар texture ангилалд convolutional filter banks ашиглан CNN-ийн гүйцэтгэлийг сайжруулсан судалгаа хийсэн байдаг. Joan Bruna, Stephane Mallat [4] нар invariant scattering convolution networks ашиглан дүрсний гадаргуугийн

онцлогийг илүү нарийн түвшинд тодорхойлох аргачлал санал болгосон.

Li Liu нар [5] өнгөрсөн хорин жилд texture representation-ийн хөгжлийг BoW (Bag-of-Words) загвараас CNN-д шилжсэн үйл явцаар тодорхойлсон бол Sean Bell нар [12] MINC (Materials in Context Database) өгөгдлийн санг ашиглан бодит нөхцөл дэх материал ангиллын системийг боловсруулжээ. Bai L. нар [15] VGG загварт суурилсан rock thin section classification хийж, эрдэс чулуулгийн ангилалд гүн сургалт амжилттай болохыг баталсан. Мөн Weihao Chen нар [14] ResNet архитектурт transfer learning ашиглан чулуулгийн зургийн ангиллыг хийж, уламжлалт аргуудаас 15–20%-иар илүү үр дүн гаргасан байна.

Эдгээр судалгаанууд нь гүн сургалтын архитектурууд texture болон гадаргуугийн шинж чанарыг ялгахад маш үр дүнтэй болохыг нотолж байна. Гэвч эдгээр ажлуудын ихэнх нь лабораторийн нөхцөлд авсан цэвэр дүрс дээр хийгдсэн байдаг бол энэхүү судалгаа нь үйлдвэрлэлийн бодит орчны өгөгдөлд тулгуурласан гэдгээрээ онцлог юм. Мөн DTD өгөгдлийн санг ашиглан cross-domain fine-tuning хийх нь өмнөх судалгаануудаас ялгаатай, шинэ арга зүйн онцлогтой болж байна.

III. ӨГӨГДЛИЙН САН БА АРГА ЗҮЙ

3.1 Өгөгдлийн сан

Энэхүү судалгаанд ашиглагдсан өгөгдлийн сан нь хоёр үндсэн хэсгээс бүрдэнэ:

1. Үндсэн үйлдвэрийн материалын өгөгдлийн сан (Factory Dataset)
2. DTD (Describable Textures Dataset) нээлттэй өгөгдлийн сан

3.1.1 Үндсэн материалын өгөгдлийн сан

Өөрийн өгөгдлийн сан нь МАК цементийн үйлдвэрийн түүхий эд материалыг бодит орчинд суурилуулсан Р хэлбэрийн арктай камерийн системийн тусламжтайгаар цуглуулсан зургууд юм. Энэхүү өгөгдөл нь үйлдвэрлэлийн орчны гэрэлтэлт, өнгө, сүүдэр, тооcжилт, гадаргуугийн ялгаа зэрэг бодит нөхцөлд авсан бөгөөд автомат таних системд тохирохуйц өгөгдлийг бий болгосон.

- ***Материалын төрөл:*** 15 (azurite, baryte, beryl, calcite, cerussite, copper, fluorite, gypsum, hematite, malachite, pyrite, pyromorphite, quartz, smithsonite, wulfenite)
- ***Нийт зураг:*** 37,710 (640×640 пиксел хэмжээтэй)
- ***Хуваалт:*** Training 70%, Validation 20%, Test 10%
- ***Зургийн төрөл:*** RGB өнгөт формат
- ***Бодит орчны нөхцөл:*** гэрэлтэлт, сүүдэр, өнгөний ялгаа, материалын барзгар байдал зэрэг хүчин зүйлс тусгасан.

Доорх хүснэгтэд үндсэн өгөгдлийн сангийн бүтэц болон Data Augmentation дараах байдлаар өгөгдсөн болно.

1 - Р ХҮСНЭГТ. ҮНДСЭН ӨГӨГДЛИЙН БАГЦЫН БҮТЭЦ

Төрөл	Нийт зураг	training	validation	test
azurite	1029	720	205	102
baryte	2211	1547	442	221
beryl	1615	1130	323	161
calcite	6574	4601	1314	657
cerussite	1367	956	273	136
copper	1429	1000	285	142
fluorite	5669	3968	1133	566
gypsum	1351	945	270	135
hematite	1284	898	256	128
malachite	1607	1124	321	160
pyrite	2339	1637	467	233
pyromorphite	1705	1193	341	170
quartz	6828	4779	1365	682
smithsonite	1188	831	237	118
wulfenite	1521	1064	304	152

Data Augmentation дараах байдлаар хийгдсэн:

640×640 хэмжээсийн зургуудыг дараах нэмэлт хэмжээнүүдтэйгээр туршсан:

- 320×320
- 160×160

Augmentation-ийн дараах өгөгдлийн тоо хэмжээ:

2-Р ХҮСНЭГТ. DATA AUGMENTATION ДАРААХ ӨГӨГДЛИЙН ХЭМЖЭЭ (640×640, 320×320, 160×160)

Төрөл	640×640	320×320	160×160
azurite	10290	2058	8232
baryte	22110	4422	17688
beryl	16150	3230	12920
calcite	65740	13148	52592
cerussite	13670	2734	10936
copper	14290	2858	11432
fluorite	56690	11338	45352
gypsum	13510	2702	10808
hematite	12840	2568	10272
malachite	16070	3214	12856
pyrite	23390	4678	18712
pyromorphite	17050	3410	13640
quartz	68280	13656	54624
smithsonite	11880	2376	9504
wulfenite	15210	3042	12168

Augmentation нь сургалтын өгөгдлийн төрөлжилтийг нэмэгдүүлж, overfitting-ийг бууруулсан бөгөөд загварын generalization сайжирсан. Баяжуулалт

хийгдсэн зургууд нь эргэлт, тусгал, таталт, гэрэлтэлт, өнгөний өөрчлөлт зэрэг олон янзын хувилбартайгаар үүссэн.

3.1.2 DTD (Describable Textures Dataset) нээлттэй өгөгдлийн сан

DTD өгөгдлийн сан нь Оксфордын Visual Geometry Group (VGG)-ийн боловсруулсан, гадаргуугийн шинж чанар болон texture ангилалд зориулагдсан нээлттэй өгөгдлийн сан юм. Энэ өгөгдлийн сан нь 47 төрлийн текстурын ангилал, 5640 зураг агуулдаг бөгөөд “striped”, “dotted”, “woven”, “rough”, “bumpy”, “fibrous” гэх мэт өдөр тутмын хэллэгт тохирох байдлаар тодорхойлогдсон гадаргуугийн төрлүүдийг багтаадаг. Зургууд нь өндөр ялгаралттай, өнгөт (RGB) форматтай бөгөөд texture-тэй холбоотой шинж чанаруудыг тод томруун илэрхийлдэг.

DTD нь материалын гадаргуугийн онцлогийг танихад хамгийн чухал болох хээ, барзгар байдал, гэрэлтэлтийн хэлбэлзэл, өнгөний ялгарал зэрэг хүчин зүйлсийг хамарсан тул энэхүү судалгаанд гүн сургалтын загваруудыг texture мэдээлэлд илүү мэдрэмтгий болгох зорилгоор ашиглагдсан.

Судалгаанд DTD өгөгдлийн санг дараах байдлаар ашигласан:

1. **Pre-training:** DTD өгөгдлийн сан дээр ResNet152 архитектурыг урьдчилан сургаж, texture мэдээлэлд мэдрэмтгий болгосон.
2. **Fine-tuning:** Дараа нь өөрийн үйлдвэрийн материалын өгөгдлийн сан дээр fine-tune хийж, DTD дээр сурсан texture representation-ийг материалын ангилалд ашигласан.

Энэхүү cross-domain transfer learning стратеги нь DTD өгөгдлийн сангийн давуу талыг бүрэн ашиглаж, texture-тэй холбоотой мэдээлэлд гүн сургалтын архитектуруудын гүйцэтгэлийг үлэмж сайжруулсан.

3.1.3 Өгөгдлийн сангуудыг нэгтгэн ашигласан стратеги

Судалгаанд DTD ба үйлдвэрийн өгөгдлийн санг дараах дарааллаар нэгтгэн ашигласан:

1. DTD өгөгдлийн сан дээр урьдчилсан сургалт (***pre-training***) хийсэн;
2. Өөрийн үйлдвэрийн материалын өгөгдөл дээр ***fine-tuning*** гүйцэтгэсэн;
3. ***Data augmentation*** ашиглан сургалтын өгөгдлийг олон хувилбартай болгосон.

Энэ аргаар хоёр өөр эх үүсвэрийн өгөгдлийг уялдуулан ашигласнаар загварын feature extraction, generalization болон texture sensitivity чадварууд эрс нэмэгдсэн.

Судалгаанд ашигласан өгөгдлийн сан нь 15 ангилал бүхий 37,710 зураг (640×640 хэмжээтэй)-ээс бүрдэнэ. Энэ өгөгдлийн санг сургалтын (70%), баталгаажуулалтын (20%), туршилтын (10%) хэсгүүдэд хуваасан. Материал тус бүрийн зургуудын тоо харилцан адилгүй бөгөөд calcite, quartz зэрэг төрлүүд илүү олон зурагтай, харин hematite, smithsonite зэрэг төрөл бага хэмжээний зурагтай байсан. Энэ нь өгөгдлийн тэнцвэргүй байдлыг үүсгэж болзошгүй тул Data Augmentation ашиглан зохицуулсан.

Data Augmentation нь сургалтын өгөгдлийг хиймлээр баяжуулах зорилготой бөгөөд дараах аргуудыг хэрэглэсэн:

- Rotation: 10°–40° хооронд эргүүлэх.
- Horizontal болон Vertical flipping.
- Random zoom (±15–20%).
- Brightness, contrast тохируулга.
- Gaussian noise нэмэх.

Баяжуулалтын дараа нийт өгөгдлийн хэмжээ 377,105 зураг болсон бөгөөд ингэснээр сургалтын загвар илүү олон төрлийн өгөгдөл дээр суралцаж, ерөнхийлөх чадвар нэмэгдсэн.

3.2 Ашигласан архитектуруудын тайлбар

ResNet (Residual Network):ResNet нь 2015 онд Microsoft Research-ийн багийн боловсруулсан архитектур бөгөөд гүн сүлжээний сургалтанд үүсдэг градиент алдагдах (vanishing gradient) асуудлыг шийдвэрлэдэг. Энэ нь skip connection буюу residual learning-ийн зарчмаар ажилладаг. Ингэснээр мэдээлэл зарим давхаргыг алгасч, илүү тогтвортой сургалт явагддаг. Судалгаанд ResNet34, ResNet50, ResNet101, ResNet152 загваруудыг туршсан бөгөөд илүү гүн давхаргатай загварууд илүү сайн нарийвчлал үзүүлсэн.

VGG (Visual Geometry Group):VGG нь Оксфордын их сургуулийн боловсруулсан архитектур бөгөөд 3×3 convolution filter ашиглаж, энгийн бүтэцтэй хэдий ч хүчирхэг гүйцэтгэлтэй. Судалгаанд VGG16 болон VGG19 загваруудыг ашигласан бөгөөд VGG19 илүү олон давхаргатай тул илүү гүн сургалтад тохиромжтой байв.

DTD Cross Fine-tuning: DTD (Describable Textures Dataset) нь 47 ангилал бүхий 5640 зургийг агуулдаг бөгөөд гадаргуугийн бүтэц, өнгө, хээ зэрэг texture шинж чанарыг тодорхойлоход зориулагдсан. DTD дээр урьдчилсан сургалт хийж, texture мэдээллийг илүү сайн тусгасан загварыг өөрийн өгөгдөлд fine-tune хийх нь cross-domain transfer learning-ийн жишээ юм.

Canny Edge Detection: Canny edge илрүүлэлт нь дүрсний ирмэгийг тодруулах preprocessing арга боловч энэхүү судалгаанд texture болон өнгөний мэдээлэл илүү чухал байсан тул энэ арга хангалттай сайжруулалт үзүүлээгүй.

3.3 Туршилтын орчин ба параметрүүд

Туршилтыг Google Colab Pro орчинд TensorFlow/Keras, OpenCV, NumPy, Matplotlib зэрэг

сан ашиглан гүйцэтгэсэн. GPU нь NVIDIA Tesla T4 байсан

3-Р ХҮСНЭГТ. ТУРШИЛТЫН ОРЧИН ГИПЕР ПАРАМЕТР

Параметр	Утга
Batch size	32
Learning rate	0.0001
Optimizer	Adam
Loss function	Categorical Crossentropy
Epochs	50

IV. ТУРШИЛТЫН ҮР ДҮН БА ХЭЛЭЛЦҮҮЛЭГ

Өмнөх бүлэгт дурдсаны дагуу туршилтуудыг гүйцэтгэж үр дүнг дараах Хүснэгт 4, 5 болон 6-д тус тус үзүүллээ. Харьцуулалтаас харахад зургийн хэмжээ 640×640 байхад хамгийн өндөр нарийвчлал гарч, хэмжээ багасах тусам ангиллын алдаа нэмэгдсэн байна. Энэ нь материалын texture буюу гадаргуугийн нарийн мэдээлэл жижиг зурганд алдагдаж байгаатай холбоотой.

4-Р ХҮСНЭГТ. ШУУД СУРГАЛТЫН ҮР ДҮН (ӨГӨГДЛИЙН ХЭМЖЭЭНИЙ ӨӨРЧЛӨЛТӨД ХАРГАЛЗАХ ЗАГВАРЫН НАРИЙВЧЛАЛЫН ҮЗҮҮЛЭЛТҮҮД)

Загвар	640×640	320×320	160×160
ResNet34	0.83	0.75	0.34
ResNet50	0.85	0.7	0.66
ResNet101	0.8	0.6	0.51
ResNet152	0.82	0.66	0.55
VGG16	0.85	0.7	0.57
VGG19	0.86	0.71	0.68

4.2 Data Augmentation ба Image Slicing-ийн үр нөлөө

Өгөгдлийг 640×640, 320×320, 160×160 хэмжээгээр туршсан. 640×640 хэмжээний зургууд хамгийн сайн үр дүн өгсөн бол 160×160 хэмжээний зургууд нарийвчлал бууруулсан. Data augmentation нь сургалтын өгөгдлийн төрөлжилтийг нэмэгдүүлж, overfitting бууруулсан нь validation loss-ийн багасалтаар харагдсан.

5-Р ХҮСНЭГТ. CANNY EDGE DETECTION ҮР ДҮН (ИРМЭГ ИЛРҮҮЛЭЛТ АШИГЛАСАН ТУРШИЛТЫН ҮР ДҮН)

Загвар	640×640	320×320
ResNet152	0.55	0.31
VGG19	0.63	0.35

Canny Edge илрүүлэлт ашигласан туршилтад нарийвчлал 20–30%-иар буурсан. Энэ нь тухайн өгөгдлийн хувьд өнгө ба гадаргуугийн мэдээлэл илүү чухал байсныг харуулж байна.

DTD-ийн texture representation нь ResNet152 загвартай хослон хамгийн өндөр гүйцэтгэл үзүүлсэн. Энэ стратеги нь cross-domain transfer learning-ийн бодит үр ашгийг нотолж байна.

6-Р ХҮСНЭГТ. DTD FINE-TUNING БА DATA AUGMENTATION ХОСОЛСОН ҮР ДҮН (DTD ӨГӨГДЛИЙН САН ДЭЭР УРЬДЧИЛСАН СУРГАЛТ БА AUGMENTATION СТРАТЕГИЙН ХАРЬЦУУЛАЛТ)

Туршилт	Загвар	Нарийвчлал (%)
DTD Fine-tune	ResNet152	98.9
DTD Fine-tune	VGG19	83.4
DTD + Data Augmentation	ResNet152	***99.21***
DTD + Data Augmentation	VGG19	88.9

Алдааны анализ (Error Analysis):

DTD өгөгдлийн сан дээр урьдчилсан сургалт хийсний дараах fine-tuning болон өгөгдлийн augmentation-ийн хосолсон стратегийн үр дүнг харьцуулахад нийт ангиллын 99.21%-ийн нарийвчлалд хүрсэн. Үлдсэн 0.79%-ийн алдаа нь ихэвчлэн бие биетэйгээ төстэй өнгө, хээ, бүтэцтэй ангиллуудаас шалтгаалж байсан.

Тухайлбал, fluorite ба quartz, мөн azurite ба malachite зэрэг материалуудын өнгөний спектр болон гадаргуугийн хээ төстэй тул CNN-ийн feature map-д ялгарах онцлог шинжүүд бүрэн ялгагдаагүй. Энэ нь texture төвтэй сургалтын давуу талыг батлахын зэрэгцээ, өнгөний мэдээлэлд хэт тулгуурласан feature extraction зарим тохиолдолд төөрөгдөл үүсгэж байгааг харуулж байна.

Нөгөө талаар, DTD дээр хийсэн урьдчилсан сургалт нь edge болон fine-grain pattern-ийг илүү сайн ялгаж байсан ч материалын гэрэлтэлтийн өөрчлөлт, сүүдрийн хэлбэлзэлд мэдрэг байсныг confusion matrix-ийн үр дүн харуулсан. Энэ нь үйлдвэрлэлийн орчинд гэрэлтэлтийн нөхцөл тогтмол биш үед нарийвчлал бага зэрэг буурах шалтгаан болсон.

Findings ба товч дүгнэлт

1. DTD Fine-tuning стратеги нь texture шинж чанарыг онцлон суралцуулах замаар материалын ангилалд илүү үр дүнтэй байгааг баталсан.
2. Data Augmentation нь сургалтын өгөгдлийн төрөлжилтийг нэмэгдүүлж, overfitting-ийг бууруулан нийт нарийвчлалыг ~1% орчим нэмэгдүүлсэн.
3. ResNet152 архитектур нь VGG загваруудаас илүү сайн generalization үзүүлж, DTD-тэй fine-tune хийхэд хамгийн тогтвортой гүйцэтгэлтэй байв.
4. Error case-уудын дийлэнх нь өнгө ба texture төстэй ангиллуудад төвлөрсөн байсан тул ирээдүйд multi-modal feature fusion (өнгө + texture + орон зайн хээний хослол) аргуудыг судлах шаардлагатай.

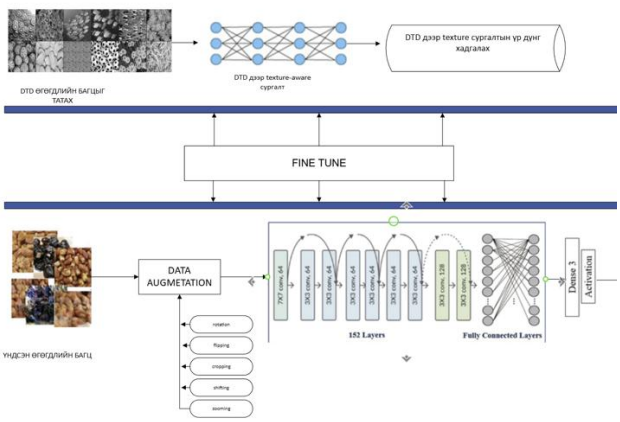
5. Үр дүнгээр, DTD болон өөрийн өгөгдлийн санг хослуулсан стратеги нь материал ангиллын салбарт cross-domain transfer learning-ийн үр ашигтай хэрэглээг нотолж байна.

Санал болгож буй архитектурын загвар:

Судалгаанд санал болгосон архитектур дараах үндсэн үе шаттай:

1. Texture Extraction: DTD өгөгдлийн сан дээр урьдчилсан сургалт хийж, texture feature-уудыг ялгана.
2. Feature Transfer & Fine-tuning: DTD дээр суралцсан мэдлэгийг материалын өгөгдөлд шилжүүлж, fine-tune хийж тохируулна.
3. Data Augmentation: Өгөгдлийг баяжуулж, generalization чадварыг сайжруулна.
4. Classification Layer: Fully connected layer дээр softmax classifier ашиглан ангиллыг хийнэ.

Энэхүү архитектур нь texture ба өнгөний шинж чанарыг нэгтгэн авч үзсэн тул илүү нарийвчлалтай үр дүн өгсөн.



1– р зураг. Санал болгож буй аргын бүдүүвч

V. ДҮГНЭЛТ БА ЦААШДЫН АЖИЛ

Энэхүү судалгаагаар цементийн үйлдвэрлэлийн материал ангиллыг гүн сургалтын аргаар автоматжуулах боломжтойг нотоллоо. Судалгаанд ашигласан ***ResNet152 + DTD + Data Augmentation стратеги*** хамгийн өндөр нарийвчлалтай гарч, үйлдвэрлэлийн орчны хэрэглээнд шууд нэвтрүүлэхэд тохиромжтойг баталсан. Мөн түүнчлэн:

- Зургийн өндөр нарийвчлал ангиллын үр дүнг сайжруулдаг.
- DTD өгөгдлийн сан ашиглах нь texture мэдээллийг илүү сайн тусгаж өгдөг.
- Data augmentation нь overfitting-ийг бууруулах үр дүнтэй арга.
- Canny edge preprocessing нь энэхүү өгөгдлийн хувьд тохиромжгүй.
- ResNet152 архитектур хамгийн сайн гүйцэтгэлтэй байсан.

Цаашид энэхүү системийг үйлдвэрийн бодит орчинд туршиж, бодит камерийн өгөгдлийг ашиглан реаль цагийн боловсруулалт хийх, материалын эзэлхүүн ба хэмжээ тооцоолох нэмэлт модулиудтай холбох нь судалгааны дараагийн чиглэл байх болно.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Igneous rock classification using Convolutional neural networks (CNN) June 2022IOP Conference Series Earth and Environmental Science 1032(1):012045 Surendra Patro, Dalchand Jhariya National Institute of Technology Raipur Mridu Sahu,Pankaj Dewangan

[2] Vincent Andrearczyk and Paul F. Whelan. Using filter banks in convolutional neural networks for texture classification. Pattern Recognit. LETT, 84:63–69, 2016. 1, 2, 3

[3] Hicham Badri, Hussein Yahia, and Khalid Daoudi. Fast and accurate texture recognition with multilayer convolution and

[4] Joan Bruna and Stephane Mallat. Invariant scattering con- ´ volution networks. IEEE Trans. Pattern Anal. Mach. Intell, 35:1872–1886, 08 2013. 2, 3

[5] Li Liu, Jie Chen, Paul Fieguth, Guoying Zhao, Rama Chellappa, and Matti Pietikainen. From bow to cnn: Two decades ¨ of texture representation for texture classification.

[6] Barbara Caputo, Eric Hayman, and P. Mallikarjuna. Classspecific material categorisation. In Proc. ICCV, volume 2, pages 1597 – 1604 Vol. 2, 2005. 1, 3, 6

[7] Zhenhua Guo, Lei Zhang, and David Zhang. A completed modeling of local binary pattern operator for texture classification. IEEE Trans. Image Process., 19(6):1657–1663, 2010. 3

[8] Thomas Leung and Jitendra Malik. Representing and recognizing the visual appearance of materials using threedimensional textons. Int. J. Comput. Vision, 43:29–44, 06 2001. 3

[9] Manik Varma and Rahul Garg. Locally invariant fractal features for statistical texture classification. In Proc. ICCV, 2007. 2, 3

[10] Ali, S. B., Wate, R., Kujur, S., Singh, A., and Kumar, S. (2020). "Wall crack detection using transfer learning-based cnn models," in 2020 IEEE 17th India Council International Conference (INDICON) (IEEE), 1–7.

[11] Xingyuan Bu, Yuwei Wu, Zhi Gao, and Yunde Jia. Deep convolutional network with locality and sparsity constraints for texture classification. Pattern Recognit.

[12] Sean Bell, Paul Upchurch, Noah Snavely, and Kavita Bala. Material recognition in the wild with the materials in context database. In Proc. CVPR, 2015. 1, 6

[13] multifractal analysis. In Proc. ECCV, pages 505–519. Springer International Publishing, 2014. 2, 3

[14] Rock image classification using deep residual neural network with transfer learning Weihao Chen Lumei Su, Lumei Su1,Xinqiang Chen Xinqiang HuangZhihao

[15] Bai, L., Wei, X., Liu, Y., Wu, C., and Chen, L. (2019). Rock thin section image recognition and classification based on vgg model. *Geol. Bull. China* 38, 2053–2058.

[16] Bai, L., Yao, Y., Li, S., Xu, D., and Wei, X. (2018). Mineral composition analysis of rock image based on deep learning feature extraction. *China Min. Mag.* 27, 178–182.

[17] Bai, L., Wei, X., Liu, Y., Wu, C., and Chen, L. (2019). Rock thin section image recognition and classification based on vgg model. *Geol. Bull. China* 38, 2053–2058.

COMPARATIVE ANALYSIS OF SQL INJECTION DETECTION MODELS

GEGENTANA[1], ENKHTUR Tsogbaatar[2] , ODONCHIMEG Lkhagva[3] , JUNXU Wei[4]

[1,2]Mongolia, Ulaanbaata, MUST, School of Information and Communication Technology, Department of Cybersecurity

Correspondence should be addressed to: J.SA23E005@must.edu.mn[1]

Abstract*: Structured Query Language injection (SQLi) remains one of the most persistent and damaging web security threats, enabling attackers to gain unauthorized access to sensitive databases. Given its continuing prevalence and far-reaching impact, this study conducts a comparative experiment to evaluate the performance trade-offs between the classical machine learning (ML) and deep learning (DL) approaches for SQL injection detection using a publicly available and standardized dataset. For ML models, feature representations combined character-level Term Frequency–Inverse Document Frequency (TF-IDF), word-level TF-IDF based on a custom SQL tokenizer, and numeric behavioral indicators. For DL models, a vocabulary was constructed from the training dataset, and pattern fragments prone to vocabulary explosion were replaced with placeholders to ensure stable embedding representations. A threefold analysis of feature importance (ablation, permutation importance, and coefficient analysis) consistently shows that word-level TF-IDF contributes the most to model performance. The Linear Support Vector Classifier (LinearSVC) achieved the best performance among the ML models, with an F1-macro of 0.9983 and an Area Under the Receiver Operating Characteristic Curve (AUC-ROC) score of 0.9994, while the Long Short-Term Memory (LSTM) network with Multi-Head Attention performed best among the DL models, reaching an F1-macro of 0.9964, an accuracy of 0.9967, and an AUC-ROC of 0.9996. These results suggest that, with carefully engineered hybrid features, linear models can perform on par with deep architectures. Meanwhile, attention-based networks trained on customized tokenized inputs demonstrate a strong ability to capture structural and contextual dependencies in SQL queries. This finding highlights a promising research direction toward further optimizing attention-based neural architectures and exploring more expressive and domain-adaptive embedding strategies to enhance model generalization and robustness in real-world SQL injection detection.

Index Terms: SQL Injection Detection, Deep Learning, Machine Learning, TF-IDF, LinearSVC, LSTM

I. INTRODUCTION

Despite decades of research and defensive measures, SQL injection (SQLi) continues to pose a major challenge in web application security. It occurs when user input is improperly handled by a web application, allowing attackers to inject malicious SQL code into database queries. Such manipulation enables unauthorized access to sensitive information and may also allow data modification or deletion. In critical situations, SQLi can be leveraged to compromise the entire database or even the hosting server. Such attacks often result in prolonged exposure of confidential data, service disruption, and severe reputational or financial damage to affected organizations.

According to the Open Web Application Security Project (OWASP) Top 10: 2021 report [1], injection attacks—including SQL injection—remain among the most critical web application security risks. The report highlights that applications are vulnerable when untrusted data is directly interpreted or used to construct dynamic queries without adequate sanitization, a flaw that can lead to malicious code execution and other severe consequences. Although extensive awareness campaigns and modern development frameworks have been introduced, injection vulnerabilities remain among the most persistent security risks. Moreover, the continuous disclosure of new SQL injection vulnerabilities in 2025 further demonstrates the enduring nature of this threat. For instance, the high-severity vulnerability CVE-2025-25257 [2] was responsibly reported earlier this year, allowing unauthenticated attackers to execute arbitrary SQL queries in affected web platforms. Similar cases such as CVE-2025-1094 [3] and CVE-2025-22974 [4] confirm that SQL injection remains an active and exploitable weakness in current web systems. These findings underscore the necessity for more robust, automated, and learning-based detection mechanisms to mitigate evolving SQLi attack patterns.

Numerous studies have explored the detection of SQL injection attacks using rule-based methods, machine learning algorithms, and deep learning architectures. Rule-based approaches often rely on manually crafted signatures and regular expressions, which can effectively detect known attack patterns but fail to identify obfuscated or zero-day variants. Classical machine learning models, such as Logistic Regression or Support Vector Machines, improve detection accuracy through feature engineering but still depend heavily on predefined features. Deep learning techniques, on the other hand, demonstrate superior generalization ability yet typically require large-scale labeled datasets and high computational cost. These limitations highlight the need for more efficient, adaptive, and feature-aware detection strategies.

This study aims to address this issue by conducting a comparative analysis between machine learning–based and deep learning–based models to determine which approach performs more effectively in SQLi detection. The remainder of this paper is organized as follows. Section II reviews the related works on SQL injection detection. Section III describes the research methodology, including dataset preparation, feature engineering, and model training procedures. Section IV presents the experimental results and comparative

analysis of traditional and deep learning models. Finally, Section V concludes the paper and outlines potential directions for future work.

II. RELATED WORKS

Early studies on SQL injection detection focused on rule-based analysis and traditional machine learning. Initial works demonstrated that Support Vector Machines (SVM) could effectively distinguish malicious query patterns [5], while subsequent surveys summarized early input-validation and sanitization techniques [6]. Later research introduced hybrid static–dynamic detection methods that removed attribute values from SQL queries before analysis, improving precision in identifying injection attempts [7]. These approaches laid the groundwork for subsequent learning-based detection models. As web traffic and attack complexity increased, predictive analytics and feature-based machine learning methods emerged. Encoded traffic features and anomaly-detection frameworks were applied to identify SQLi patterns [8]. Further studies explored multiple supervised algorithms for early-stage detection and prevention [9], while hybrid feature-engineered approaches proved more effective than purely statistical ones [10]. Later, behavioral profiling with G-test–based feature selection achieved higher detection accuracy and stronger generalization across query types [11]. With the rise of deep learning, researchers began leveraging neural architectures for automatic feature extraction. Convolutional and multilayer perceptron (MLP) models were shown to be robust against obfuscated SQL payloads [12]. Recurrent autoencoders achieved 94% accuracy and 92% F1-score, capturing latent patterns within query sequences [13]. Autoencoder–XGBoost hybrids further improved detection performance, reaching approximately 99% accuracy on large-scale datasets [14]. Semantic-learning models such as synBERT captured contextual dependencies between SQL tokens, outperforming Convolutional Neural Network (CNN), LSTM, and MLP baselines [15], while lightweight multi-head attention architectures optimized self-attention for edge deployment [16]. Recent advances have extended detection beyond traditional query logs. Network-flow–based approaches achieved over 97% detection rate with minimal false alarms [17]. Hybrid deep-learning frameworks combining CNN, Gated Recurrent Unit (GRU), and attention mechanisms further expanded coverage to broader web vulnerabilities [18], [19]. These designs illustrate an ongoing trend toward multi-modal learning and real-time adaptability. Significant progress has been made, yet several challenges remain. Most existing systems rely on limited datasets such as the Kaggle SQL Injection dataset [20], which lack diversity and real-world query distributions. Cross-dataset generalization, interpretability of deep models, and integration with runtime protection remain open research questions. Future work should focus on robust data representation, transfer learning for unseen attack variants, and explainable AI mechanisms to balance accuracy, interpretability, and efficiency.

III. RESEARCH METHODOLOGY

This section describes the research methodology adopted in this study to develop and evaluate machine learning and deep learning models for SQL injection detection. The primary objective is to ensure a fair and reproducible comparison under identical experimental conditions. The methodology covers six stages: problem definition, dataset preparation, preprocessing, feature engineering, model training, and performance evaluation. The following subsections detail each component, beginning with the formal definition of the detection problem.

A. Problem Definition

Each SQL query is treated as an individual input sample, and the objective is to determine whether the query is malicious (injection) or benign (normal). The detection task is formulated as a binary text classification problem in which the model receives a SQL query and produces a binary label. A label of 1 represents an injection query, while 0 corresponds to a normal query. Prior to classification, every query string is converted into a numerical representation using a tokenizer or feature extraction method. Based on these representations, the classifier predicts the category of each query.

B. Data Collection

The dataset used in this study was obtained from a publicly available source on Kaggle, titled SQL Injection Dataset by Sajid (2021) [20]. It contains raw SQL query strings labeled as either benign or malicious. Each record includes two main fields: the Query column, which stores the raw SQL statement, and the Label column, which is an integer value indicating whether the query is non-malicious (0) or malicious (1). The dataset originally consists of 30,919 samples, which were further deduplicated and cleaned in this study to ensure the integrity of experimental evaluation. This publicly available dataset provides a practical benchmark for evaluating machine learning and deep learning models for SQL injection detection.

C. Data Preprocessing

We normalized whitespace and removed duplicate entries from the dataset. A stratified 80/20 split was then performed to preserve the class distribution, and cross-duplicates between the training and test subsets were eliminated to prevent data leakage. The final dataset contained 30,826 SQL queries, with 24,660 used for training and 6,166 for testing. The label distribution of the training set included 15,629 benign queries (63.19%) and 9,106 malicious queries (36.81%), while the test set contained 3,908 benign queries (63.20%) and 2,276 malicious queries (36.80%). This indicates that the dataset is relatively balanced across both subsets, ensuring unbiased evaluation of model performance.

D. Feature Engineering

In most machine learning frameworks, the default tokenization strategy is whitespace-based, where tokens are split only by spaces or punctuation marks. While effective for natural language text, this approach is

inadequate for SQL injection queries, which often contain concatenated keywords and symbols without explicit delimiters. During preliminary dataset inspection, we observed cases such as "**SELECT** UserId, Name, **PasswordFROM** Users," where SQL keywords and identifiers were merged. Such malformed instances disrupt syntactic boundaries and contextual cues, consequently degrading model performance.

To address this issue, we extended the tokenizer with a regex-driven module capable of parsing SQL keywords, identifiers, and non-word symbols while further splitting non-keyword segments. The enhanced tokenizer incorporates the following mechanisms:

- **Keyword-Prioritized Matching:** A pattern library of 112 standard SQL keywords is constructed, employing a longest-match-first strategy to preserve the integrity of SQL semantic units.
- **Adaptive Space-Agnostic Parsing:** To handle obfuscated SQL injection attacks that concatenate keywords without spaces (e.g., SELECT*FROM), recursive pattern matching is applied to automatically segment semantic units.
- **Special Character Preservation:** SQL operators (e.g., =, OR, --) are treated as independent tokens to maintain their semantic importance in injection patterns.

This design, aligned with linguistic feature engineering principles, ensures that obfuscated or malformed SQL queries are consistently segmented, thereby improving token representation quality and enhancing model robustness. The resulting tokens serve as the foundation for both machine learning (ML) and deep learning (DL) feature construction.

Unlike the G-test–based feature selection in [18], which focuses on statistically significant categorical variables, this study adopts a hybrid feature representation that integrates complementary textual and behavioral descriptors to capture richer structural and semantic cues.

Term Frequency–Inverse Document Frequency (TF-IDF) is employed to quantify word importance within the corpus. Specifically,

- **Term Frequency (TF):** measures how often a term appears in a document.
- **Inverse Document Frequency (IDF):** reflects how rare a term is across the corpus.

Three complementary feature channels are constructed as follows:

- **Character-level TF-IDF (1–4 gram):** captures fine-grained character patterns, special symbols, and obfuscated token boundaries.
- **Word-level TF-IDF (1–2 gram):** models token co-occurrences and keyword semantics using the custom SQL tokenizer while maintaining case sensitivity.
- **Numeric Statistical Features:** include query length, character composition ratios, case-switch counts, zero-width characters, quote pairing consistency, counts of risky functions and schema references (e.g., SLEEP, BENCHMARK, INFORMATION_SCHEMA), as well as hexadecimal pattern frequency and Shannon entropy.

This hybrid representation integrates textual and behavioral information, allowing traditional classifiers to capture both statistical and structural regularities of SQL injection queries, thereby forming a strong baseline for subsequent DL-based comparisons.

For deep learning models, vocabulary normalization is performed by replacing specific substrings—such as numbers, URLs, email addresses, file paths, hexadecimal strings, and Base64 segments—with placeholders (<NUM>, <URL>, <EMAIL>, <PATH>, <HEX>, <BASE64>). Case sensitivity and Unicode variants are preserved. The vocabulary is built exclusively from the training set, with a fixed size limit; unseen or out-of-range tokens are mapped to <UNK>.

SQL statements are encoded into fixed-length token sequences using the following configuration:

- **Maximum Sequence Length:** set to 128 tokens, covering over 99.5% of queries based on corpus statistics.
- **Truncation:** head truncation is applied to retain prefix information of SQL statements.
- **Padding:** post-zero padding is used for shorter sequences to ensure batch consistency.
- **Index Validation:** boundary clipping is employed to maintain valid token indices and enhance training stability.

A trainable embedding layer maps discrete tokens into a 128-dimensional continuous vector space. Learned end-to-end, this layer captures latent syntactic and semantic associations between SQL constructs and injection behaviors. The resulting embeddings encode contextual dependencies, enabling downstream neural layers to effectively discriminate between benign and malicious queries. With a vocabulary size of 50,000 and embedding dimension of 128, the embedding layer alone comprises approximately 6.4 million parameters. This end-to-end differentiable design eliminates the need for manual feature crafting, allowing the model to learn optimal representations directly from raw SQL statements.

E. Model Training

To evaluate detection performance comprehensively, both machine learning (ML) and deep learning (DL) models were trained on the same standardized SQL injection dataset under unified preprocessing and splitting protocols.

For the machine learning branch, four representative algorithms were employed: Logistic Regression, Linear Support Vector Classifier (LinearSVC), Random Forest, and Stochastic Gradient Descent (SGD) Classifier. Logistic Regression provides a probabilistic baseline

capable of modeling linear decision boundaries through maximum likelihood estimation. LinearSVC, as a margin-based classifier, performs robustly with high-dimensional sparse TF-IDF vectors. Random Forest leverages an ensemble of decision trees to capture nonlinear dependencies and feature interactions, while the SGDClassifier offers a stochastic optimization variant optimized for large-scale datasets. All ML models were trained using five-fold stratified cross-validation to maintain label balance and improve generalization. Their input features combined character-level TF-IDF, word-level TF-IDF generated by a custom SQL tokenizer, and numeric behavioral indicators derived from query-level statistics.

For the deep learning branch, sequential neural architectures were designed and trained on tokenized query sequences. The implemented models included Long Short-Term Memory (LSTM) networks for capturing long-range dependencies, Gated Recurrent Unit (GRU) networks for efficient sequence modeling with fewer parameters, and Transformer-based architectures capable of parallel sequence processing through self-attention mechanisms. Variants with and without self-attention were compared to analyze the contribution of attention to representation learning. All DL models used identical training-validation splits, early stopping, and consistent hyperparameter tuning strategies to ensure fair and reproducible comparison across architectures.

F. Model Evaluation

Model performance was primarily evaluated using the **F1-macro** score as the main evaluation metric, with the **Area Under the Receiver Operating Characteristic Curve (AUC-ROC)** serving as a complementary indicator. The F1-macro provides a balanced assessment of precision and recall across both classes, mitigating the influence of label imbalance. In contrast, the AUC-ROC measures the model's overall ability to distinguish between positive and negative samples across all possible classification thresholds, reflecting its discriminative power rather than sensitivity stability. Together, these metrics provide a comprehensive evaluation of detection accuracy and robustness. In binary classification, model performance can also be interpreted using a confusion matrix, which consists of four outcomes:

- **True Positive (TP):** Positive samples correctly predicted as positive.
- **False Positive (FP):** Negative samples incorrectly predicted as positive.
- **True Negative (TN):** Negative samples correctly predicted as negative.
- **False Negative (FN**): Positive samples incorrectly predicted as negative.

Based on these four values, the commonly used evaluation metrics are defined as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (4)$$

The Accuracy metric measures the overall proportion of correctly classified samples. Precision quantifies the ratio of correctly predicted positive samples among all predicted positive samples. Recall reflects the ability of the model to identify all actual positive samples. The F1-score represents the harmonic mean of Precision and Recall, providing a balanced measure that is particularly useful when dealing with imbalanced datasets.

The macro-averaged F1-score (F1-macro) computes the F1-score independently for each class and then takes the unweighted mean:

$$F_{1\text{-}macro} = \frac{1}{N}\sum_{i=1}^{N} F_{1i} \quad (5)$$

where N denotes the number of classes. This averaging method ensures that both majority and minority classes contribute equally to the final score, preventing the evaluation from being dominated by the class with more samples. Therefore, F1-macro provides a balanced view of model performance, which is particularly important in security-related detection tasks such as SQL injection identification, where data distribution may be slightly imbalanced.

The Area Under the Receiver Operating Characteristic Curve (AUC-ROC) measures the model's ability to distinguish between positive and negative samples across various classification thresholds. It reflects the trade-off between the True Positive Rate (TPR) and False Positive Rate (FPR), providing a threshold-independent evaluation of discriminative capability. A higher AUC-ROC value indicates that the model can effectively separate attack and benign samples under different decision boundaries, implying strong generalization and robustness in detection tasks.

In summary, the F1-macro score captures the model's overall classification balance, while the AUC-ROC quantifies its discriminative power across varying thresholds. By jointly analyzing both indicators, the study ensures a comprehensive and reliable evaluation of model performance, stability, and robustness.

To further understand the contribution of each feature group, we designed a threefold feature-importance analysis framework consisting of ablation study, permutation importance, and coefficient-based interpretation. The ablation study isolates the influence of each feature group—such as character-level TF-IDF, word-level TF-IDF, and numeric behavioral indicators—by retraining models with specific components removed, thereby revealing their relative impact on detection performance. Permutation importance evaluates feature sensitivity by randomly shuffling individual feature values and observing the resulting decline in model accuracy or F1-macro, offering a model-agnostic estimate of feature relevance. Finally, coefficient-based interpretation leverages the learned weights from linear

models (e.g., Logistic Regression, LinearSVC) to identify the most influential features that drive the classification boundary. Together, these complementary analyses provide both global and local insights into how different representations contribute to SQL injection detection.

IV. EXPERIMENTAL RESULTS

This section reports the experimental results and comparative performance analysis of multiple machine learning and deep learning models for SQL injection detection. All models were trained and evaluated under identical preprocessing and training settings to ensure fair and reproducible comparison. The results include overall performance metrics such as F1-macro, accuracy, and AUC-ROC, followed by further analyses on feature ablation, permutation importance, and coefficient interpretation to investigate the contribution of different feature groups.

A. Results of Machine Learning Models

Table I summarizes the overall performance of the evaluated machine learning models, while the confusion matrix of the best-performing model, LinearSVC, is presented in Fig. 1. The results show that LinearSVC achieved near-perfect classification performance, correctly identifying almost all benign and injection queries. Out of 6166 test samples, only 10 were misclassified (2 false positives and 8 false negatives), yielding an overall accuracy of 99.84%. The strong diagonal dominance in the confusion matrix demonstrates that the model generalizes well and effectively captures discriminative patterns in the hybrid feature space. The corresponding AUC-ROC of 0.9994 further indicates stable precision and recall across varying thresholds. This stability supports the robustness of the linear decision boundary when enriched with both textual and statistical representations. Overall, these findings confirm that even a simple linear model can achieve state-of-the-art performance in SQL injection detection when trained on well-engineered features.

PERFORMANCE COMPARISON OF MACHINE LEARNING MODELS

TABLE 1.

Model	*F1_macro*	*Accuracy*	*AUC_ROC*
LinearSVC	**0.9983**	**0.9984**	0.9994
Random Forest	0.9981	0.9982	**0.9999**
Logistic Regression	0.9969	0.9971	0.9992
SGDClassifier	0.9956	0.9959	0.9986

[a.] Note: Bold indicates the best-performing metrics across models

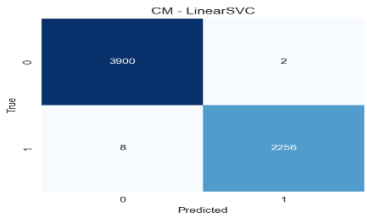


Fig. 1. Confusion Matrix of LinearSVC

To evaluate the contribution of each feature group, a feature ablation study was performed using the LinearSVC model as the baseline. In each configuration, one or more feature groups were removed to observe the corresponding performance drop in F1-macro and Area Under the Precision–Recall Curve (AUC-PR). The results are summarized in Fig. 2.

As shown in Fig. 2, removing any single feature group resulted in only a minor degradation, indicating that the hybrid design provides overlapping yet complementary information. When the character-level TF-IDF was excluded, the model maintained a comparable score (F1 = 0.9981), indicating that fine-grained character information contributes moderately to the overall classification. In contrast, removing word-level TF-IDF or numeric indicators both led to a slightly larger drop in F1 (around 0.14%), confirming their complementary roles in capturing semantic and statistical cues. Using only individual feature groups further validated this trend: Only Numeric achieved an F1 of 0.9932, Only Char-TFIDF reached 0.9956, and Only Word-TFIDF reached 0.9963, which correspond to 99.5%, 99.7%, and 99.8% of the baseline performance, respectively.

The feature-removal impact ranking highlights that numeric indicators yield the most noticeable decline (0.51%), followed by character- and word-level TF-IDF (0.26% and 0.19%). This pattern indicates that numeric behavioral metrics—such as query length, symbol ratios, and risky function counts—serve as strong discriminative signals that cannot be fully substituted by textual embeddings.

Regarding computational cost, the training time ranged from 1.3 seconds for the numeric-only configuration to 23.1 seconds for the full hybrid model. Excluding TF-IDF components significantly reduced training time, demonstrating the expected trade-off between representational richness and computational efficiency.

Overall, the ablation results confirm that the hybrid feature design effectively integrates complementary perspectives of SQL query characteristics. Word-level and numeric features play the most decisive roles in maintaining high precision and recall, while character-level signals provide fine-grained support for edge cases such as obfuscated payloads.

To validate these observations from another perspective, two complementary feature-importance analyses were conducted: permutation importance and coefficient interpretation. The permutation importance analysis quantifies the impact of each feature group by measuring the F1-macro decrease after random shuffling, while the coefficient analysis directly examines the absolute weights, L2 norms, and sparsity patterns of linear models. The detailed results of these analyses are presented in Fig. 3 and Fig. 4.

As shown in Fig. 3, the numeric feature group produced the largest performance degradation when permuted, with an importance mean of 0.2647 ± 0.0042, accounting for 78.4% of the total normalized contribution. This confirms that handcrafted numeric statistics—such as query length, symbol ratios, quote-

pair consistency, and risky function counts—encode highly discriminative behavioral cues that cannot be replaced by textual representations.

The word-level TF-IDF group ranked second, with an importance of 0.0679 ± 0.0050 (20.1%), indicating its effectiveness in modeling the lexical and semantic patterns of SQL keywords and operators. In contrast, character-level TF-IDF contributed only 0.0051 ± 0.0019 (1.5%), reflecting its role as a supplementary signal for detecting obfuscated tokens and minor encoding anomalies rather than major structural patterns.

Interestingly, the numeric features, while constituting less than 0.2% of the total dimensionality, contributed more than three-quarters of the model's predictive strength. This imbalance underscores the high information density of numeric behavioral metrics relative to high-dimensional TF-IDF representations. Consequently, these results reaffirm the complementary nature of the hybrid feature design—where numeric indicators capture macro-level statistical anomalies, and TF-IDF features encode finer lexical and symbolic variations within SQL queries.

To provide further interpretability for linear models, coefficient analysis was performed on the LinearSVC classifier. This analysis examined the magnitude, sparsity, and sign distribution of learned coefficients for each feature group. The results are visualized in Fig. 4.

As shown in Fig. 4, the word-level TF-IDF group dominates the model in total weight, accounting for 81.8% of the summed coefficient magnitude. This confirms its central role in determining decision boundaries by capturing the presence and interaction of key SQL tokens such as SELECT, FROM, WHERE, and conditional operators. The character-level TF-IDF features contribute 14.1%, providing additional sensitivity to special characters, case variations, and obfuscated payload fragments that are invisible at the token level. The numeric features, while responsible for only 4.2% of the total weight, show the highest average coefficient magnitude (0.5214) and the lowest sparsity (11.4%), suggesting that each numeric indicator exerts a strong, consistent influence on the model's decision process.

From a geometric perspective, the L2 norm values (11.1 for word-level, 5.3 for char-level, and 4.4 for numeric) further confirm that the learned hyperplane relies heavily on the dense word-based feature space, while numeric features provide compact yet high-impact signals. The sign distribution analysis reveals a balanced pattern across feature groups, with roughly equal proportions of positive and negative coefficients, indicating that both the presence and absence of certain patterns contribute meaningfully to prediction.

In summary, the coefficient-based interpretation aligns with the ablation and permutation results: word-level TF-IDF features drive the majority of discrimination, character-level TF-IDF refines boundary precision for obfuscated cases, and numeric indicators act as strong behavioral anchors that enhance the model's robustness and interpretability.

To consolidate the findings from the previous analyses, an integrated comparison of feature importance across the three evaluation methods—feature ablation, permutation importance, and coefficient analysis—was performed. The combined results are presented in Fig. 5.

The three analytical perspectives yield a broadly consistent pattern while highlighting complementary aspects of the feature contributions. Across all methods, word-level TF-IDF remains the most influential feature group, accounting for nearly half of the overall importance (49.6%). This dominance demonstrates that lexical and semantic cues extracted through token-level modeling play a decisive role in identifying injection-related query structures. The numeric indicators rank second (43.2%), showing that a small set of statistical descriptors—such as query length, character ratios, and risky function counts—capture behavioral anomalies that text-based features alone cannot represent. Finally, character-level TF-IDF contributes about 7.2%, providing complementary sensitivity to subtle lexical variations and encoding noise.

Method-wise comparisons confirm the complementary nature of these analyses. Ablation testing emphasizes the practical performance impact of each feature group on model accuracy, permutation importance reflects their predictive dependency strength, and coefficient analysis quantifies their direct influence on the decision boundary. The radar plot and stacked bar chart jointly indicate that the three methods converge on the same hierarchical order—word-level TF-IDF > numeric stats > char-level TF-IDF—while differing slightly in magnitude due to methodological bias.

Overall, these results verify that the proposed hybrid feature representation effectively integrates symbolic, statistical, and lexical perspectives. Word-level features capture contextual semantics, numeric metrics detect statistical irregularities, and character-level patterns reinforce robustness against obfuscation. This cross-method consensus provides strong empirical evidence for the interpretability and stability of the final LinearSVC model.

PERFORMANCE COMPARISON OF DEEP LEARNING MODELS

TABLE 2.

Model	*F1_macro*	*Accuracy*	*AUC-ROC*
LSTM + Multi-Head Attention	**0.9964**	**0.9967**	**0.9996**
LSTM + Self-Attention	0.9959	0.9963	0.9995
GRU + Multi-Head Attention	0.9959	0.9963	0.9994
LSTM	0.9955	0.9959	0.9991
GRU + Self-Attention	0.9955	0.9959	0.9995
Transformer	0.9951	0.9955	0.9990
GRU	0.9942	0.9947	0.9994

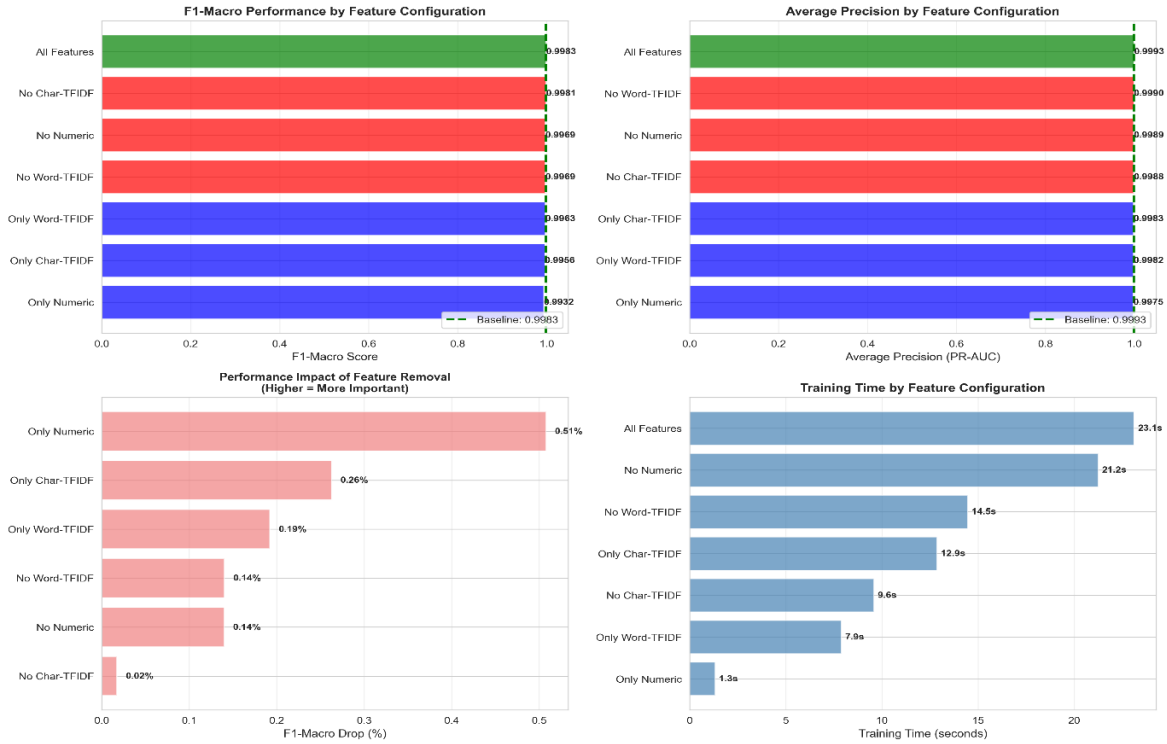


Fig. 2. Impact of feature group removal on F1 macro, PR-AUC, and training time using the LinearSVC model.

Fig. 3. Permutation importance analysis of feature groups in the LinearSVC model.

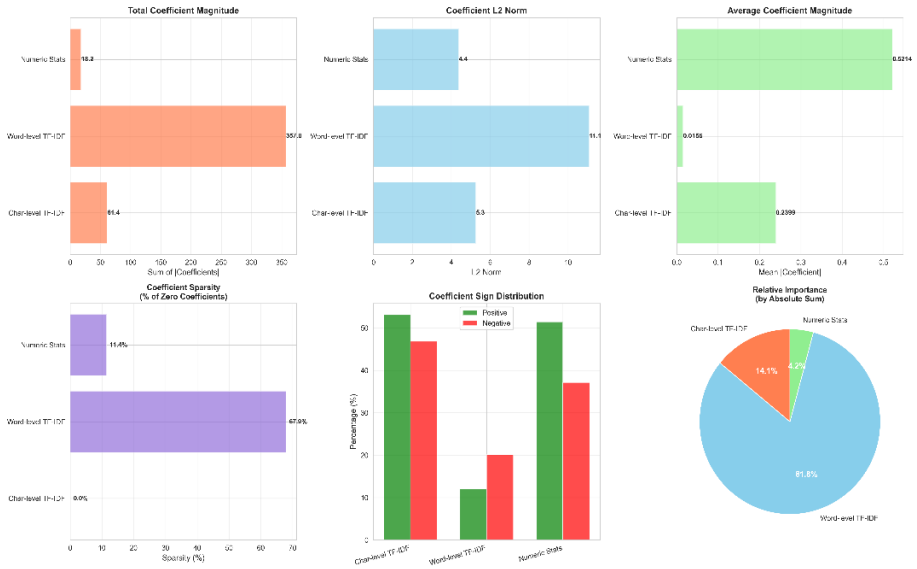


Fig. 4. Coefficient-based feature weight distribution of the LinearSVC model.

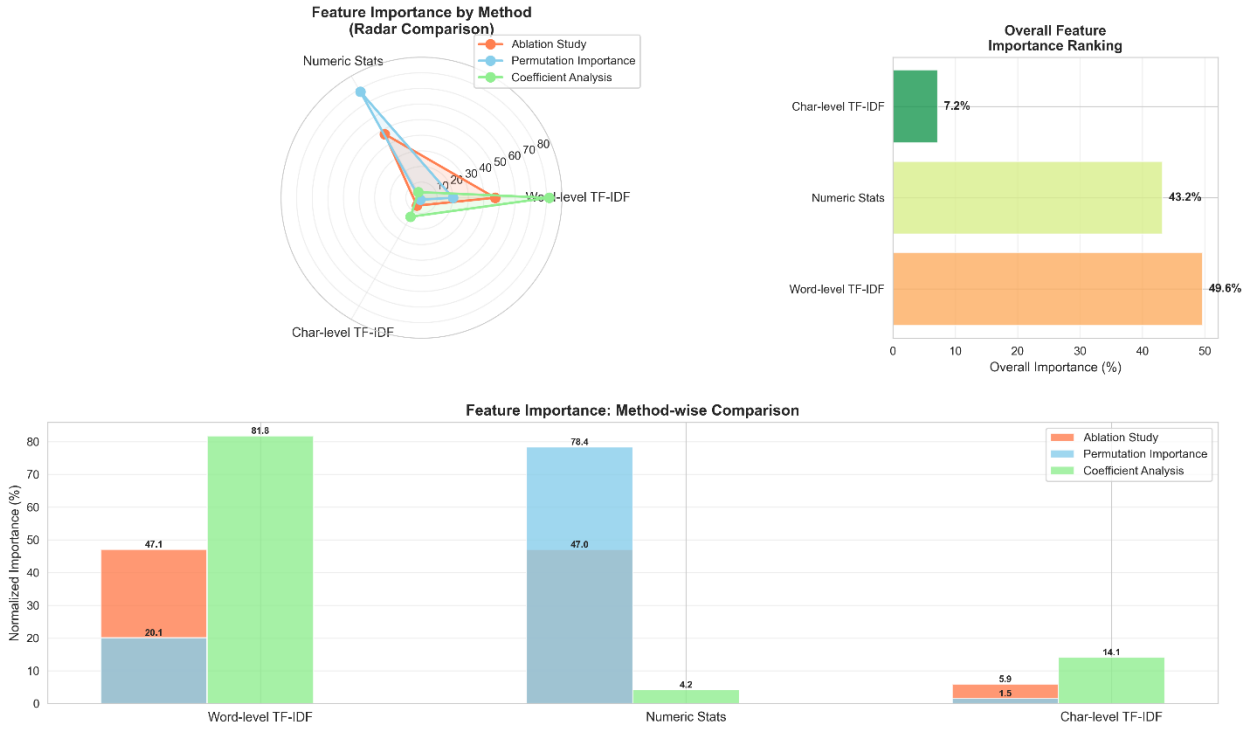


Fig. 5. Integrated comparison of feature importance across ablation, permutation, and coefficient analyses.

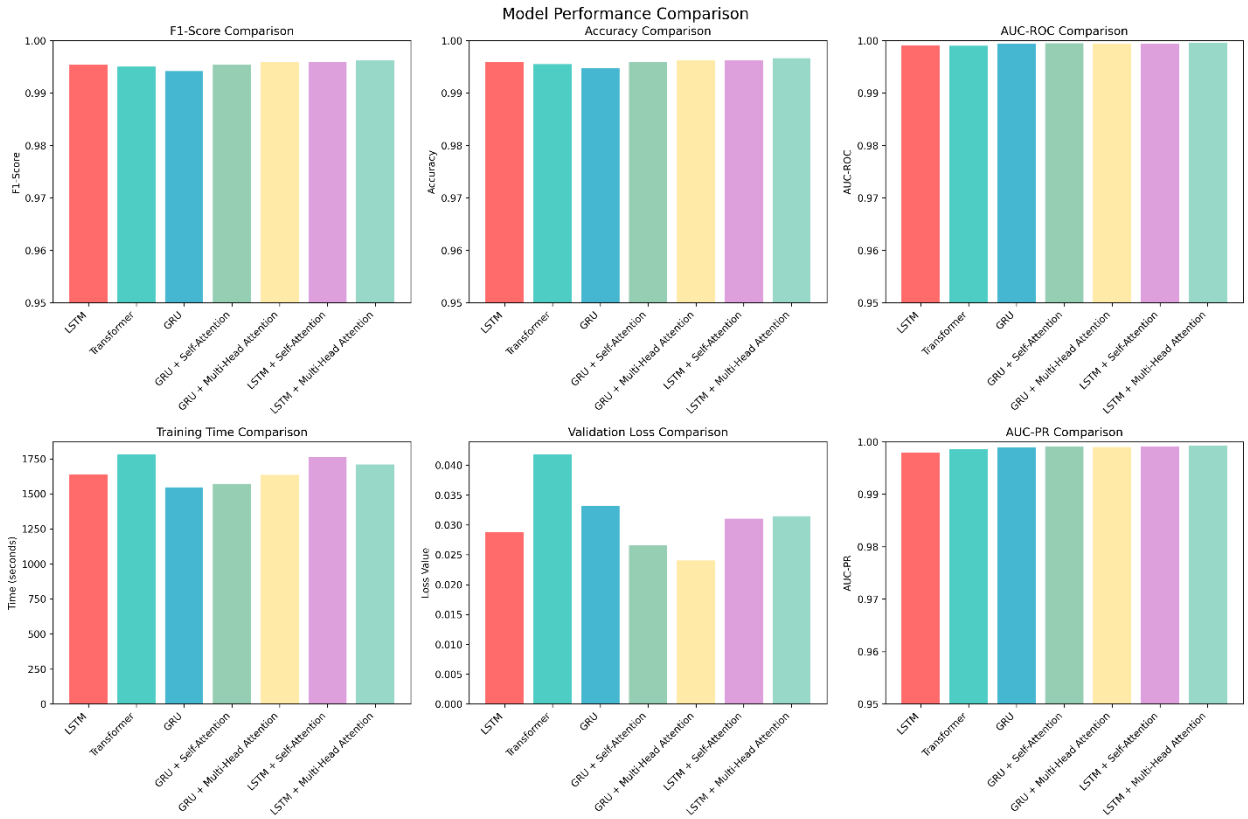


Fig. 6. Deep learning model performance comparison on SQLi detection.

B. Results of Deep Learning Models

Table II summarizes the quantitative results of all deep learning models evaluated in this study. As shown, all architectures—including LSTM, GRU, and Transformer variants—achieved strong detection performance, with AUC-ROC values above 0.9990 and F1-macro scores exceeding 0.994. Among the baseline models, the LSTM attained the highest performance (F1-macro = 0.9955, Accuracy = 0.9959), confirming its effectiveness in capturing sequential dependencies within SQL queries. In contrast, the GRU achieved slightly lower results (F1-macro = 0.9942), suggesting that its simplified gating structure may limit long-range context modeling, while the Transformer exhibited competitive accuracy but required the longest training time due to its multi-head attention operations.

When attention mechanisms were introduced, overall performance further improved across all recurrent architectures. The LSTM + Multi-Head Attention model achieved the best overall results (F1-macro = 0.9964, Accuracy = 0.9967, AUC-ROC = 0.9996), followed closely by the LSTM + Self-Attention and GRU + Multi-Head Attention configurations. These results demonstrate that attention modules effectively enhance feature discrimination by enabling the network to focus on semantically critical tokens (e.g., SQL operators, functions, and delimiters) that distinguish injection patterns. Figure 6 visualizes the comparative performance across all evaluated deep learning models, showing that attention-augmented recurrent architectures consistently achieve higher F1-scores, accuracy, and more stable convergence compared to their baseline counterparts.

C. Comparative Analysis and Discussion

The experimental results demonstrate that both traditional machine learning (ML) and deep learning (DL) models achieve near-perfect detection performance on the standardized SQL injection dataset. However, several important insights emerge when comparing their internal mechanisms and feature dependencies.

First, linear models—particularly the LinearSVC—achieve outstanding results, with an F1-macro of 0.9983 and AUC-ROC of 0.9994. The hybrid feature space, composed of character-level, word-level, and numeric descriptors, provides sufficient discriminative capacity for linear decision boundaries to separate benign and malicious queries effectively. The comprehensive feature-importance analyses indicate that word-level TF-IDF features contribute the most to model performance, followed by numeric behavioral indicators and character-level n-gram patterns. This finding highlights that lexical and contextual relationships between SQL keywords are the primary drivers of accurate classification, while numeric features serve as complementary behavioral signals that enhance stability and robustness.

Nevertheless, the performance of traditional ML models still depends on the predefined feature representation. Although the TF-IDF embeddings capture surface-level context effectively, they lack the deeper structural and syntactic understanding required to handle obfuscated or context-shifted attacks. This limitation suggests that the impressive accuracy of ML models largely stems from well-engineered features rather than true adaptability to unseen injection styles.

In contrast, deep learning architectures, such as LSTM with Multi-Head Attention, learn hierarchical dependencies directly from token sequences. This enables them to model richer contextual interactions between operators, keywords, and parameters without explicit feature engineering. Despite achieving comparable quantitative results, the deep learning models exhibit a stronger capacity for contextual understanding and generalization, making them better suited for dynamic and unpredictable attack environments.

In summary, traditional ML models remain efficient, interpretable, and competitive under optimized hybrid features, whereas DL models provide stronger potential for context-aware generalization. A promising direction for future work lies in hybridizing both paradigms—leveraging TF-IDF-based lexical signals and numeric descriptors for fast static filtering, followed by attention-based neural models for deeper semantic verification and anomaly detection.

CONCLUSION AND FUTURE WORK

This study conducted a comprehensive comparative analysis of traditional machine learning (ML) and deep learning (DL) models for SQL injection (SQLi) detection under a unified experimental framework. Both model categories achieved near-perfect accuracy and reliability on a standardized dataset, with the Linear Support Vector Classifier (LinearSVC) and the LSTM architecture with Multi-Head Attention emerging as the top performers. The results reveal that linear models can achieve highly competitive performance when supported by a well-engineered hybrid feature space. Among all feature groups, word-level TF-IDF features were found to be the most decisive, capturing contextual and lexical relationships between SQL keywords. Numeric indicators, such as query length, symbol ratios, and risky function occurrences, serve as complementary behavioral signals that enhance detection stability, while character-level TF-IDF features provide fine-grained sensitivity to obfuscation patterns. This multi-view representation enables linear models to construct effective decision boundaries without complex architectures. However, such performance still depends on the quality of predefined feature engineering. While ML models perform efficiently and interpretably, their reliance on manually designed representations may limit adaptability to unseen or obfuscated attack variants. In contrast, deep learning models demonstrate stronger flexibility through automatic feature extraction. Architectures equipped with attention mechanisms effectively capture structural and contextual dependencies within SQL queries, offering higher robustness against evolving attack behaviors. Although computationally more expensive, their capacity for representation learning makes them promising candidates for large-scale or continuously changing environments. Future work will focus on combining the

strengths of both paradigms. A hybrid detection framework could employ lightweight ML models with engineered lexical–numeric features for fast pre-screening, followed by attention-based neural networks for deep semantic validation. Further research directions include the construction of larger and more diverse SQLi datasets covering zero-day and obfuscated patterns, the application of continual or self-supervised learning for adaptive model updates, and the exploration of cross-dataset transfer learning to improve real-world generalization.

REFERENCES

[1] OWASP Foundation. (2021) OWASP Top 10: 2021 – The Ten Most Critical Web Application Security Risks. Accessed: Nov. 3, 2025. [Online]. Available: https://owasp.org/Top10/

[2] National Vulnerability Database. (2025) CVE-2025-25257 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-25257.

[3] ——. (2025) CVE-2025-1094 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-1094.

[4] ——. (2025) CVE-2025-22974 Detail. https://nvd.nist.gov/vuln/detail/CVE-2025-22974.

[5] S. Rawat and R. Shrivastav, "SQL Injection Attack Detection Using SVM," International Journal of Computer Applications, vol. 57, no. 7, pp. 10–15, 2012. Introduced one of the first ML-based SQL injection detection systems using Support Vector Machine for real-time query analysis. [Online]. Available: https://doi.org/10.5120/5749-7043

[6] A. Kumar and P. K. Pateriya, "A Survey on SQL Injection Attacks, Detection and Prevention Techniques," in 2012 International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2012, pp. 1–5. Comprehensive early survey summarizing SQLi detection and prevention mechanisms. [Online]. Available: https://doi.org/10.1109/ICCCNT.2012.6396096

[7] H.-C. Lee, S. K. Jeong, S. Yeo, and J. Moon, "A Novel Method for SQL Injection Attack Detection Based on Removing SQL Query Attribute Values," Mathematical and Computer Modelling, vol. 55, no. 1–2, pp. 58–68, 2012. Proposed a combined static and dynamic analysis method by removing query attribute values for SQLi detection. [Online]. Available: https://doi.org/10.1016/j.mcm.2011.01.050

[8] S. O. Uwagbole, W. J. Buchanan, and L. Fan, "Applied Machine Learning Predictive Analytics to SQL Injection Attack Detection and Prevention," in 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 1087–1090. Predictive analytics on encoded web traffic for SQL injection attack detection. [Online]. Available: https://doi.org/10.23919/INM.2017.7987433

[9] I. Jemal, O. Cheikhrouhou, H. Hamam, and A. Mahfoudhi, "SQL Injection Attack Detection and Prevention Techniques Using Machine Learning," International Journal of Applied Engineering Research, pp. 569–580, 2020.

[10] T. Muhammad and H. Ghafory, "SQL Injection Attack Detection Using Machine Learning Algorithm," Mesopotamian Journal of CyberSecurity, vol. 2022, pp. 5–17, 2022. Comparative study of different ML models for SQL injection detection. [Online]. Available: https://doi.org/10.58496/MJCS/2022/002

[11] S. A. Balogun, M. Ijiga, N. Okika, L. A. Enyejo, and J. O. Ogboji, "Machine Learning-Based Detection of SQL Injection and Data Exfiltration Through Behavioral Profiling of Relational Query Patterns," International Journal of Innovative Science and Research Technology, vol. 8, no. 8, pp. 324–332, 2023.

[12] D. Chen, Q. Yan, C. Wu, and J. Zhao, "SQL Injection Attack Detection and Prevention Techniques Using Deep Learning," in Journal of Physics: Conference Series (ICCBDAI 2020), vol. 1757, no. 1, 2021, p. 012055. Evaluated CNN and MLP architectures for SQLi detection, achieving high accuracy against obfuscated payloads. [Online]. Available: https://doi.org/10.1088/1742-6596/1757/1/012055

[13] M. Alghawazi, D. Alghazzawi, and S. Alarifi, "Deep Learning Architecture for Detecting SQL Injection Attacks Based on RNN Autoencoder Model," Mathematics, vol. 11, no. 15, p. 3286, 2023. Proposed RNN autoencoder architecture for SQLi detection, achieving 94% accuracy.

[14] N. Thalji, A. Raza, M. S. Islam, N. Abdel Samee, and M. M. Jamjoom, "AE-Net: Novel Autoencoder-Based Deep Features for SQL Injection Attack Detection," IEEE Access, vol. 11, pp. 135507–135516, 2023. Proposed an autoencoder ("AE-Net") to automatically extract deep features from SQL queries; achieved 0.99 accuracy via XGBoost on 46,392 SQL queries. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3337645

[15] D. Lu, J. Fei, and L. Liu, "A Semantic Learning-Based SQL Injection Attack Detection Technology," Electronics, vol. 12, no. 6, p. 1344, 2023. Introduced the synBERT semantic-learning model for SQLi detection, outperforming CNN, MLP, and LSTM on diverse datasets. [Online]. Available: https://doi.org/10.3390/electronics12061344

[16] R.-T. Lo, W.-J. Hwang, and T.-M. Tai, "SQL Injection Detection Based on Lightweight Multi-Head Self-Attention," Applied Sciences, vol. 15, no. 2, p. 571, 2025. Proposed a lightweight multi-head self-attention NLP model for SQL injection detection suitable for edge deployment. [Online]. Available: https://doi.org/10.3390/app15020571

[17] I. S. Crespo Martínez, A. Campazas Vega, M. Guerrero Higueras, V. Riego Del Castillo, C. Álvarez Aparicio, and C. Fernández Llamas, "SQL Injection Attack Detection in Network Flow Data," Computers & Security, vol. 127, p. 103093, 2023. Extends SQLi detection to network-flow data rather than just application logs. [Online]. Available: https://doi.org/10.1016/j.cose.2023.103093

[18] R. Vadisetty, P. C. R. Chinta, C. Moore, L. M. Karaka, M. Sakuru, V. Bodepudi, S. R. Maka, and S. R. Vangala, "Intelligent Detection of Injection Attacks via SQL Based on Supervised Machine Learning Models for Enhancing Web Security," Journal of Artificial Intelligence and Big Data, vol. 4, no. 2, p. 11, 2024. Proposed supervised ML models (e.g., GRU) for SQL injection detection achieving 96.65% accuracy.

[19] S. Ali, A. Mohammed, S. Mustafa, and S. Salih, "Web Vulnerabilities Detection Using a Hybrid Model of CNN, GRU and Attention Mechanism," Science Journal of University of Zakho, vol. 13, no. 1, pp. 58–64, 2025. DOI link currently inactive; article accessible via ResearchGate and SJZ University repository.

[20] M. Sajid, "SQL Injection Dataset," Kaggle Datasets, 2021. Accessed: Nov. 4, 2025. Public dataset of labeled SQL queries used for SQL injection detection. [Online]. Available: https://www.kaggle.com/datasets/sajid576/sql-injection-dataset

ДРОНЫГ ХҮРГЭЛТИЙН ҮЙЛЧИЛГЭЭНД АШИГЛАХ БОЛОМЖЫН СУДАЛГАА

Батзоригийн АМАРЖАРГАЛ, Соном-Очирын ӨЛЗИЙБАЯР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн технологийн тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: J.DS25E005@must.edu.mn[1], ulziibayar@must.edu.mn[2]

Хураангуй - Энэхүү судалгааны зорилго нь Монгол Улсын нөхцөлд дронд суурилсан хүргэлтийн системийг нутагшуулах техникийн болон зохион байгуулалтын боломжийг тодорхойлох, уур амьсгал, газарзүй, дэд бүтцийн онцлогт нийцсэн системийн загвар боловсруулахад оршино. Судалгаанд PX4, QGroundControl, MAVSDK зэрэг open source системийг ашиглан дрон нислэгийн автомат удирдлага, замын төлөвлөлт, эрчим хүчний оновчлолыг туршилтаар шинжилсэн. Dijkstra, A*, RRT болон Energy-aware A* алгоритмуудыг харьцуулан үнэлэхэд A* арга замын оновчлол, тооцооллын хурдны хувьд илүү үр ашигтай болохыг харуулсан бол Energy-aware A* загвар нь салхи болон эрчим хүчний хэрэглээг тооцсон нөхцөлд батерейны ашиглалтын үр ашгийг 20–25 хувиар нэмэгдүүлж, нислэгийн хугацаа, эрчим хүчний зарцуулалтын тэнцвэрийг сайжруулсан байсан. Туршилтын үр дүн болон системийн загварчлалд үндэслэн Монгол Улсад дронд суурилсан хүргэлтийн системийг үе шаттайгаар хэрэгжүүлэхэд шаардлагатай техникийн болон дэд бүтцийн нөхцөлийг тодорхойлсон. Үүнд хяналтын төвийн байрлал, буулт-хөөрөлтийн талбайн зохион байгуулалт, холбооны сүлжээний найдвартай байдал зэрэг гол хүчин зүйлсийг тодорхойлсон. Судалгааны үр дүн нь дронд суурилсан хүргэлтийн системийг Монгол Улсад үе шаттайгаар нэвтрүүлэхэд шаардлагатай техникийн болон дэд бүтцийн үндэс суурийг тодорхойлж, логистикийн үр ашгийг нэмэгдүүлэх, хүргэлтийн хугацааг 30–40 хувиар богиносгох, авто замын түгжрэлийг бууруулах, агаарын бохирдлыг хязгаарлах боломжийг харуулж байна.

Түлхүүр үг: U UAV, Drone Delivery, PX4, QGroundControl, MAVSDK, Autonomous Navigation, System Architecture, Route Planning, Emergency Management, Urban Infrastructure, Mongolia

I. УДИРТГАЛ

Сүүлийн жилүүдэд дроныг хүргэлтийн үйлчилгээнд ашиглах нь эрчимтэй хөгжиж, логистикийн үр ашгийг нэмэгдүүлэх шинэ шийдэл болж байна. Гэвч эдгээр систем нь ихэвчлэн өндөр дэд бүтэц, зохицуулалттай орнуудад туршигдсан байдаг. Монгол Улсад газарзүйн өндөрлөг байршил, эрс тэс уур амьсгал, түгжрэл, агаарын бохирдол зэрэг нөхцөл нь дрон хүргэлтийн системийг нутагшуулахад техникийн сорилт үүсгэдэг. Иймээс энэхүү судалгааны зорилго нь Улаанбаатар хотын орчны онцлогт нийцсэн дронд суурилсан хүргэлтийн системийн архитектур, замын төлөвлөлт, удирдлагын бүтэц, дэд бүтцийн шаардлагыг тодорхойлон, нутагшуулах техникийн боломжийг тодорхойлход оршино.

II. ИЖИЛ ТӨСТЭЙ АЖЛУУДЫН СУДАЛГАА

Дронд суурилсан хүргэлтийн судалгаа сүүлийн жилүүдэд эрчимтэй хөгжиж, хүргэлтийн үр ашгийг дээшлүүлэх, зардал ба цагийн алдагдлыг бууруулах, логистикийн шинэ загвар бий болгох чиглэлд өргөжиж байна. Судалгааны ажлуудыг ерөнхийд нь гурван ангилалд хуваж болно: (1) системийн архитектур ба удирдлагын бүтэц, (2) зам төлөвлөлт ба энергийн оновчлол, (3) дэд бүтэц ба зохицуулалтын орчин.

Шинжээчид дрон хүргэлтийн системийг хэрэглэгчийн аппликейшн, маршрутын тооцоолол, нислэгийн удирдлага, хяналтын төв гэсэн дөрвөн бүрэлдэхүүнтэй гэж тодорхойлсон. Jazairy ба Al-Hassan дрон хүргэлтийн нийгэм-эдийн засаг, экологийн нөлөөллийг үнэлж, CO_2 ялгарлыг 70–90 %-иар бууруулах боломжтойг тооцсон бол Aurambout нар Европын туршилтаар 10–15 км радиуст хүргэлт хамгийн үр ашигтай болохыг тогтоожээ. Persson буулт-хөөрөлтийн талбайн зохицуулалтын дутагдал, хяналтын дүрмийн тодорхой бус байдал дрон хүргэлтийн гол саад болдгийг онцолсон.

Алгоритмын судалгаанд Garcia ба Santoso Dijkstra ба A* аргуудыг харьцуулж, A* нь бодит цагийн төлөвлөлтөд илүү үр ашигтай болохыг, Hong нар Energy-aware A* моделийг салхины нөлөө ба энергийн хэрэглээг тооцсон сайжруулсан хувилбар болохыг нотолсон. Qin нар олон дрон зэрэг ажиллуулах үед хиймэл оюунд суурилсан хяналтын механизм нь эрчим хүч ба хугацааны оновчлолыг 10–15%-иар сайжруулдгийг харуулсан. Grofelnik нар аюулгүй ажиллагааны судалгаанд geofencing, автомат RTH системийг стандартчлах шаардлагатайг тодорхойлсон бол Su нар дрон ба газрын тээврийг хослуулсан загвар логистикийн зардлыг 20–25 %-иар бууруулах боломжтойг дүгнэсэн.

Эдгээр судалгааныудын нийтлэг дүгнэлтээр дрон хүргэлтийн технологийг амжилттай нутагшуулахын тулд зам төлөвлөлт, энергийн менежмент, дэд бүтэц, аюулгүй ажиллагаа, хууль эрх зүйн зохицуулалтыг цогцоор шийдвэрлэх шаардлагатайг харуулж байна.

III. СИСТЕМИЙН ЕРӨНХИЙ АРХИТЕКТУР

Дрон хүргэлтийн систем нь хэрэглэгчийн захиалгаас эхлэн нислэгийг гүйцэтгэж, хүргэлт баталгаажуулах хүртэлх уялдаа холбоотой үе шатуудаас бүрдэнэ. Үйл ажиллагааг оновчтой зохион байгуулахын тулд системийг дараах дөрвөн үндсэн давхаргад хуваан төлөвлөдөг.

1. Захиалга ба даалгаврын давхарга: хэрэглэгчийн хүсэлт, хүргэлтийн хаяг, багцын мэдээллийг хүлээн авч системд бүртгэнэ.

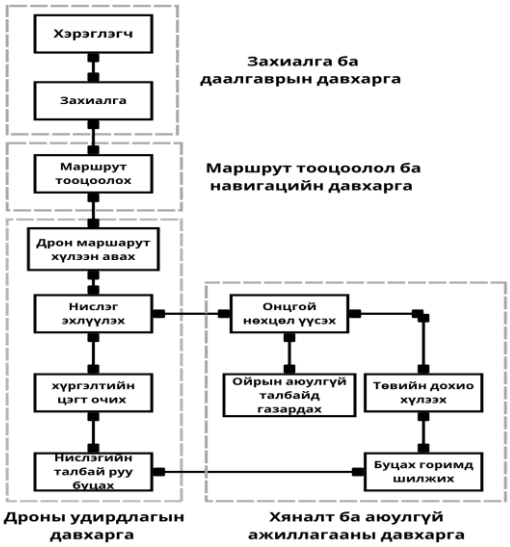
2. Маршрут төлөвлөлтийн давхарга: A*, Dijkstra зэрэг алгоритмаар хүргэлтийн хамгийн оновчтой замыг тодорхойлж, салхи болон өндрийн ялгааг тооцдог.

3. Удирдлагын давхарга: нислэгийн төлөвлөгөөг дронд дамжуулж, GPS болон мэдрэгчийн мэдээллээр байрлал, хурд, өндрийг хянаж бодит цагийн мэдээлэл илгээнэ.

4. Хяналт ба аюулгүй ажиллагааны давхарга: системийн найдвартай ажиллагааг хангах зорилгоор гео-хашаалалт, буцах горим (*Return-to-Home*), холбоо тасрах, ослын үеийн хамгаалалт зэрэг функц агуулна.

Хэрэглэгч захиалгаа илгээмэгц систем автоматаар нислэгийн маршрутыг тооцож, дрон үүрэг хүлээн авч нислэгийг эхлүүлнэ. Хяналтын төвтэй бодит цагийн холболт үүсч, байрлал, хурд, батерейны түвшин зэрэг өгөгдөл тасралтгүй солигдоно. Хүргэлтийн дараа дрон буцах маршрутаар буцаж, нислэгийн мэдээлэл системд хадгалагдана.

Монголын өндөрлөг газарзүй, хүчтэй салхи, хүйтэн уур амьсгалын нөхцөлд эдгээр хамгаалалтын механизмууд дрон хүргэлтийн системийн тогтвортой, аюулгүй ажиллагааг хангах инженерийн үндэс болдог.



1 – р зураг. Системийн архитектур

IV. ТЕХНОЛОГИЙН ШИЙДЭЛ

Дронд суурилсан хүргэлтийн систем нь олон дэд системийн уялдаа холбоонд тулгуурлан ажилладаг. Түүний найдвартай байдал, үр ашиг, аюулгүй ажиллагаа нь технологийн шийдлүүдийн зохистой хослолоос хамаарна. Энэхүү хэсэгт системийн гол технологийн бүрэлдэхүүн — холбоо ба удирдлага, байршил тогтоох мэдрэгч, аюул илрүүлэх логик, байгаль орчны сорилт, өгөгдлийн хяналт — зэргийг нэгтгэн авч үзэв.

4.1. Холбоо ба удирдлагын систем.

Холбоо ба удирдлагын дэд систем нь дрон болон хяналтын төвийн хооронд хоёр чиглэлтэй өгөгдөл дамжуулах үүрэгтэй. Хяналтын төвөөс нислэгийн команд илгээгдэж, дрон байрлал, хурд, батерейны түвшин зэрэг телеметрийн мэдээллийг бодит цагт буцаана. Холбооны найдвартай ажиллагааг хангахын тулд **LTE/4G/5G** болон **радио давтамжийн (RF)** сувгийг хослуулсан **fail-safe communication** бүтэц ашиглагдана. Энэ нь үндсэн сүлжээ тасарсан үед RF сувгаар мэдээлэл үргэлжлэх нөхцөл бүрдүүлдэг. Удирдлагын хэсэг нь нислэгийн төлөвлөгөөг боловсруулж дрон руу илгээх, гүйцэтгэлийг хянах бөгөөд **bidirectional control protocol** ашигласнаар команд баталгаажиж өгөгдлийн алдагдлаас сэргийлдэг. Хяналтын програм хангамж нь **Python** эсвэл **C++** хэлээр боловсруулагдсан серверийн модуль хэлбэртэй бөгөөд даалгавар боловсруулах, команд баталгаажуулах, телеметрийн өгөгдөл дүрслэх, ослын хамгаалалт идэвхжүүлэх зэрэг үйлдлийг гүйцэтгэнэ.

4.2. Байршил тогтоох ба мэдрэгчийн систем.

Дрон хүргэлтийн системийн үндсэн нөхцөл нь байршлыг өндөр нарийвчлалтай тогтоох, орчны мэдээллийг тасралтгүй үнэлэх явдал юм. Үүний тулд **GNSS** (GPS, GLONASS, Galileo, BeiDou)-ийн өгөгдлийг **sensor fusion** аргаар бусад мэдрэгчийн мэдээлэлтэй нэгтгэдэг. **IMU** хурдатгал, өнцгийн хурдыг; **барометр ба өндрийн мэдрэгч** даралтын өөрчлөлтөөр өндрийг; **магнетометр** чиг баримжаа тодорхойлно. **Оптик урсгалын мэдрэгч**, **лидар**, **ультра-дууны мэдрэгч** нь буулт болон саад илрүүлэлтийг сайжруулна. Эдгээрийг **EKF (Extended Kalman Filter)** алгоритмаар нэгтгэснээр GNSS-ийн алдааг засварлаж, байршлын мэдээллийг секунд бүр шинэчилж, салхи ба даралтын нөлөөг автоматаар нөхдөг.

4.3. Аюул илрүүлэх ба онцгой нөхцлийн шийдэл.

Нислэгийн явцад үүсэх техникийн болон орчны аюулыг илрүүлж хариу өгөх механизм системийн аюулгүй ажиллагааны үндэс юм. Лидар, радар, камерын мэдрэгч орчны саадыг тодорхойлж, **self-diagnostics** модуль мотор, батерей, мэдрэгчийн доголдлыг илрүүлдэг. Онцгой нөхцөлд автоматаар идэвхжих хамгаалалтын логик нь дараах үндсэн үйлдэлтэй: (1) батерей багасахад буцах цэгийг

автоматаар сонгох; (2) холбоо тасарвал хүлээлтийн дараа буцах эсвэл hover горимд шилжих; (3) GNSS алдаанд IMU-гаар чиг баримжаа хадгалах; (4) цаг агаарын хэт өөрчлөлт илэрвэл хамгаалалтын буулт хийх. Нэмж, гар удирдлагын нөөц горим ашиглагдаж, оператор бодит цагт нислэгийг хянах, зогсоох, чиг өөрчлөх боломжтой.

4.4. Байгаль орчны сорилтууд.

Температур, салхи, агаарын нягт, хур тунадас, цахилгаан орон зэрэг орчны нөхцөл нь дроны нислэгт шууд нөлөөлдөг. Хэт хүйтэн нөхцөлд батерейны хүчин чадал буурч, халуун орчинд хэт халалт үүсдэг тул температурын хязгаарт тохирсон нислэг төлөвлөх шаардлагатай. Салхи, даралтын өөрчлөлт нь тогтвортой байдалд нөлөөлөх тул хяналтын программд салхины хурдны хязгаар оруулна. Чийг, тоосжилт, цаснаас хамгаалахын тулд IP54 ба түүнээс дээш хамгаалалттай бүрхүүл, гидрофоб бүрхүүл хэрэглэнэ. Соронзон орон, цахилгаан шугамын нөлөөг багасгахын тулд IMU ба GPS-ийн өгөгдлийг нэгтгэн дундажлах алгоритм ашигладаг.

4.5. Нислэгийн хяналт ба өгөгдлийн дүн шинжилгээ.

Хяналтын систем нь нислэгийн параметрүүдийг бодит цагт бүртгэж, серверт дамжуулна. Байршил, хурд, өндрийн өөрчлөлт, батерей, холбооны чанарыг хянаж, хязгаараас хэтрэхэд анхааруулга илгээдэг. Бүх телеметрийн болон цаг агаарын өгөгдлийг *flight log* хэлбэрээр хадгалж, статистик болон машин сургалтын аргаар боловсруулснаар моторын гүйцэтгэл, батерейны элэгдэл, салхины нөлөөг урьдчилан таамаглах боломжтой. Ингэснээр систем “predictive maintenance” буюу урьдчилан засварын төлөвлөлт хэрэгжүүлэх чадвартай болж, тасалдал буурна. Нэгдсэн хяналтын самбар нь нислэгийн төлөв, гүйцэтгэл, хүргэлтийн тоо, замын урт, хугацааг нэг дэлгэцэнд харуулж, операторт бодит мэдээлэл дээр үндэслэн шийдвэр гаргах боломж олгоно.

Ийнхүү дронд суурилсан хүргэлтийн систем нь холбоо хяналт, мэдрэгчийн уялдаа, аюул илрүүлэх логик, орчны дасан зохицол, өгөгдлийн дүн шинжилгээний нэгдсэн технологийн шийдлүүдэд тулгуурлан найдвартай, тогтвортой ажиллагааг хангадаг.

V. ЗАМЫН ТООЦООЛОЛ, АЛГОРИТМЫН ТУРШИЛТ

Дронд суурилсан хүргэлтийн системийн гүйцэтгэлийг тодорхойлох хамгийн чухал элемент бол нислэгийн замын оновчлол юм. Замын тооцооллын зорилго нь дрон эхлэл ба хүрэх цэгийн хооронд хамгийн богино, аюулгүй, эрчим хүчний хувьд хэмнэлттэй маршрутыг тодорхойлох бөгөөд бодит орчны саад, салхи, батерейны хүчин чадал зэрэг нөхцөлүүдийг тооцдог динамик процесс юм.

5.1. Судалгааны зорилго ба асуудлын тодорхойлолт

Энэхүү судалгаанд замын оновчлолын дөрвөн алгоритмын (Dijkstra, A*, Energy-A*, RRT*) гүйцэтгэлийг тооцооллын хурд, замын урт, нээлттэй зангилааны тоо, эрчим хүчний хэрэглээ гэсэн үндсэн шалгууруар харьцуулан туршсан. Туршилт нь хоёр шаттайгаар явагдсан:

Offline орчин — алгоритмуудыг хиймэл 2D occupancy grid орчинд туршиж, тоон үр дүнг гаргах;

Симуляцийн орчин — PX4 SITL ба MAVSDK ашиглан бодит нөхцөлд ойролцоо орчинд маршрутын үр ашгийг баталгаажуулах.

Газрын зураг нь 40×40–100×100 хэмжээтэй occupancy grid хэлбэртэй бөгөөд нүд бүр “саадтай” (1) эсвэл “чөлөөтэй” (0) зайг илэрхийлнэ. Эхлэл ба хүрэх цэгийг диагональ байдлаар байрлуулж, салхи, саадын нягтрал зэрэг нөхцөлүүдийг өөрчилж олон хувилбар үүсгэсэн.

5.2. Алгоритмууд

Dijkstra алгоритм.

Хамгийн бага өртөгтэй замыг баталгаатайгаар гаргадаг сонгодог арга. Гэхдээ бүх зангилааг шалгадаг тул тооцооллын хугацаа урт, нөөцийн хэрэглээ өндөр. Жижиг талбайд тохиромжтой.

A алгоритм.*

Dijkstra-ийн heuristic сайжруулсан хувилбар. f = g + h функц ашиглан зорилт руу чиглэсэн хайлт хийдэг. Замын урт Dijkstra-тэй адил боловч тооцооллын хугацаа 40–60 %-иар бага тул бодит цагийн нислэгт хамгийн тохиромжтой.

Energy-A алгоритм.*

A* загварыг өргөжүүлж, салхи, батерей, жин, чиглэл зэрэг параметрийг energy cost function-д оруулсан хувилбар. Илүү богино биш ч эрчим хүчний хувьд хэмнэлттэй зам гаргадаг тул урт зайн хүргэлтэд илүү үр ашигтай.

RRT алгоритм.*

Санамсаргүй дээжлэлтийн зарчимд тулгуурлан том талбайд хурдан шийдэл олдог. Гэхдээ саад ихтэй, нарийн орчинд тогтворгүй зам үүсгэх хандлагатай.

Алгоритмуудыг сонгох гол зорилго нь тооцооллын үр ашиг, замын урт, эрчим хүчний хэрэглээ болон саадтай орчинд дасан зохицох чадварыг харьцуулан үнэлэхэд оршино.

5.3. Туршилтын орчин

1. Offline орчин:

Тооцооллын түвшинд алгоритмын гүйцэтгэлийг харьцуулах зорилготой. Газрын зураг нь 2 хэмжээст occupancy grid бөгөөд 40×40–100×100 хэмжээтэй торон талбайд саадын хувь 20–30 % байхаар тохируулсан. “Baseline,” “Dense,” “Corridor,” “Wind-opposed,” “Long-range” гэх таван хувилбар бүхий орчны загвар ашиглагдсан.

Хэмжсэн үзүүлэлтүүд:

- Замын дундаж урт (м)
- Тооцооллын хугацаа (сек)

- Нээлттэй зангилааны тоо
- Эрчим хүчний хэрэглээний индекс

ТУРШИЛТЫН ОРЧИН

1-р хүснэгт

Орчны төрөл	Тайлбар	Саадын нягтрал (%)	Нэмэлт нөхцөл
Baseline 40×40	Энгийн, саад багатай	20	—
Dense 40×40	Саад ихтэй орчин	30	—
Corridor 60×20	Нарийн замтай орчин	25	—
Wind-opposed 50×50	Салхины эсрэг нөхцөл	25	5 м/с эсрэг салхи
Long-range 100×100	Том талбайд чиглүүлэх	20	—

2. Симуляцийн орчин:

Бодит нөхцөлтэй ойролцоо виртуал орчинд туршилт хийж, offline дүнг баталгаажуулсан.

- Нислэгийн талбай: 100×100 м
- Өндөр: 30 м
- Салхины дундаж хурд: 3–4 м/с
- GPS, батерей, хугацааны өгөгдлийг бодит цагт бүртгэсэн.

Хэмжсэн үзүүлэлтүүд:

- Төлөвлөсөн ба бодит зам (м)
- Нислэгийн хугацаа (сек)
- Батерей хэрэглээ (мА·цаг)
- GPS-ийн зөрүү (м)

5.4. Offline туршилтын үр дүн

OFFLINE ТУРШИЛТЫН ҮР ДҮН

2-р хүснэгт

Алгоритм	Замын дундаж урт (м)	Тооцооллын хугацаа (сек)	Нээлттэй зангилаа (ширхэг)	Эрчим хүчний зардлын индекс*
Dijkstra	**55.3 ± 1.2**	**1.82 ± 0.15**	**1180**	**1.00**
A*	**54.9 ± 1.1**	**1.12 ± 0.10**	**640**	**0.97**
Energy-A*	**56.2 ± 1.3**	**1.47 ± 0.11**	**700**	**0.85**
RRT*	**58.4 ± 2.5**	**2.34 ± 0.21**	**—**	**0.95**

(*Dijkstra = 1.00 харьцангуй суурь)

Үр дүнгийн дүгнэлт:

- **Замын урт:** Dijkstra, A* ойролцоо үр дүнтэй байсан ч Energy-A* салхины эсрэг нөхцөлд илүү тогтвортой байж, нийт эрчим хүчний хэрэглээг 10–15 %-иар бууруулсан.
- **Тооцооллын хугацаа:** A* алгоритм Dijkstra-аас ≈45 % хурдан ажилласан. Energy-A* нэмэлт тооцоолол хийдэг ч дундаж хугацаанд багтсан.
- **Нээлттэй зангилааны тоо:** A* хамгийн бага зангилаа ашиглаж, хайлтын үр ашиг хамгийн өндөр байсан.
- **Эрчим хүчний хэрэглээ:** Energy-A* илүү урт зам гаргасан ч хамгийн бага батерей хэрэглэсэн.

Дүгнэлт:

Offline туршилтаар A* алгоритм тооцооллын хувьд хамгийн үр ашигтай, Energy-A* нь эрчим хүчний менежментэд илүү тохиромжтой болохыг баталсан.

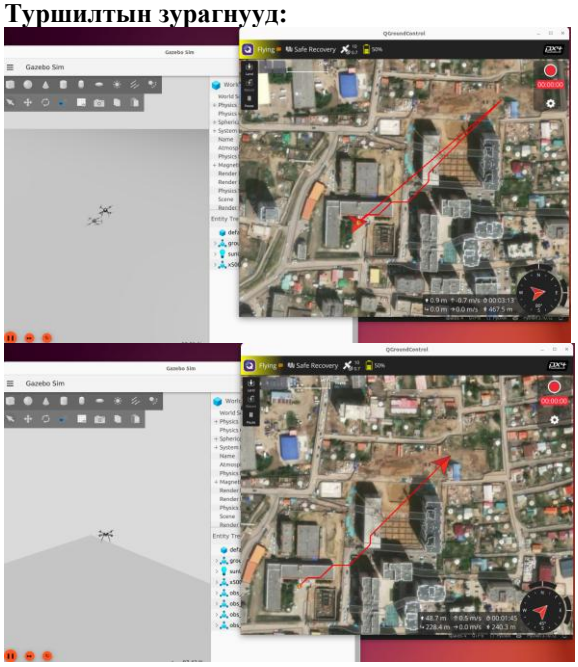
5.5 Симуляцийн туршилтын үр дүн

СИМУЛЯЦИЙН ТУРШИЛТЫН ҮР ДҮН

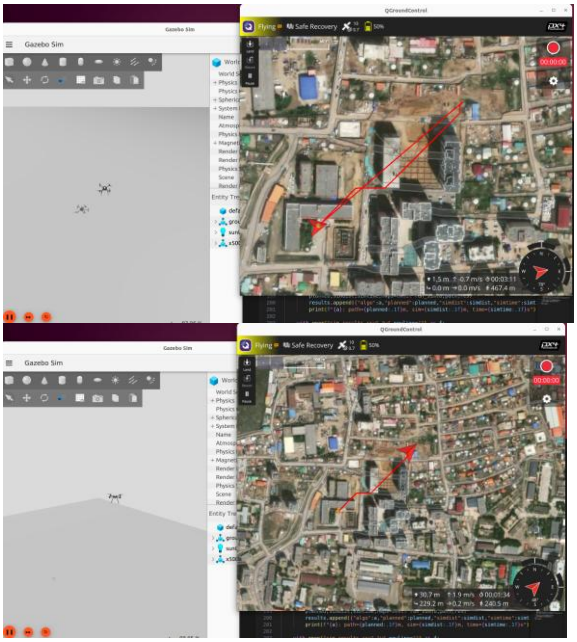
3-р хүснэгт

Алгоритм	Төлөвлөсөн зам (м)	Бодит нислэгийн зам (м)	Нислэгийн хугацаа (сек)	Батерей хэрэглээ (мА·цаг)	GPS зөрүү (м)
Dijkstra	**120.5**	**126.3**	**89.3**	**1820**	**±1.2**
A*	**118.7**	**122.0**	**77.8**	**1620**	**±0.8**
Energy-A*	**123.1**	**125.5**	**81.6**	**1560**	**±0.9**
RRT*	**129.0**	**134.6**	**94.2**	**1900**	**±1.4**

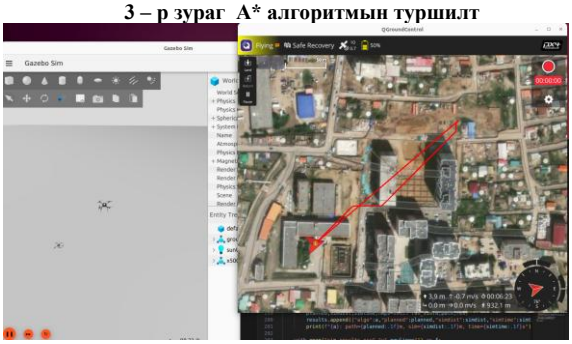
Туршилтын зурагнууд:



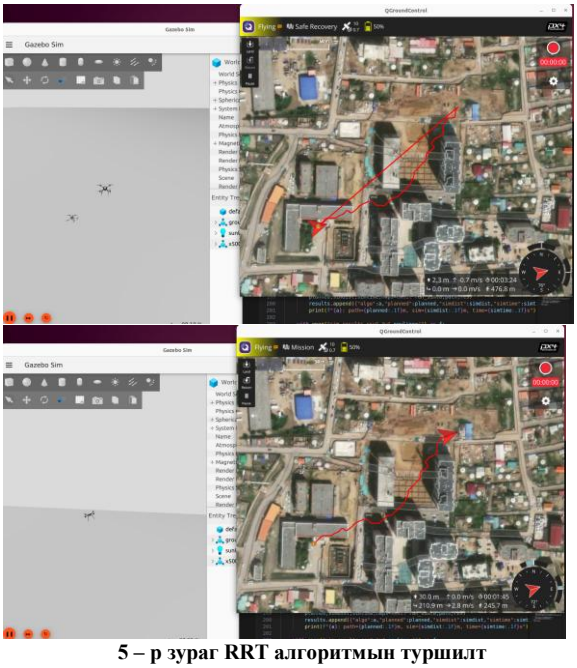
2 – р зураг Djikstra алгоритмын туршилт



3 – р зураг A* алгоритмын туршилт



4 – р зураг Energy-A* алгоритмын туршилт



5 – р зураг RRT алгоритмын туршилт

Төлөвлөсөн ба бодит зам:
Бүх алгоритмуудын бодит зам төлөвлөснөөс дунджаар 4–6 %-иар урт гарсан. A* хамгийн бага зөрүүтэй (≈2.8 %) байсан бөгөөд төлөвлөсөн ба бодит траектор бараг бүрэн давхцсан. Energy-A* ижил чиглэлтэй ч салхины эсрэг нөхцөлд илүү тогтвортой хурд хадгалсан. RRT* замын хэлбэлзэл ихтэй, олон “мушгиа” гаргасан нь хотын орчинд тохиромжгүйг харуулсан.

Нислэгийн хугацаа:
A* хамгийн богино хугацаанд зорилтот цэгт хүрч, Dijkstra-аас 12–15 % хурдан байсан. Energy-A* дундаж хугацаанд орсон, RRT* хамгийн удаан.

Батерей хэрэглээ:
Energy-A* хамгийн бага хэрэглээтэй (≈14 % хэмнэлт), A* дараагийн сайн үзүүлэлттэй. Dijkstra ба RRT* илүү их энерги зарцуулсан.

GPS зөрүү:
A* ба Energy-A* ±1 м-ээс бага зөрүүтэй байсан нь waypoint хяналтын нарийвчлал өндөр байгааг нотолсон. Dijkstra ба RRT* илүү хэлбэлзэлтэй (±1.2–1.4 м).

Дүгнэлт:
A* алгоритм бодит нислэгийн орчинд хамгийн тогтвортой, хамгийн богино зам гаргасан. Energy-A* илүү тогтвортой хурд, хамгийн бага батерей хэрэглээг үзүүлсэн. Dijkstra алгоритм баталгаатай ч хэт тооцоололтой, RRT* тогтворгүй байв.

5.6 Offline ба симуляцийн туршилтын дүгнэлт

Offline ба симуляцийн орчны нийлмэл үр дүнгээс дараах гол дүгнэлтүүд гарсан:

- **A*** алгоритм хамгийн оновчтой гүйцэтгэлтэй: Dijkstra-аас 45 % хурдан, замын урт ижил, зангилааны хэрэглээ 50 % бага.
- **Energy-A*** нь салхины эсрэг нөхцөлд 10–15 % эрчим хүчний хэмнэлт үзүүлж, батерей ашиглалтыг сайжруулсан.
- **Туршилтын нотолт:** бодит орчинд A* ба Energy-A* траекторууд төлөвлөсөн замтай бараг давхцаж, GPS зөрүү ≤ ±1 м байсан.
- **Дүгнэлт:** A* нь хурд ба замын оновчлолд, Energy-A* нь тогтвортой байдал ба энергийн менежментэд хамгийн тохиромжтой алгоритмууд юм.

Иймхүү туршилтын үр дүнгээр A* болон Energy-A* алгоритмууд дронд суурилсан хүргэлтийн системд хамгийн үр ашигтай, бодит нөхцөлд хэрэгжих боломжтой шийдэл болохыг нотоллоо. Системийн зорилгоос хамааран хурд ба тогтвортой байдлын тэнцвэрийг **A*** , **Energy-A***алгоритмуудаар авж болно.

VI. МОНГОЛД ДРОНД СУУРИЛСАН ХҮРГЭЛТИЙН СИСТЕМИЙГ ХЭРЭГЖҮҮЛЭХ БОЛОМЖ БА УЯЛДАА

6.1. Монголын нөхцөл байдал, онцлог

Монгол Улсын газарзүй, уур амьсгал, хот төлөвлөлтийн онцлог нь дронд суурилсан хүргэлтийн системийг нутагшуулахад техникийн болон зохион байгуулалтын хязгаар үүсгэдэг. Тиймээс системийн загвар нь эдгээр нөхцөлд тохируулан инженерийн түвшинд оновчтой төлөвлөгдөх шаардлагатай.

Газарзүйн болон агаартай холбоотой хүчин зүйл.

Улаанбаатар хот далайн түвшнээс 1300–1400 м өндөрт байрладаг тул агаарыг харьцангуй сийрэг болгож, сэнсний түлхэлт ба батерейны үр ашгийг бууруулдаг. Үүний нөлөөгөөр нислэгийн хугацаа богиносож, хүргэлтийн зай хязгаарлагддаг. Иймээс нөхцөлд дроны моторын хүчин чадал, батерейны багтаамжийг илүү өндөр стандарттайгаар тооцох шаардлагатай.

Уур амьсгалын нөлөө.

Өвөл −30 °C хүртэл хүйтэрч, батерейны багтаамж 30–50 %-иар буурдаг. Салхи тогтмол, хүчтэй, хонхор бүсэд урвуу урсгал үүсгэдэг нь нислэгийн тогтвортой байдалд сөргөөр нөлөөлнө. Иймээс дронд батерей халаах систем, салхины илрүүлэгч, хурд хязгаарлагч хамгаалалтын логик зайлшгүй хэрэгтэй.

Хотын дэд бүтэц ба буулт-хөөрөлт.

Барилгын өндөр, цахилгааны болон холбооны шугамын ил байршил нь буулт хийхэд хүндрэл үүсгэдэг. Тиймээс хүргэлтийн маршрутын төлөвлөлт зөвхөн зайгаар бус буулт хийх аюулгүй цэгийн байршлаар тодорхойлогдох ёстой. Гео-хашаалалт, автомат буулт-хөөрөлтийн талбайн төлөвлөлт чухал ач холбогдолтой.

Харилцаа холбоо ба удирдлагын орчин.

Монголд 4G сүлжээ өргөн тархсан ч 5G зөвхөн төвийн дүүрэгт бий. BVLOS (алсын удирдлага) нислэгт мэдээллийн саатал гарах магадлалтай. Иймд системийг GNSS болон дотоод мэдрэгчийн нэгтгэлд тулгуурлан ажилладаг, хоёр түвшний (анхан + нөөц) холбоотой болгох шаардлагатай.

Хууль эрх зүйн орчин.

Нисгэгчгүй төхөөрөмжийн үйл ажиллагааны журам бүрэн боловсроогүй. Олон нийтийн аюулгүй байдал, нууцлал, зөвшөөрлийн хүрээ тодорхой бус байгаа нь дрон хүргэлтийг эхний шатанд туршилтын түвшинд, гео-хашаалалттай бүсэд хэрэгжүүлэхийг шаардана.

Дүгнэлт.

Монголын нөхцөлд дрон хүргэлтийн системийг төлөвлөхдөө дараах үндсэн хүчин зүйлсийг зайлшгүй тооцох ёстой:

- өндөрлөг агаартай орчны нөлөө → мотор ба батерейны тохируулга,
- эрс тэс уур амьсгал → дулаалга ба нислэгийн горим,
- хотын бүтэц → аюулгүй буултын талбай,
- холбоо ба зохицуулалт → найдвартай давхар удирдлага.

Эдгээрийг инженерийн шийдлээр (батерей халаалт, салхи илрүүлэлт, гео-хашаалалт, backup холбоо) хослуулснаар системийг Монголд амжилттай хэрэгжүүлэх бүрэн боломжтой.

6.2. Дроны сонголт

Монголын нөхцөлд дунд зайн хүргэлтэд **олон сэнст (multirotor)** дрон илүү тохиромжтой. Hexacopter, octocopter төрлийн дрон нь 5–8 кг даацтай, 10–15 км радиуст хүргэлт гүйцэтгэх чадвартай бөгөөд барилга хоорондын нарийн орчинд босоо хөөрөлт, буулт хийж чаддаг. Нислэгийн хугацаа 25–35 минут, хурд 70 км/цаг орчим бөгөөд −20 °C хүртэл ажиллах чадвартай хос батерейны системтэй байвал хамгийн тохиромжтой.

САНАЛ БОЛГОХ MULTIROTOR ТӨРЛИЙН ДРОНУУД

4-Р ХҮСНЭГТ

Дрон загвар	Үйлдвэрлэгч	Үндсэн үзүүлэлт	Тайлбар
DJI Matrice 350 RTK	DJI	Даац 6 kg / нисэх хугцаа 55 min / нислэгийн урт 20 km	Хүйтэн нөхцөлд –20 °C хүртэл ажиллах чадвартай, хоёрдогч батерейтай. Хотын дунд зайн хүргэлтэд хамгийн тохиромжтой.
DJI Matrice 300 RTK	DJI	Даац 5.9 kg / нисэх хугцаа 45 min / нислэгийн урт 15 km	Мэргэжлийн зураглал, хүргэлтийн платформ; олон мэдрэгчийн дэмжлэгтэй.
Freefly Alta X	Freefly Systems	Даац 15 kg / нисэх хугцаа 30 min / нислэгийн урт 15 km	Өндөр хүчин чадалтай, батерейг хослуулан ашигладаг; дунд – хүнд даацын хүргэлтэд тохиромжтой.
Inspired Flight IF1200A	Inspired Flight	Даац 8 kg / нисэх хугцаа 43 min / нислэгийн урт 20 km	Нээлттэй эхийн PX4-д нийцдэг, арилжааны зориулалттай олон сэнст дрон.

Хот хоорондын болон урт зайн хүргэлтэд **VTOL (fixed-wing hybrid)** төрлийн дрон илүү тохиромжтой. Тэдгээр нь 70–120 км хүртэл нислэгийн урттай ч илүү том буултын талбай шаарддаг тул орон нутгийн хүргэлтэд тохиромжтой.

САНАЛ БОЛГОХ FIXED-WING ТӨРЛИЙН ДРОНУУД

5-Р ХҮСНЭГТ

Дрон загвар	Үйлдвэрлэгч	Үндсэн үзүүлэлт	Тайлбар
Wingcopter 198	Wingcopter	Даац 6 kg / нислэгийн урт 75 km / хурд 100 km/h	Hybrid VTOL; автоматаар буух, хөөрөх чадвартай; дунд-урт зайн хүргэлтэд тохиромжтой.
Quantum-Systems Trinity Pro	Quantum Systems	Даац 3 kg / нислэгийн урт 100 km / хурд 90 min	Fixed-wing VTOL; урт нислэгийн хугацаатай, хөнгөн хүргэлтэд тохиромжтой.
Zipline P2 Zip	Zipline	Даац 8 kg / нислэгийн урт 90 km / хурд 110 km/h	Эрүүл мэндийн хүргэлтэд ашиглагдаж буй баталгаатай систем; BVLOS (алсын удирдлага) ажиллагаанд туршигдсан.
Vertical Technologies DeltaQuad Pro EV	Vertical Tech	Даац 2 kg / нислэгийн урт 120 km / хурд 100 min	Нээлттэй эхийн PX4 системтэй VTOL; сургалт, судалгаанд өргөн хэрэглэгддэг.

Байгаль орчин болон экологийн нөлөө

Дронууд цахилгаан хөдөлгүүртэй тул нислэгийн үеэр CO_2 ялгаруулдаггүй. Улаанбаатарт автомашин 10 км хүргэлтэд 2000–2800 г CO_2 ялгаруулдаг бол ижил даалгавар гүйцэтгэх дрон ≈350 г CO_2-д тэнцэх эрчим хүч хэрэглэдэг.

ТЭЭВРИЙН ХЭРЭГСЛИЙН НҮҮРСТӨРӨГЧИЙН ЯЛГАРУУЛАЛТЫН ХАРЬЦУУЛАЛТ

6-Р ХҮСНЭГТ

Хүргэлтийн төрөл	Түгжрэлгүй үед CO_2 ялгаруулалт (г/10 км)	15 минутын саатлын үед CO_2 ялгаруулалт (г/10 км)	Тайлбар
Автомашин (жижиг суудлын)	**2 000 г**	**2 800 г**	Дундаж түлшний зарцуулалт 9 л/100 км; түгжрэлийн үед 30–40 %-иар нэмэгддэг.
Мотоцикл (150 cc)	**1 000 г**	**1 200 г**	Түлшний зарцуулалт 3–4 л/100 км; түгжрэлд бага хугацаанд саатдаг.
Олон сэнст дрон (5–8 кг даацтай)	**350 г**	**350 г**	Цахилгаан хөдөлгүүр; нислэгийн үеийн шууд ялгаруулалт үгүй, эрчим хүчний хэрэглээнээс үүссэн дундаж тооцоо.

Энэ нь дрон хүргэлтийн системийг ашигласнаар CO_2 ялгарлыг 80–88 %-иар бууруулах боломжтойг харуулж байна. Өдөрт 1000 хүргэлт хийдэг гэж тооцвол ≈2–2.5 тонн CO_2-ийн ялгарлыг өдөр бүр хэмнэнэ. Хэрэв дронуудыг нарны эсвэл сэргээгдэх эрчим хүчээр цэнэглэвэл уг ялгаруулалт бараг бүрэн арилна. Иймээс дрон хүргэлтийн систем нь хүрээлэн буй орчны бохирдлыг бууруулах бодит инженерийн шийдэл юм.

6.3. Монголд хэрэгжүүлэх үе шат, дэд бүтэц

Монголд дрон хүргэлтийн системийг үе шаттайгаар хөгжүүлэх нь хамгийн оновчтой арга юм.

МОНГОЛ УЛСАД ХЭРЭГЖҮҮЛЭХ ҮЕ ШАТ

7-Р ХҮСНЭГТ

Үе шат	Гол зорилго	Хэрэгжүүлэх хүрээ	Түлхүүр үйл ажиллагаа
I. Туршилтын үе шат	Технологийн туршилт, нислэгийн зөвшөөрөл, маршрутын баталгаажуулалт	Хязгаарлагдмал бүс (жишээнь: Налайх, Сонгинохайрхан дүүргийн захын хэсэг)	Нислэгийн хяналтын төв байгуулах, туршилтын нислэг гүйцэтгэх, гео-хашаалалт болон GPS тохиргоо хийх, анхан шатны маршрутын өгөгдөл цуглуулах
II. Хязгаарлагдмал үйлчилгээний үе шат	Хөнгөн 2–5 кг-ын хүргэлтийг туршилтаас үйлчилгээний түвшинд шилжүүлэх	Хот дотор, тодорхой маршрутын хүрээнд	Хүргэлтийн төв байгуулах, хэрэглэгчийн аппликейшн хөгжүүлэх, аюулгүйн ажиллагааны туршилт, автомат нислэгийн горимыг тогтворжуулах
III. Бүрэн хэмжээний үйлчилгээний үе шат	Хот хооронд болон хот доторх олон төвийн уялдаа бүхий хүргэлтийн сүлжээ бий болгох	Улаанбаатар болон Улаанбаатар артай ойрхон аймаг, сум	Нэгдсэн хяналтын платформ нэвтрүүлэх, BVLOS (Beyond Visual Line-of-Sight) нислэгийг хэрэгжүүлэх, батерей цэнэглэх ба солих станцуудыг байгуулж өргөтгөх

Эдгээр үе шат нь технологи, эрх зүй, хэрэглэгчийн итгэлцлийг зэрэг хөгжүүлэхэд чиглэнэ.

Гол дэд бүтэц.

Хяналтын төв: Дронуудын нислэгийг бодит цагт хянах, ослын үед автоматаар мэдэгдэх, олон дроны өгөгдлийн урсгалыг төвлөрүүлэх үүрэгтэй.

Буулт, хөөрөлтийн талбай: Барилгын дээвэр, агуулахын талбайд байрлуулж, IP54 хамгаалалт, гео-хашаалалт, хурдан цэнэглэх станцтай байна.

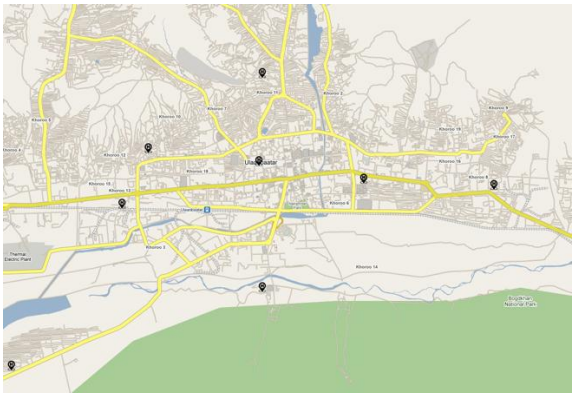
Харилцаа холбоо: 4G/5G сүлжээг ашиглах, backup RF холболттой fail-safe горим хэрэгжүүлэх.

Гео-хашаалалт ба зохицуулалт: Төрийн ордон, онгоцны буудал зэрэг хориг бүсийг координатаар системд урьдчилан бүртгэх.

Буулт-хөөрөлтийн байрлалын санал.
Судалгааны дүнгээр Улаанбаатар хотыг цагираг байдлаар 6–7 стратегийн цэгээр хамарвал 10–15 км радиуст бүхий үйлчилгээний сүлжээ бүрдэнэ:

1. Төв хяналтын зангилаа (вокзал орчим),
2. Баруун талбай (3–4-р хороолол),
3. Хойд талбай (Дэнжийн мянга),
4. Зүүн талбай (Амгалан),
5. Зайсангийн бүс,
6. Яармаг–Буянт-Ухаа орчим,
7. Нөөц талбай (Гандангийн доод хэсэг).

Ийм бүтэц нь хотын төв, зах, шинэ хорооллыг хамарч, нэг нислэгийн хүрээнд нийт хүргэлтийн маршрутыг гүйцэтгэх боломж олгоно.



6 – р зураг дээрх тэмдэглэгээний тайлбар

Системийн үйл ажиллагааны дарааллын зураглал

Дронд суурилсан хүргэлтийн системийн үйл ажиллагаа нь хэрэглэгчийн захиалгыг хүлээн авах, маршрутыг тооцоолох, нислэгийг гүйцэтгэх, хүргэлтийг баталгаажуулах зэрэг шаталсан урсгалтай. **7-р зураг** хэрэглэгчийн түвшний урсгалыг, **8-р зураг** инженерийн буюу дотоод системийн үйл явцыг тус тус харуулсан. Эхнийх нь хүргэлтийн процессийн гаднах үе шатыг, хоёр дахь нь сервер, дрон, хяналтын төвийн мэдээллийн уялдаа ба хяналтын урсгалыг илэрхийлнэ. Энэ хоёр түвшний загварын уялдаа нь системийн автомат ажиллагааг бүрдүүлж, Монголын нөхцөлд найдвартай хэрэгжилтийн үндэс болно.

7-р зураг. Хэрэглэгчийн талаас харсан дрон хүргэлтийн процесс

8-р зураг. Инженерийн талаас харсан системийн урсгал ба дэд бүтэц

СОРИЛТ БА ШИЙДЭЛ

7-Р ХҮСНЭГТ

Сорилт	Нөлөөлөл	Боломжит шийдэл
Хүйтэн уур амьсгал ба салхи	Батерейны багтаамж буурах, нислэгийн тогтворгүй байдал	Температурын хамгаалалттай батерей, давхар тэжээлийн систем, салхины хурд илрүүлэх мэдрэгч суурилуулах
Хотын нягт барилга ба GPS ийн хязгаарлалт	Байршлын алдаа, гео-хашааны зөрчил үүсэх	Хосолсон мэдрэгч суурилсан байршлын фьюжн (GPS + IMU + барометр), дүрс боловсруулах навигаци ашиглах
Зохицуулалтын тодорхойгүй байдал	Нислэгийн зөвшөөрөл ба хариуцлагын тодорхой гүйцэтгэл	ИНЕГ-тэй хамтран туршилтын бүс тодорхойлох, байнгын зөвшөөрөл авах журам боловсруулах
Холбооны саатал эсвэл тасалдал	Дрон удирдлагын алдаа, ослын эрсдэл	Давхар холболт (primary + backup link), автомат буцах (Return-to-Home) горим идэвхжүүлэх
Хэрэглэгчийн итгэлцэл ба нийтийн ойлголт	Үйлчилгээний хүлээн зөвшөөрөл бага, аюулгүй байдалдаа болгоомжлох	Хүргэлтийн ил тод мэдээлэл, GPS-ээр дагах аппликейшн, нийтийн сургалт болон демо нислэгийн үзүүлэлт

ДҮГНЭЛТ

Энэхүү судалгаагаар дронд суурилсан хүргэлтийн системийг Монгол Улсад хэрэгжүүлэх техникийн болон зохион байгуулалтын боломжийг судалж, үндсэн загварыг боловсруулаа. Судалгааны үр дүнгээс харахад Улаанбаатар хотын уур амьсгал, газар зүйн онцлог, дэд бүтцийн нөхцөлийг тооцсон тохиолдолд хүргэлтийн зориулалттай олон сэнст дрон ашиглах нь техник, үйл ажиллагааны хувьд боломжтой шийдэл юм. GNSS ба гео-хашаалалт хосолсон зам тооцооллын систем, A* болон Energy-A* алгоритмын үндсэнд суурилсан маршрутын төлөвлөлт нь хотын орчинд тогтвортой, эрчим хүчний хувьд хэмнэлттэй ажиллаж байгааг симуляцийн үр дүн харуулсан. Хяналт-удирдлагын төв, батерей солих станц, буулт-хөөрөлтийн талбай зэргийг үе шаттайгаар хөгжүүлэх замаар хотын доторх хүргэлтийн сүлжээг бүрдүүлэх боломжтой бөгөөд энэ нь замын түгжрэлийг бууруулах, CO_2 ялгаруулалтыг багасгах давуу талтай. Иймд Монголын нөхцөлд дрон хүргэлтийн системийг инженерчлэлийн хувьд хэрэгжүүлэх бүрэн боломжтой гэж үзэж байна.

АШИГЛАСАН МАТЕРИАЛ

[1] Mohamed, A., & Mohamed, M. (2025). *Unmanned Aerial Vehicles in Last-Mile Parcel Delivery: A State-of-the-Art Review.* Drones, 9(6), 413. DOI: 10.3390/drones9060413. MDPI

[2] Jazairy, A., & Al-Hassan, A. (2024). *Drones in Last-Mile Delivery: A Systematic Review on Efficiency, Accessibility and Sustainability.* International Journal of Logistics Management, 36(7), 1-26. DOI: 10.1108/IJLM-03-2023-0273. Emerald

[3] Aurambout, J.-P., Gkoumas, K., & Ciuffo, B. (2019). *Last-mile delivery by drone: an estimation of viable market and environmental potential.* European Transport Research Review, 11, 36. DOI: 10.1186/s12544-019-0368-2. SpringerOpen

[4] Persson, E. (2021). *A Systematic Literature Review on Drones' Application in Last-Mile Delivery.* [Master's Thesis, Malmö University]. Retrieved from Diva Portal. Diva Portal

[5] Garcia, O., Santoso, J. (2019). *Comparative Evaluation of Drone Delivery Systems in Last-Mile Logistics.* Proceedings, MIT DSpace. DSpace

[6] Qin, C., Narayanan, A., & Pournaras, E. (2025). *Coordinated Multi-Drone Last-mile Delivery: Learning Strategies for Energy-aware and Timely Operations.* arXiv preprint arXiv:2509.15830. arXiv

[7] Hong, F., Wu, G., Luo, Q., Liu, H., Fang, X., & Pedrycz, W. (2022). *Logistics in the Sky: A Two-phase Optimization Approach for the Drone Package Pickup and Delivery System.* arXiv preprint arXiv:2204.01335. arXiv

[8] Grofelnik, I., et al. (2022). *Drone Last Mile Delivery: An Assessment of the Viable Market and Security Potential of Drone Delivery.* Ekonomski Vjesnik, 35(2), 337-351. ojs.srce.hr

[9] Su, E., Qin, H., Li, J., Zhang, R. (2025). *The Freight Multimodal Transport Problem with Buses and Drones: An Integrated Approach for Last-Mile Delivery.* arXiv preprint arXiv:2506.10311. arXiv

[10] "Operation Zenith." (2018). *Demonstration of Unmanned Aerial Vehicle and ATM Integration.* Retrieved from Wikipedia. Wikipedia

[11] Government of Mongolia, Civil Aviation Authority. (2024). *Нисгэгчгүй нисэх төхөөрөмжийн нислэгийн журам (Эрх зүйн акт)*. Улаанбаатар. Хууль

[12] PX4 Autopilot. (2024). *PX4 User Guide: Mission Planning, Geofencing and Failsafe Logic.* https://docs.px4.io

[13] QGroundControl Development Team. (2024). *QGroundControl Documentation: Mission Upload and Telemetry Monitoring*.https://docs.qgroundcontrol.com

[14] MAVSDK Team. (2024). *MAVSDK Guide for PX4 SITL Simulation and Mission Execution*. https://mavsdk.mavlink.io

5G/WI-FI ХОЛИМОГ СҮЛЖЭЭНД МЭДЭЭЛЛИЙН АЧААЛЛЫГ ШИЛЖҮҮЛЭХ БОЛОМЖ, ТҮҮНИЙ ҮР АШГИЙН СУДАЛГАА

Рагчаагийн БАЯРМАА[1], Бат-Аюушийн АЗЖАРГАЛ[2]

[1,2]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Холбооны инженерчлэлийн тэнхим

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

Хураангуй: **5G сүлжээн дэх траффик оффлоудинг нь тодорхой дата урсгалыг үүрэн сүлжээний цөм ба магистраль хэсгээс Wi-Fi-ийн захын зангилаа зэрэг өөр төрлийн хандалтын зам руу чиглүүлэн дамжуулах боломжийг бүрдүүлдэг. Ийм арга нь сүлжээний ачааллыг бууруулж, эсийн захын хамрах хүрээг сайжруулан, QoS (Quality of Service)-ийг дээшлүүлж, үйл ажиллагааны зардлыг хэмнэх давуу талтай. 5G–Wi-Fi оффлоудинг нь лицензгүй давтамжийн зурвасыг ашигласнаар нэмэлт багтаамж бий болгож, өгөгдлийн саадыг бууруулдаг. 5G-ийн нэвтрэлт өргөжиж буй өнөө үед Wi-Fi-ийн өргөн хамрах хүрээ, өртгийн хувьд үр ашигтай байдал нь үүрэн сүлжээний стратегийн салшгүй хэсэг болж байна. LTE-U болон Licensed Assisted Access (LAA) зэрэг сүүлийн үеийн шийдлүүд нь 5 GHz зурваст Carrier Sense Adaptive Transmission (CSAT)-ыг ашиглан үүрэн/Wi-Fi-ийн хамтран орших нөхцөлийг бүрдүүлдэг бөгөөд эдгээр нь 3GPP-ийн Release 12 болон Release 14-д стандарчлал хийгдсэн. Зөв зохион байгуулсан оффлоудинг нь тасралтгүй, зардал багатай холболтыг хангахад нэн чухал. Миллиметрийн долгионы (mmWave) нэвтрэлтийн хүндрэлүүдийг харгалзан үзвэл дотор болон захын бүсийн хамрах хүрээг өргөтгөхөд Wi-Fi-ийн байршуулалт зайлшгүй шаардлагатай. Мөн машин-машинд (M2M) болон өргөн хүрээний машин-төрлийн харилцаа (mMTC) эрчимтэй өсөж буй нь 5G орчинд тасралтгүй холболтын чухлыг улам бүр нэмэгдүүлж байна. Ухаалаг хот болон IoT санаачилгууд тэлж буй өнөөгийн нөхцөлд Wi-Fi оффлоудинг нь 5G сүлжээний гол идэвхжүүлэгч хүчин зүйл болжээ. Улаанбаатар хотын өндөр хөдөлгөөний нягтралтай бүс болох Сүхбаатарын талбай орчимд хийсэн бодит орчны туршилтын үр дүнд 5G/Wi-Fi HetNet орчинд оффлоудинг хэрэгжүүлснээр 5G секторын ачаалал ~90 %-иас 65 %-д буурч, Wi-Fi сувгийн ашиглалт 40 %-иас 65 %-д өссөн байна. Үүний зэрэгцээ дундаж QoS индекс 0.42-оос 0.71 болж, Voice-over-IP (MOS) чанар 3.2-оос 4.1 болж сайжирсан нь ухаалаг траффик оффлоудинг нь хэрэглэгчийн туршлага болон сүлжээний үр ашигт өндөр эерэг нөлөө үзүүлдгийг харуулж байна.**

Түлхүүр үг: IFOM, ATSSS, ANDSF, LBO, Wi-Fi оффлоудинг, миллиметрийн долгион (mmWave)

I. ОРШИЛ

Өндөр нягтаршилтай видео стриминг, IoT хэрэглээ, ухаалаг хотын үйлчилгээний эрчимтэй өсөлт нь үүрэн сүлжээний ачааллыг урьд өмнө байгаагүй өндөр түвшинд хүргэж байна. 5G технологийн нэвтрэлт өргөжин тэлж буй өнөө үед операторууд оргил хэрэглээний үе дэх бөглөрөл, үйл ажиллагааны зардлыг бууруулж, сүлжээний чанарыг тогтвортой хадгалах гэсэн хос сорилттой тулгарч байна. Сайжруулсан спектрийн үр ашигтай байсан ч уламжлалт 5G макро эсийн байршуулалт нь эсийн захын бүс болон хүн амын нягтаршил өндөртэй хотын орчинд өндөр өгөгдлийн хурд, тогтвортой холболтыг хангахад бэрхшээлтэй хэвээр байна. Эдгээр сорилтыг шийдвэрлэх үр дүнтэй чиглэлийн нэг нь траффик оффлоудинг бөгөөд энэ нь сонгогдсон өгөгдлийн урсгалыг үүрэн цөм сүлжээнээс Wi-Fi зэрэг хувилбар хандалтын сүлжээнд чиглүүлэн дамжуулах стратеги юм. Лицензгүй зурвасыг ашигласнаар Wi-Fi оффлоудинг нь нэмэлт багтаамж бий болгож, лабораторийн орчинд төвлөрсөн бөгөөд бодит хотын орчинд хийгдсэн туршилтын нотолгоо хомс байна. Энэ судалгаа дээрх цоорхойг нөхөх зорилгоор Улаанбаатар хотын хамгийн их ачаалалтай бүсүүдийн нэг болох Сүхбаатарын талбайд 5G/Wi-Fi оффлоудинг механизмын талбарын туршилт, гүйцэтгэлийн үнэлгээг хийсэн. Судалгаанд IFOM, ATSSS, ANDSF, LBO зэрэг механизмуудын гүйцэтгэлийг оргил ачааллын үед QoS, VoIP-ийн дундаж үнэлгээ (MOS), Wi-Fi дотоод болон халуун цэгийн (hotspot) орчинд өртөг багатайгаар хамрах хүрээг өргөтгөх боломж олгодог. Энэ ойлголтыг 3GPP, IEEE, ITU-T, Wi-Fi Alliance зэрэг стандартчиллын олон байгууллага дэмжиж, тэдгээрийн үр дүнд гибрид 5G/Wi-Fi гетероген сүлжээ (HetNet)-ийн хөгжүүлэлт хурдацтай явагдаж байна. Сүүлийн үеийн стандартчиллын ахиц дэвшил болох 3GPP Release 10 дахь IP Flow Mobility (IFOM), Release 11 дахь Access Network Discovery and Selection Function (ANDSF), Local Breakout (LBO), мөн Release 16-д танилцуулагдсан Access Traffic Steering, Switching, and Splitting (ATSSS) зэрэг нь 5G болон Wi-Fi орчныг саадгүй уялдуулах боломжийг бүрдүүлсэн. Эдгээр механизмууд нь хэрэглэгчийн төхөөрөмжид (UE) бодит цагийн холбоосын чанар, бодлогын дүрэм болон үйлчилгээний шаардлагад үндэслэн сүлжээнүүд хооронд траффикийг чиглүүлэх, хуваах, эсвэл шилжүүлэх боломжийг олгодог. Гэвч өнөөгийн судалгаануудын ихэнх нь симуляци эсвэл хяналттай

сувгийн ашиглалт, 5G секторын ачааллын бууралт зэрэг гол үзүүлэлтээр харьцуулан шинжилсэн.

Энэхүү ажлын гол хувь нэмэр нь дараах байдалтай:

Монгол Улсад бодит 5G/Wi-Fi HetNet орчинд 3GPP стандартчилсан оффлоудингийн хүрээг ашиглан гүйцэтгэлийн анхны бодит үнэлгээг хийсэн;

Ухаалаг траффик чиглүүлэлт нь хэрэглэгчийн туршлага сайжруулахын зэрэгцээ 5G-ийн ачааллыг 25 % хүртэл бууруулж болохыг QoS болон MOS-ийн тоон үзүүлэлтээр харуулсан;

Хүн амын нягтралтай ухаалаг хотын орчинд гибрид 5G сүлжээний гүйцэтгэлийг оновчтой болгох практик загварчлалын зөвлөмжүүдийг санал болгосон.

II. ХОЛБОГДОХ СУДАЛГААНУУД

Сүүлийн үеийн судалгаанууд 5G/Wi-Fi гетероген сүлжээн дэх траффик оффлоудинг болон олон хандалтын уялдаа холбоог алгоритмын, архитектурын болон тээврийн үе давхаргын (transport layer) үүднээс өргөн авч үзжээ. [1]-д 5G гетероген сүлжээний нийтлэг орчинд Wi-Fi оффлоудингийн бөглөрөлд мэдрэмтгий алгоритмыг танилцуулж, загварчлалын нөхцөлд дамжуулах хурд болон ачаалал тэнцвэржүүлэх үзүүлэлт сайжирсан болохыг харуулсан. Wi-Fi оффлоудинг ба жижиг эсүүдийн хамтын ажиллагааны харьцуулсан судалгааг [2]-т танилцуулсан бөгөөд жижиг эсүүдийн зохицуулсан ажиллагаа нь макро эсийн бөглөрлийг бууруулахад нэмэлт үр ашигтай болохыг тогтоосон. 3GPP хүрээнд [3]-т ATSSS-д зориулсан олон үйлчилгээт траффик төлөвлөлтийн аргыг санал болгосон бол [5], [7]-д олон төрлийн радио хандалтын технологийг зэрэг ашиглах боломж болон түүний хэрэгжилтийн сорилтыг авч үзсэн. Мөн [8]-д салбарын түвшний судалгаагаар найдвартай Wi-Fi хандалт болон 5G нэгдсэн цөм нь өргөн цар хүрээтэй ATSSS хэрэгжилтийг хангахад гол үүрэгтэй болохыг онцолсон. Тээврийн үе давхаргын түвшинд [4] нь 4G/5G/Wi-Fi системд MPTCP-д суурилсан олон замын нэгдэл (multipath aggregation)-ийн гүйцэтгэлийг үнэлж, дамжуулах хурд мэдэгдэхүйц сайжирч байгааг харуулсан. Харин [9] нь олон замын туннелчлэлтэй нөхцөлд давхцсан бөглөрөл хяналтын нөлөөллийг шинжилсэн. [10], [6]-д AI болон өртөг-үр ашиг сайтай нөөц хуваарилалт нь edge-cloud болон ATSSS-д суурилсан системд хэрхэн ажиллахыг судалсан бол [11]-д олон домэйны 5G орчинд найдвартай байдал, аудитын боломжийг хангахын тулд блокчэйн ашигласан аюулгүй оффлоудингийг авч үзсэн. Өмнөх судалгаануудын ихэнх нь [1]–[11] симуляци эсвэл лабораторийн хяналттай орчинд хийгдсэн тул 3GPP-ийн стандартизсан оффлоудинг механизмуудыг өндөр нягтаршилтай хотын бодит сүлжээний орчинд туршин нотолсон ажил хомс байна. Харин манай судалгаанд Улаанбаатар хотын өндөр ачаалалтай бүс болох Сүхбаатарын талбайд оргил цагийн нөхцөлд IFOM (Rel-10), ANDSF (Rel-11), LBO, ATSSS (Rel-16) зэрэг механизмуудыг 5G NR болон Wi-Fi 6 бодит дэд бүтцэд суурилан туршиж, харьцуулсан үнэлгээ хийв. Туршилтын бодит үр дүнд 5G секторын ачаалал ~90 %-иас 65 %-д буурч, Wi-Fi сувгийн ашиглалт 40 %-иас 70 %-д өссөн; дундаж QoS индекс 0.42-оос 0.71 болж нэмэгдэж, VoIP MOS нь 3.2-оос 4.2-т хүрч сайжирсан.

III. СИСТЕМИЙН АРХИТЕКТУР БА ТУРШИЛТЫН ОРЧИН

Уг туршилтын систем нь өндөр хэрэглээтэй хотын бодит нөхцөлд 5G/Wi-Fi гетероген сүлжээ (HetNet) орчин дахь бодит цагийн траффик оффлоудингийн гүйцэтгэлийг үнэлэх зорилгоор зохион байгуулагдсан. Ерөнхий архитектур нь 5G New Radio (NR) макро эс, Wi-Fi 6 (IEEE 802.11ax) хандалтын сүлжээ, мөн IFOM, ATSSS, ANDSF, LBO зэрэг 3GPP стандарт оффлоудинг механизмуудыг дэмжих олон хандалтын захын гарц (multi-access edge gateway)-аас бүрдэнэ.

A. Сүлжээний архитектур

Туршилтын орчинг Улаанбаатар хотын өндөр ачаалалтай бүсүүдийн нэг болох Сүхбаатарын талбайн орчимд байршуулсан бөгөөд энэ бүс нь оргил үеийн их нягт хөдөлгөөн, өндөр хэрэглээний онцлогтой. 5G хандалтын сүлжээ нь 3.5 GHz (n78) давтамжийн зурваст 100 MHz сувгийн өргөнтэй, хамгийн ихдээ 1.5 Gbps хүртэл буух хурдтайгаар ажиллав. Суурь станц (gNB) нь 5G цөм (5GC)-тэй оптик баекхаул шугамаар холбогдсон. Wi-Fi дэд систем нь 5 GHz, 80 MHz зурваст ажиллах гурван Wi-Fi 6 хандалтын төхөөрөмжөөс бүрдсэн бөгөөд эдгээрийг гудамжны түвшинд болон барилгын орох хэсэгт байршуулж, MU-MIMO дэмжлэгтэйгээр 1.2 Gbps хүртэл дамжуулах чадвартайгаар тохируулсан. Аль аль сүлжээ нь операторын орон нутгийн дата төвд хувьсах хандалтын захын тооцоолол (MEC) сервертэй холбогдсон бөгөөд энэхүү сервер нь оффлоудинг удирдлагын функц болон нутгийн breakout гарцыг агуулсан. Энэ нь хандалтын орчин хоорондох траффикийг бараг бодит цагийн горимоор чиглүүлэх болон бага сааталтай зам сонголтыг дэмжих боломжийг бүрдүүлэв.

B. Оффлоудинг удирдлагын хүрээ

Тухайн оффлоудингийн механизмуудыг 3GPP-ийн тодорхойлолтын дагуу тохируулсан:

IFOM (Rel.10): 5G болон Wi-Fi холболтыг зэрэг ажиллуулах давхар IP стек ашиглаж, IP давхаргад урсгал тус бүрээр чиглүүлэх боломжийг бүрдүүлсэн.

ATSSS (Rel.16): 5GC-ийн PCF болон UPF-д нэгтгэгдсэн бөгөөд олон замын дата хуваалт болон сешнд суурилсан удирдлагыг дэмжсэн.

ANDSF (Rel.11): Статик сүлжээ сонголтын бодлогыг UE-ийн бодлогын шинэчлэлээр түгээх байдлаар ашигласан.

LBO: Захын үйлчилгээний урсгалыг нутгийн түвшинд чиглүүлснээр цөм сүлжээг тойрох боломжийг бүрдүүлж, саатлыг бууруулав.

Траффик ангиллыг Deep Packet Inspection (DPI) ашиглан гүйцэтгэж, VoIP, видео стриминг болон бусад өгөгдлийн үйлчилгээний урсгалыг ялган сонгомол оффлоудинг хийх боломжийг бүрдүүлсэн.

C. Хэмжилт ба өгөгдөл цуглуулалт

Хэмжилтийг бодит хотын нөхцөлд тохирохуйц өгөгдөл цуглуулах зорилгоор ажлын өдрүүдийн

12:00–14:00 цагийн оргил үеэр гурван өдөр дараалан гүйцэтгэсэн. Дараах үзүүлэлтүүдийг бүртгэв:

- 5G секторын ачаалал (%) — gNB ашиглалт болон PRB эзлэх хувиар
- Wi-Fi сувгийн ашиглалт (%) — хандалтын төхөөрөмжийн контроллераас
- Дамжуулах хурд (Mbps) — хэрэглэгч бүрийн дундаж DL хурд
- QoS индекс — саатал, хэлбэлзэл (jitter), packet loss-ийн нийлмэл үнэлгээ
- MOS — VoIP үйлчилгээний чанарыг PESQ-д суурилан үнэлэв
- Төгсгөл-хүртэлх саатал (ms) — ICMP болон RTP timestamp ашиглан

Туршилт бүрийг гурван удаа давтан гүйцэтгэж, статистик хэлбийллийг багасгах үүднээс дундажлан тооцсон. 5G цөм болон Wi-Fi контроллерийн бүртгэлийн өгөгдлийг MATLAB болон Wireshark програм ашиглан боловсруулж, синхрончлолын нарийвчлал болон пакетийн хуваарилалтыг баталгаажуулав.

D. Туршилтын орчин

Туршилтын явцад сектор бүрт идэвхтэй хэрэглэгчийн тоо дунджаар 350–400 орчим байсан бөгөөд тэдгээрийн 40 % нь Wi-Fi-г давхар ашиглаж байв. Гадаад орчны температур 4–7 °C, салхины нөлөөлөл бага, Wi-Fi хандалтын төхөөрөмж болон туршилтын төхөөрөмж хооронд шууд хараагүй нэвтрэлттэй (line-of-sight) нөхцөл бүрдсэн. Туршилтын дэд бүтэц нь тасралтгүй өгөгдөл цуглуулахын тулд сүлжээнд суурилсан нөөц тэжээлтэй ажиллав.

IV. ТУРШИЛТЫН ҮР ДҮН БА ХАРЬЦУУЛСАН ШИНЖИЛГЭЭ

Гетероген оффлоудинг механизмуудын бодит хотын орчин дахь үр нөлөөг үнэлэхийн тулд Улаанбаатар хотын явган болон тээврийн хэрэгслийн хөдөлгөөн хамгийн ихтэй бүсүүдийн нэг болох Сүхбаатарын талбайн орчимд талбарын туршилт гүйцэтгэсэн. Туршилтын орчин нь 3.5 GHz давтамжийн зурваст, 100 MHz сувгийн өргөнтэй 5G NR макро эс болон 5 GHz лицензгүй зурваст ажиллах Wi-Fi 6 хандалтын цэгүүдээс бүрдэв. Хэмжилтийг оргил ачааллын үе (12:00–14:00)-ийн хооронд IFOM, ATSSS, ANDSF, LBO зэрэг оффлоудинг стратеги тус бүрийн дагуу авсан.

A. IFOM-д суурилсан оффлоудинг

IFOM механизмаар видео стриминг, VoIP зэрэг тодорхой IP урсгалыг бодит цагийн дамжуулах хурдын үнэлгээнд үндэслэн 5G ба Wi-Fi хооронд динамик байдлаар чиглүүлсэн. Ингэснээр 5G секторын ачаалал ~88 %-аас 68 %-д буурч, Wi-Fi сувгийн ашиглалт 45 %-иас 66 %-д өссөн. Дундаж доош дамжуулах хурд 31 %-иар сайжирч, дундаж QoS индекс 0.44-өөс 0.69 болж нэмэгдсэн.

B. ATSSS арга

ATSSS нь 5G NR болон Wi-Fi-ийн зэрэг дамжуулалтыг зөвшөөрч, 5G цөмийн Policy Control Function (PCF)-ээр олон замын өгөгдөл хуваарилалтыг удирдсан. Туршилтад үзүүлсэн бүх аргачлалуудын дундаас хамгийн өндөр дамжуулах хурдны сайжруулалтыг (36 %) хүргэсэн. 5G-ийн ачаалал 65 % болж буурч, Wi-Fi сувгийн ашиглалт 70 %-д хүрсэн. VoIP үйлчилгээний чанарыг илэрхийлэх дундаж MOS 3.2-оос 4.2 болж сайжирсан нь бодит цагийн аппликэйшний гүйцэтгэл мэдэгдэхүйц дээшилснийг харуулна.

C. ANDSF-ийн бодлого-суурилсан сонголт

3GPP Release 11-д тодорхойлогдсон ANDSF механизм нь статик сүлжээ сонгох дүрэм болон UE-ийн бодлогын хэрэгжилтэд тулгуурласан. Хэрэгжүүлэхэд харьцангуй хялбар боловч дасан зохицох чадвар сул байв. Үр дүнд нь 5G-ийн ачаалал 90 %-аас 73 %-д буурч, Wi-Fi-ийн ашиглалт 62 %-д хүрч, QoS индекс 0.61 болж хязгаарлагдмал сайжрал үзүүлсэн.

D. Local Breakout (LBO) орчин

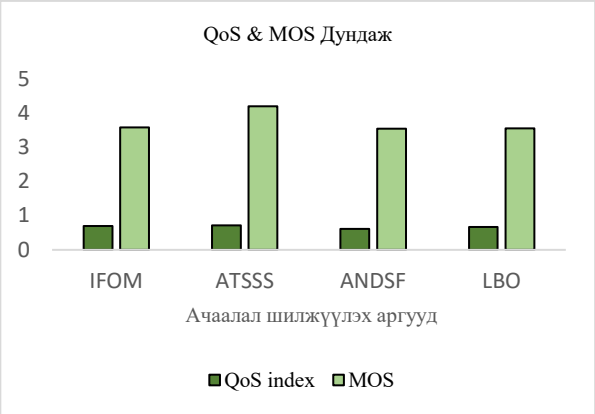
LBO тохиргоонд орон нутгийн контент дамжуулалт (жишээ нь: видео кэшлэлт, ухаалаг хотын мэдрэгчийн өгөгдөл) нь 5G цөмөөр дамжихгүйгээр захын гарцад оффлоуд хийгдсэн. Энэ арга нь цөмийн сүлжээний саатлыг 25 %-иар бууруулж, QoS-ийн үнэлгээг 0.67 хүртэл сайжруулсан ч, олон замын зэрэг агрегаци байхгүй тул ATSSS-тай харьцуулахад дамжуулах хурдын өсөлт харьцангуй бага байв.

E. Харьцуулсан дүн

Method	5G Load	Wi-Fi Utilization	QoS Index	MOS (VoIP)	Давуу тал
IFOM	88% to 68%	45% to 66%	0.69	3.9	Урсгал-суурилсан саадгүй чиглүүлэлт
ATSSS	90% to 65%	40% to 70%	0.71	4.2	Олон замын хуваалт, хамгийн өндөр гүйцэтгэл
ANDSF	90% to 73%	41% to 62%	0.61	3.7	Бодлого-суурилсан энгийн чиглүүлэлт
LBO	87% to 70%	43% to 60%	0.67	3.8	Цөмийн саатал бууралт

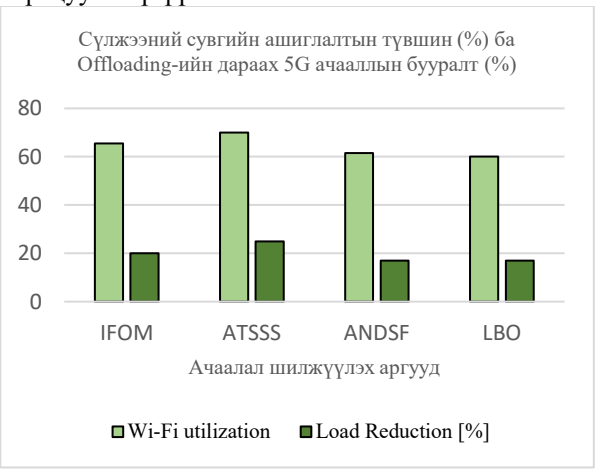
Тайлбар:

Харьцуулсан шинжилгээнээс харахад ATSSS арга нь QoS болон хэрэглэгчийн VoIP чанарын хувьд (MOS > 4.0) бусад оффлоудинг механизмуудаас илүүрхсэн гүйцэтгэлтэй байлаа. Энэ нь тухайн аргын динамик, сешн-суурилсан олон замын удирдлагаас шалтгаалсан юм. 1-р зурагт өөр-өөрхөн оффлоудингийн аргуудын дундаж QoS болон MOS утгуудыг харьцуулан үзүүлэв.



Зураг 1. Дундаж QoS ба MOS-ын харьцуулалт

Зураг 2. Янз бүрийн offloading аргуудын үед гарсан сувгийн ашиглалтын хувь (%) болон offloading-ийн дараах 5G-ийн ачаалал бууралт (%)–ын утгуудыг харьцуулан үзүүлж байна.



Зураг 2. Wi-Fi сувгийн ашиглалт (%) болон оффлоудинг хийсний дараа 5G-ийн ачаалал хэдэн хувиар буурсныг өөр-өөрхөн оффлоудинг аргуудаар харьцуулсан байдлаар үзүүлэв.

IFOM нь урсгалын түвшний оффлоудингийн хувьд найдвартай гүйцэтгэлтэй боловч давхар IP удирдлагын нэмэлт ачаалал шаарддаг. ANDSF нь хэрэгжилтийн түвшинд энгийн, бага нарийнслалтай орчинд тохиромжтой бол LBO нь захын зангилааны ойролцоох локал траффикийн ачааллыг бууруулахад хамгийн үр дүнтэй.

Ерөнхий дүгнэлтээс үзвэл, талбарын туршилтын үр дүн нь ATSSS болон IFOM-ыг ашигласан ухаалаг 5G/Wi-Fi нэгтгэл нь хотын төв хэсэг зэрэг өндөр нягтаршилтай орчинд сүлжээний бөглөрлийг мэдэгдэхүйц бууруулж, үйлчилгээний тасралтгүй байдлыг ханган, хэрэглэгчийн туршлагыг сайжруулдаг болохыг нотлов.

V. ГҮЙЦЭТГЭЛИЙН ҮНЭЛГЭЭ

Энэхүү 5G/Wi-Fi гетероген оффлоудингийн хүрээний гүйцэтгэлийг Улаанбаатар хотын Сүхбаатарын талбайд хийсэн талбарын туршилтаас цуглуулсан бодит хэмжилтийн үр дүнд үндэслэн үнэлэв. Үнэлгээг 5G-ийн ачааллыг бууруулалт, Wi-Fi сувгийн ашиглалт, QoS индекс, VoIP-ийн MOS зэрэг гол гүйцэтгэлийн үзүүлэлтүүд (KPI)-д тулгуурлан хийсэн.

A. Сүлжээний ачаалал ба ашиглалт

Туршилтын үр дүнд Wi-Fi сүлжээнд оффлоуд хийснээр 5G секторын ачаалал мэдэгдэхүйц буурсан нь тогтоогдов. ATSSS механизмыг ашиглахад 5G эсийн ачаалал ~90 %-иас 65 % болж, 25 %-ийн бууралт үзүүлсэн нь зөвхөн 5G-д ажиллах үндсэн хувилбарын харьцуулахад илт сайжрал юм.

IFOM нь ачааллыг 20 % орчим бууруулсан бол ANDSF болон LBO нь тус бүр ойролцоогоор 17 %-ийн дунд зэргийн бууралт хүргэв. Үүнийг дагаад Wi-Fi сувгийн ашиглалт ATSSS-ийн үед 40 %-иас 70 % болж, IFOM-ын үед 45 %-иас 66 % болж өссөн нь хандалтын сүлжээнүүдийн хооронд нөөцийг үр ашигтай хуваарилж байгааг харуулж байна.

B. Үйлчилгээний чанар ба хэрэглэгчийн туршлага

Саатал, хэлбэлзэл (jitter), packet loss зэрэг параметрүүдэд тулгуурлан тооцсон дундаж QoS индекс суурь нөхцөлд 0.42 байсан бол ATSSS-ийн үед 0.71, IFOM-ын үед 0.69, LBO-д 0.67, ANDSF-д 0.61 болсон. Энэ нь олон замын дасан зохицох чиглүүлэлт (ATSSS) нь оргил ачааллын үед илүү найдвартай, тогтвортой ажиллагааг хангаж байгааг харуулж байна.

ITU-T-ийн PESQ загварт тулгуурлан хэмжсэн VoIP үйлчилгээний MOS нь зөвхөн 5G-ийн хувилбарт 3.2 байсан бол ATSSS механизмтэй үед 4.2 болж, бараг маш сайн түвшинд хүрэв.

IFOM болон LBO тус бүр MOS-ийг 3.9, 3.8 болгон сайжруулсан бол ANDSF нь 3.7 хүргэсэн нь бодит цагийн сувгийн өөрчлөлтөд дасан зохицох чадвар хязгаарлагдмал болохыг илтгэнэ. Зураг 1-д бүх оффлоудингийн механизмуудын дундаж QoS болон MOS үзүүлэлтүүдийн харьцуулсан гүйцэтгэлийг үзүүлэв.

C. Саатал ба дамжуулах хурд

MEC гарц дахь локал чиглэлээр дамжуулсны үр дүнд LBO-ийн үед төгсгөл-хүртэлх саатал 25 %-иар буурсан.

ATSSS нь 5G/Wi-Fi-ийн зэрэг дамжуулалт (path aggregation)-ыг дэмжсэнээр хамгийн өндөр буюу 36 %-ийн дундаж дамжуулах хурдны өсөлтийг харуулсан.

IFOM нь 31 %-ийн өсөлт үзүүлсэн бол ANDSF нь статик бодлого ашигладаг тул зөвхөн 15 %-ийн өсөлттэй байв.

D. Хэлэлцүүлэг

Үнэлгээнээс харахад ATSSS нь дамжуулах хурд, саатал, хэрэглэгчийн үйлчилгээний чанарын хооронд хамгийн тэнцвэртэй шийдлийг санал болгож байна. Энэ нь 5G цөмийн PCF-д суурилсан динамик олон замын удирдлагатай холбоотой.

IFOM нь урсгалын түвшний тогтвортой байдал, тасралтгүй хандалтыг хангадаг тул хамгийн их зурвасын шаардлагагүй, үйлчилгээний тасралтгүй байдал чухал хэрэглээнд тохиромжтой.
ANDSF нь статик бодлого хэрэгжүүлэх энгийн арга боловч бодит цагийн сувгийн өөрчлөлтөд дасан зохицохгүй.

LBO нь саатлыг бууруулж, цөм сүлжээнээс хамаарал багасгах давуу талтай боловч локал өгөгдлийн дамжуулалттай нөхцөлд илүү оновчтой.
Ерөнхийд нь авч үзвэл, гибрид 5G/Wi-Fi HetNet орчинд ATSSS болон IFOM-ыг нэгтгэн ашиглах нь бөглөрлийг бууруулж, спектрийн үр ашгийг дээшлүүлэн, хэрэглэгчийн QoE-г сайжруулах өндөр үр нөлөөтэй. Эдгээр туршилтын бодит үр дүн нь Монгол Улсын хотын 5G сүлжээний өсөн нэмэгдэж буй траффикийн хэрэгцээг хангахад стандартчилсан оффлоудинг механизмууд үр дүнтэй болохыг баталж, ирээдүйн ухаалаг хот болон mMTC хэрэглээнд бодит суурь шийдэл болох боломжтойг харууллаа.

ДҮГНЭЛТ БА ЦААШДЫН СУДАЛГААНЫ ЧИГЛЭЛ

Энэхүү өгүүлэлд Улаанбаатар хотын хамгийн өндөр ачаалалтай бүсүүдийн нэг болох Сүхбаатарын талбайд IP IFOM, ATSSS, ANDSF, LBO зэрэг 5G/Wi-Fi гетероген оффлоудингийн механизмд талбарын туршилт хийж, иж бүрэн үнэлгээ гүйцэтгэсэн. Өмнөх симуляцад суурилсан судалгаануудтай харьцуулахад энэхүү судалгаа нь бодит 5G NR болон Wi-Fi 6 сүлжээг ашиглан хотын амьд хэрэглээтэй нөхцөл дэх гүйцэтгэлийг хэмжсэнээрээ онцлогтой. Туршилтын үр дүнгээс харахад ухаалаг оффлоудинг нь сүлжээний нийт үр ашиг болон хэрэглэгчийн туршлагыг мэдэгдэхүйц дээшлүүлж байгааг нотоллоо.
Тухайлбал, 5G секторын ачаалал ~90 %-аас 65 %-д буурч, Wi-Fi сувгийн ашиглалт 40 %-иас 70 %-д өссөн бөгөөд дундаж QoS индекс 0.42-оос 0.71 болж сайжирсан. Мөн VoIP үйлчилгээний MOS 3.2-оос 4.2 болж нэмэгдсэн нь хэрэглэгчийн хүлээн авах чанар (perceived quality)-т бодитой ахиц гарсныг илтгэнэ. Судалгаанд туршсан механизмуудаас ATSSS нь динамик олон замын удирдлага болон бодит цагийн бодлого тохируулгын ачаар хамгийн өндөр үзүүлэлттэй байсан бол IFOM нь урсгал-суурилсан найдвартай чиглүүлэлт ба тасралтгүй хөдөлгөөнт байдлыг хангаж өгсөн.
Эдгээр үр дүн нь 3GPP-ийн стандартад нийцсэн механизмуудыг ухаалаг хотын түвшний траффик оффлоудингт үр дүнтэй ашиглаж болохыг, сүлжээний ашиглалт оновчтой болох, саатал буурах, үйлчилгээ тасралтгүй хангагдахад чухал ач холбогдолтойг харуулж байна. Мөн энэхүү судалгаа нь хөгжиж буй бүс нутгуудад 5G–Wi-Fi интеграцийн өртөг багатай, өргөтгөх боломжтой стратегийг хэрэгжүүлэхэд операторуудад бодитой гарын авлага болж өгнө.

Цаашдын судалгааны чиглэлүүд
Сүүлийн жилүүдэд сансрын холбоо болон хиймэл дагуулын суурьтай интернэт үйлчилгээ дэлхийн харилцаа холбооны зах зээлд эрчимтэй нэвтэрч, хэрэглээний хүрээ өсөн нэмэгдэж байна. Ийм нөхцөлд үүрэн холбоо болон мобайл сүлжээний дэд бүтцэд сансрын холбооны технологийг ашиглан холболтын хүртээмж, найдвартай байдал, үйлчилгээний чанарыг сайжруулах боломжийг судлах шаардлага улам бүр нэмэгдэж байна.
Цаашдын судалгааны ажлын хүрээнд дараах чиглэлүүдийг нарийвчлан авч үзэх шаардлагатай. Үүнд:

VSAT суурьтай хиймэл дагуулын холбооны технологи, түүний архитектур, latency, өргөтгөх боломж
Starlink сансрын интернет үйлчилгээ, LEO хиймэл дагуулын тогтолцоо, гүйцэтгэлийн үзүүлэлт
Amazon Leo (Kuiper) систем, түүний өрсөлдөх чадвар болон мобайл сүлжээнд ашиглах боломж
Дээрх гурван технологийг техник, гүйцэтгэл, үйлчилгээний чанар (хурд, саатал), үнэт өртөг, ашиглалтын нөхцөл, мөн Монгол Улсад хэрэгжүүлэх техникийн болон зохицуулалтын боломжийн хүрээнд харьцуулсан судалгаа хийх нь зүйтэй. Энэ нь үндэсний харилцаа холбооны сүлжээний хөгжлийн стратеги, хөдөө орон нутагт өргөн зурвасын хүртээмжийг нэмэгдүүлэх бодлогын шийдвэрт бодитой хувь нэмэр оруулах боломжтой юм.

Товчилсон нэр томьёоны жагсаалт

3GPP	3rd Generation Partnership Project
5GC	Fifth Generation
ANDSF	Access Network Discovery and Selection Function
ATSSS	Access Traffic Steering, Switching, and Splitting
BTS	Base Transceiver Station
EPC	Evolved Packet Core
gNB	Next Generation NodeB
HetNet	Heterogeneous Network
IFOM	IP Flow Mobility
IMT-2020	International Mobile Telecommunications-2020
IoT	Internet of Things
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
LBO	Local Breakout
LTE-U	Long-Term Evolution in Unlicensed Spectrum
MEC	Multi-Access Edge Computing
mMTC	Massive Machine-Type Communications
MOS	Mean Opinion Score
PCF	Policy Control Function
QoE	Quality of Experience
QoS	Quality of Service
RAT	Radio Access Technology
UE	User Equipment
UPF	User Plane Function
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity

АШИГЛАСАН МАТЕРИАЛ

[1]. S. Han, “Congestion-aware Wi-Fi offload algorithm for 5G heterogeneous wireless networks,” Computer Communications, vol. 164, pp. 69–76, 2020.

[2]. A. Ayub, S. A. Hassan, H. Pervaiz, and M. A. Imran, “A Comparative Analysis of Wi-Fi Offloading and SBS Cooperation,” Electronics, vol. 10, no. 12, 1493, 2021.
[3]. X. Ba, Z. Guo, J. Li, and S. Zhou, “Multiservice-Based Traffic Scheduling for 5G Access Traffic Steering, Switching and Splitting,” Sensors, vol. 22, no. 9, 3285, 2022.
[4]. Р.Баярмаа, Б.Отгонбаяр, “5G Холимог сүлжээнд мэдээллийн ачааллыг шилжүүлэх (traffic offload) боломж, түүний үр ашгийн судалгаа”, зөвлөх үйлчилгээний тайлан, 2025
[5]. I. Mahmud, A. M. Mohammed, and R. Edwards, “Performance Evaluation of MPTCP on Simultaneous Use of Multiple Access Networks for 4G/5G,” Sensors, vol. 22, no. 19, 7509, 2022.
[6]. L. Nie, J. Zhang, H. Huang, and C. Wu, “A deep reinforcement learning assisted task offloading and resource allocation scheme for edge-cloud collaboration,” Journal of Cloud Computing, vol. 12, no. 1, 2023.
[7]. H. Koo, H. Lee, and Y. Kim, “Simultaneous Utilization of Multiple Radio Access Networks: A 3GPP ATSSS Perspective,” JMSE, vol. 11, no. 11, 2106, 2023.
[8]. NCTA (Burke et al.), “How ATSSS and Trusted Wi-Fi Access Will Enable the Converged Core,” NCTA Technical Papers, 2023.
[9]. M. Pieska, A. Kassler, A. Brunstrom, V. Rakocevic, and M. Amend, “Performance Impact of Nested Congestion Control on Transport-Layer Multipath Tunneling,” Future Internet, vol. 16, no. 7, 233, 2024.
[10]. M. Amend, A. Kassler, and V. Rakocevic, “Cost-efficient multipath scheduling of video-on-demand traffic in the 3GPP ATSSS framework,” City Research Online (pre-print), 2024.
[11]. C. Regueiro, S. de Diego, and B. Urkizu, “Leveraging Blockchain Technology for Secure 5G Offloading Processes,” Future Internet, vol. 17, no. 5, 197, 202

МОНГОЛ УЛСЫН ЖИШЭЭН ДЭЭР ЦАХИМ ЗАЛИЛАН МЭХЛЭХ ГЭМТ ХЭРГИЙН ШАЛТГААН НӨХЦӨЛ БА УРЬДЧИЛАН СЭРГИЙЛЭХ АРГА, СУДАЛГАА

Төвшинтөгсийн ХАШ-ЭРДЭНЭ[1], Бат-Эрдэнийн МӨНХБАЯР[2]

[1,2]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Кибер Аюулгүй байдлын тэнхим

Холбоо барих зохиогчийн и-мэйл хаяг: Khashaa24k@gmail.com[1]

Хураангуй: **Энэхүү судалгаа нь Монгол Улсад сүүлийн үед эрчимтэй нэмэгдэж буй цахим залилангийн гэмт хэргийн тархалт, шалтгаан нөхцөл, үйлдлийн арга барил, мөрдөн шалгах ажиллагааны тулгамдсан асуудлыг иж бүрнээр судлан, урьдчилан сэргийлэх болон таслан зогсоох үр дүнтэй арга хэмжээг санал болгох зорилготой. Судалгаагаар 2023 оны эхний 7 сард залилах гэмт хэрэг өмнөх оноос 57.1 хувиар өсөж, нийт гэмт хэргийн 25.7 хувийг эзэлж байгаа нь тогтоогдсон. Гол шалтгаануудад иргэдийн цахим аюулгүй байдлын мэдлэг дутмаг байдал, гэмт хэрэгтнүүдийн олон улсын платформ, криптовалют ашиглан ул мөрөө баллах арга барил, мөн хууль сахиулах байгууллагын хүний нөөц, техник технологийн хоцрогдол зэрэг нь нөлөөлж байна. Олон улсын шилдэг туршлагаас харахад цахим залилантай тэмцэхэд 24/7 ажиллагаатай шуурхай хариу үйлдэл үзүүлэх нэгж, хиймэл оюун ухаанд суурилсан илрүүлэлтийн систем, банк болон мобайл операторуудтай хамтарсан үйл ажиллагаа чухал болохыг онцоллоо. Судалгааны үр дүнд үндэслэн урьдчилан сэргийлэх, мөрдөн шалгах чиглэлийн албадад чиглэсэн цогц зөвлөмжийг боловсруулж, энэ төрлийн гэмт хэргийг үр дүнтэйгээр таслан зогсоох боломжийг хэлэлцэв.**

Түлхүүр үгс: *Цахим залилан, гэмт хэрэг, шалтгаан нөхцөл, урьдчилан сэргийлэх, мөрдөн шалгах, кибер аюулгүй байдал.*

I. УДИРТГАЛ

Сүүлийн жилүүдэд дэлхий нийтэд мэдээллийн технологийн хурдацтай хөгжил нь кибер гэмт хэргийн тоог ихээхэн нэмэгдүүлж байна [5]. Монгол Улс ч энэхүү чиг хандлагаас хоцрохгүйгээр цахим орчинд үйлдэгдэх гэмт хэргийн, ялангуяа залилан мэхлэх хэргийн тоо огцом өсөж, нийгэм, эдийн засагт ноцтой хохирол учруулах боллоо. Цахим технологийн ашиглалт нэмэгдэхийн хэрээр гэмт хэрэгтнүүд улам нарийн арга барилтай болж, гэмт хэргийн үйлдлийн хэлбэрүүд далд байдалтай, илрүүлэхэд хүндрэлтэй болон хувирч байна.

Монгол Улсын хэмжээнд 2023 оны эхний 7 сарын байдлаар залилан мэхлэх гэмт хэрэг өмнөх оны мөн үеэс 57.1 хувиар өсөж, энэ нь нийт гэмт хэргийн өсөлтийн 24.4 хувьд шууд нөлөөлжээ. Цаашилбал, улсын хэмжээнд бүртгэгдэж буй нийт гэмт хэргийн бүтцэд залилах хэрэг 25.7 хувийг эзэлж байгаа нь энэ төрлийн гэмт хэрэгтэй тэмцэх, урьдчилан сэргийлэх, мөрдөн шалгах ажиллагааг сайжруулах зайлшгүй шаардлага байгааг харуулж байна [1]. Цахим хэлбэрт шилжсэн энэхүү гэмт хэрэг нь уламжлалт аргаар гэмт хэрэгтэй тэмцэх ажиллагаанд томоохон сорилт учруулж, хууль сахиулах байгууллагын үйл ажиллагааг шинэ түвшинд гаргах, орчин үеийн технологид суурилсан арга хэмжээг хэрэгжүүлэх хэрэгцээг бий болгож байна.

Иймд энэхүү судалгаа нь Паретогийн оновчлолын зарчимд тулгуурлан, нийт гэмт хэргийн өсөлтийн гол шалтгаан болж буй цахим залилангийн гэмт хэргийн шалтгаан нөхцөлийг тодорхойлж, улмаар цагдаагийн байгууллагын алба, нэгжүүдийн үйл ажиллагаанд шаардлагатай зөвлөмжийг боловсруулах зорилготой юм. Судалгааны үр дүн нь цахим залилангийн гэмт хэрэгтэй тэмцэх бодлого боловсруулах, иргэдийг хохирохоос урьдчилан сэргийлэх, мөрдөн шалгах ажиллагааны үр дүнг дээшлүүлэхэд чухал ач холбогдолтой болно.

Цахим залилан (cyber fraud) нь кибер гэмт хэргийн нэгэн төрөл бөгөөд хувь хүн эсвэл байгууллагыг хууран мэхлэх зорилгоор цахим холбооны хэрэгсэл (и-мэйл, мессеж, веб сайт, сошиал медиа платформ г.м.) ашиглан санхүүгийн ашиг хонжоо олохыг хэлнэ [6]. Энэ нь фишинг, хуурамч зар сурталчилгаа, хандивын луйвар, хөрөнгө оруулалтын залилан, хувийн мэдээлэл хулгайлах, цахим тоглоомын залилан зэрэг олон хэлбэртэй байдаг.

II. ЦАХИМ ЗАЛИЛАНГИЙН ӨСӨЛТИЙН ЧИГ ХАНДЛАГА

Сүүлийн арван жилд дэлхий даяар цахим залилангийн гэмт хэрэг огцом өсөх хандлагатай байна. Коронавирусын цар тахлын үе буюу 2020 оноос эхлэн улс орнууд хөл хорио тогтоосноор цахим худалдаа, үйлчилгээний хэрэглээ нэмэгдэж, цахим худалдан авагчдын тоо жил тутам 20 хувиар өссөн нь цахим залилангийн гэмт хэргийн хурдацтай өсөлтөд шууд нөлөөлсөн гэж шинжээчид үздэг. Олон улсын дата аналитикийн байгууллагын

статистик мэдээгээр дэлхий даяар цахим залилангийн гэмт хэрэг 10 их наяд орчим ам.долларын хохирол учруулж байгаа нь энэ асуудлын цар хүрээг харуулж байна.

Судлаачдын хийсэн дүгнэлтээр цахим сүлжээний төрөл, хэрэглэгчдийн хүрээ тэлэх тусам залилах гэмт хэргийн хохирогчдын тоо үржүүлэхийн хүрд адил нэмэгдэж, ирээдүйд бүртгэгдэх гэмт хэргийн дийлэнх хувийг эзлэх хандлагатай байна. Жишээлбэл, Америкийн Нэгдсэн Улсын Холбооны мөрдөх товчооны 2020 онд хийсэн судалгаагаар олон улсад хууль бус онлайн худалдаа эрхэлж буй "Silk Road", "Alpha Bay", "Hush Hush" зэрэг 3 мянга орчим цахим хуудас бүртгэгдсэн нь кибер гэмт хэргийн далд сүлжээний цар хүрээг харуулдаг. Зарим улс орны нөхцөл байдлыг жишээ татаж үзвэл, ОХУ-д нийт гэмт хэргийн 38.2%, Японд 15%, Европын холбооны гишүүн орнуудад 25% (Швейцарид 67%, БНХАУ-д 36%) нь цахим залилан байна. Энэ нь олон улсын хэмжээнд энэ төрлийн гэмт хэрэг нийт гэмт хэргийн дунджаар гуравны нэгийг эзэлж байгааг харуулж байна.

2.1. Цахим залилангийн шалтгаан нөхцөлүүд

Цахим залилангийн өсөлтөд дараах гол хүчин зүйлс нөлөөлдөг [7]:

- **Хэрэглэгчдийн кибер аюулгүй байдлын мэдлэг дутмаг байдал:** Иргэдийн цахим орчин дахь болгоомжгүй байдал, фишинг, хуурамч мэдээлэл, хувийн мэдээлэл хулгайлах оролдлогод амархан өртөх нь гэмт хэргийн хохирогч болох гол шалтгаан болдог.
- **Технологийн дэвшил ба гэмт хэрэгтнүүдийн дасан зохицох чадвар:** Гэмт хэрэгтнүүд олон улсын сервер, VPN, нууцлал өндөр мессежний аппликейшн (Telegram, WhatsApp), криптовалют зэргийг ашиглан өөрсдийн үйл ажиллагааг далдлан, ул мөрөө баллах нь мөрдөн шалгах ажиллагаанд хүндрэл учруулдаг.
- **Хууль сахиулах байгууллагын чадавхи:** Кибер гэмт хэрэгтэй тэмцэхэд шаардлагатай мэргэшсэн хүний нөөц, техник технологийн хангамж, мэдээллийн солилцооны хурд зэрэг нь дутмаг байх нь гэмт хэргийг шуурхай илрүүлэх, таслан зогсооход саад болдог.
- **Эрх зүйн орчин болон олон улсын хамтын ажиллагаа:** Хилийн чанад дахь гэмт хэрэгтнүүдийг илрүүлэх, мэдээлэл солилцох, хохирлыг нөхөн төлүүлэхэд чиглэсэн олон улсын эрх зүйн орчин болон шуурхай хамтын ажиллагааны механизм дутмаг байдаг.

Эдгээр хүчин зүйлсийг иж бүрнээр авч үзэж, Монгол Улсын нөхцөл байдалд хэрхэн илэрч байгааг энэхүү судалгаагаар тодорхойлохыг зорьсон.

III. СУДАЛГААНЫ АРГА ЗҮЙ

Энэхүү судалгааг гэмт хэргийн статистикт шинжилгээ хийх, түүний чиг хандлагад үнэлгээ өгөх, мөн харьцуулсан аналитик судалгаа хийх арга зүйн үндсэн дээр гүйцэтгэсэн болно. Судалгааны ажлыг Цагдаагийн ерөнхий газрын стратеги, бодлого, инновац, хөгжлийн албаны судалгаа, дүн шинжилгээний төвийн алба хаагчид багаар гүйцэтгэсэн.

3.1. Судалгааны эх сурвалж

Судалгааны үндсэн эх сурвалжуудад дараах мэдээллүүд багтсан:

- Цагдаагийн байгууллагын гэмт хэрэг, зөрчлийн нэгдсэн статистик мэдээлэл (2023 оны эхний 7 сар болон өмнөх оны мөн үеийн мэдээ).
- Эрүүгийн цагдаагийн алба болон Мөрдөн байцаах албаны тайлан, тоо бүртгэл.
- Хэрэг бүртгэлт, мөрдөн байцаалтын хөдөлгөөн шийдвэрлэлтийн мэдээ.
- Гадаад, дотоодын эрдэмтэн судлаачдын бүтээл, судалгааны өгүүлэл, тайлангууд.
- Шүүхийн шийтгэх тогтоол, Улсын дээд шүүхийн тогтоолын жишээ (жишээ нь, Өмнөговь аймаг дахь сум дундын эрүүгийн анхан шатны шүүхийн шийтгэх тогтоол, 2025/ШЦТ/145; Баянзүрх, Сүхбаатар, Чингэлтэй дүүргийн Эрүүгийн хэргийн анхан шатны тойргийн шүүхийн Шийтгэх тогтоол, 2025/ШЦТ/1825; Улсын дээд шүүхийн Тогтоол, 2025/ХШТ/73).
- Цагдаагийн байгууллагын өдөр тутмын мэдээлэл [8].

3.2. Мэдээлэл цуглуулах болон анализын арга

Судалгааны явцад тоон болон чанарын мэдээллийн анализыг хослуулан ашигласан.

- **Статистик анализ:** Цагдаагийн байгууллагын гэмт хэргийн статистик өгөгдлүүдэд дүн шинжилгээ хийж, залилангийн гэмт хэргийн өсөлтийн динамик, үйлдлийн арга, тархалтыг тодорхойлсон.
- **Систем динамикийн загварчлал:** Цахим залилангийн төлөв хандлагыг интернет хэрэглэгчдийн тооноос хамааруулан 2030 он хүртэлх хугацаанд 40.0 хувийн тогтмол өсөлттэй байхаар тооцоолсон.
- **Кейс судалгаа:** Залилангийн гэмт хэргийн үйлдлийн арга, хохирлын хэмжээ, мөрдөн шалгах ажиллагааны онцлогийг нарийвчлан судлах зорилгоор шүүхээр шийдвэрлэгдсэн хэргүүд болон цагдаагийн хоногийн мэдээнд

бүртгэгдсэн тохиолдлуудыг түүврийн аргаар сонгон авч, гүнзгийрүүлсэн шинжилгээ хийсэн.
- **Харьцуулсан анализ:** Олон улсын эрдэм шинжилгээний бүтээлүүд, тайлангуудтай харьцуулсан анализ хийж, Монгол Улсын нөхцөл байдлыг дэлхийн чиг хандлагатай уялдуулсан.

IV. СУДАЛГААНЫ ҮР ДҮН

Монгол Улсад цахим залилан мэхлэх гэмт хэргийн ерөнхий нөхцөл байдал нь сүүлийн 5 жилд 4–6 дахин өссөн бөгөөд 2023–2024 онд бүртгэгдсэн залилангийн ихэнх нь:
- TikTok
- Telegram
- WhatsApp
- Фэйсбүүк дээрх хуурамч хуудсаар мөнгө гуйх
- Хуурамч банкны апп/линкээр мөнгө шилжүүлэхийг шаардах
- Хөрөнгө оруулалтын нэр бүхий Ponzi схем
- Гар утас, фэйсбүүк хулгайд өртөж төлбөр төлүүлэх хэлбэрүүд байна.

4.1. Цахим залилангийн гэмт хэргийн тархалт ба чиг хандлага

2023 оны эхний 7 сарын байдлаар Монгол Улсад залилан мэхлэх гэмт хэрэг өмнөх оноос 57.1 хувиар өсөж, нийт гэмт хэргийн 25.7 хувийг эзэлсэн нь уг гэмт хэрэг нийгэмд томоохон асуудал болсныг харуулж байна. Энэ төрлийн гэмт хэргийн тархац нийслэлийн Баянзүрх, Баянгол дүүргүүд болон орон нутагт Орхон, Дархан-уул, Өмнөговь аймгуудад өндөр нягтаршилтай бүртгэгдсэн. Хохирогчдын тоо 75.6 хувиар, холбогдогчийн тоо 81.6 хувиар огцом өссөн байна.

Цахим сүлжээг ашиглан үйлдэгдэх гэмт хэргийн тоо эрс нэмэгдсэн бөгөөд үйлдлийн арга, давтамж нь анхаарал татаж байна. Тухайлбал, Telegram аппликейшнийг ашигласан залилангийн тоо өнгөрсөн оны мөн үеийн 1 тохиолдлоос 685 болж огцом өссөн нь уг платформыг гэмт хэрэгтнүүд идэвхтэй ашиглаж байгааг илтгэнэ. Иргэд цахим аюулгүй байдлын талаар хангалттай мэдлэггүй байгаагаас фишинг, хуурамч мэдээлэлд өртөх, хувийн мэдээллээ алдах тохиолдол нэмэгдэж байгаа нь энэ төрлийн гэмт хэргийн өсөлтөд нөлөөлж байна. Систем динамикийн загварчлалаар 2030 он хүртэл энэ төрлийн гэмт хэрэг 40.0 хувийн тогтмол өсөлттэй байхаар тооцоологдсон нь цаашид ч энэ асуудал хурцадсаар байх төлөвтэй байгааг харуулж байна.

4.2. Цахим залилангийн үйлдлийн арга барил ба кейс жишээ

Судалгаагаар цахим залилангийн үйлдлийн аргын 33.3 хувь нь онлайн бараа бүтээгдэхүүн худалдан борлуулах нэрээр, 23.1 хувь нь хохирогчийн танил, хувийн мэдээллийг ашиглаж, 21.4 хувь нь эх сурвалж тодорхойгүй цахим хаягт хандалт хийснээр үйлдэгдэж байна. Шүүхээр шийдвэрлэгдсэн хэргүүдийн жишээнээс харахад:
- **Хандивын луйвар:** Шүүгдэгч М, П нар Facebook сүлжээ ашиглан "гэр шатсан", "хүүхэд өвдсөн" гэх хуурамч мэдээлэл тарааж 25 удаагийн үйлдлээр хандив залилсан [2].
- **Хуурамч үйлчилгээ:** Шүүгдэгч Б нь Facebook-ээр "заал өгч байна" гэсэн зар байршуулж, 98 хүнд хуурамч түрээсийн төлбөр авч хохирол учруулсан [3].
- **Эрх олгох залилан:** Шүүгдэгч Х нь хохирогчид дархан цаазат газарт газар ашиглах эрхийн гэрчилгээ гаргуулж өгнө хэмээн хуурч, Байгаль орчин, аялал жуулчлалын сайдын хуурамч тушаалын зураг цахимаар явуулан мөнгө залилсан [4].

Цагдаагийн байгууллагын хоногийн мэдээнд бүртгэгдэж буй залилах гэмт хэргийн 70 хувь нь бүртгэгдэх үедээ эзэн холбогдогч тодорхойгүй, цахим сүлжээгээр үйлдэгдсэн байдаг. 2025 оны 08 дугаар сарын 26-ны өдөр бүртгэгдсэн 9 гэмт хэргийн дөрвөн гэмт хэрэг нь **Telegram**, нэг гэмт хэрэг нь **TikTok** ашигласан тохиолдлууд байв. Үүнд, Telegram-аар даалгавар биелүүлж, банкны данс руу их хэмжээний мөнгө шилжүүлж залилуулсан хэргүүд Архангай, Баянгол, Баянзүрх дүүргүүдэд, TikTok-оор даалгавар биелүүлж залилуулсан хэрэг Сонгинохайрхан дүүрэгт тус тус шалгагдаж байна [8].

4.3. Мөрдөн шалгах ажиллагааны үр дүн ба тулгамдсан асуудлууд

2023 оны эхний 7 сард цагдаагийн байгууллага "Залилах" төрлийн нийт 17,807 хэрэгт мөрдөн шалгах ажиллагаа явуулж, 41.7 хувийг шийдвэрлэсэн байна. Гэвч нийт 159.7 тэрбум төгрөгийн хохирол учирснаас ердөө 19.9 хувийг нөхөн төлүүлж, 20.6 сая төгрөгийг битүүмжилсэн нь хохирлыг нөхөн төлүүлэх үр дүн хангалтгүй байгааг харуулж байна.

Мөрдөн шалгах ажиллагаанд дараах хүндрэлүүд учирч байна:
- **Нотлох баримт цуглуулах хүндрэл:** Цахим орчинд үйлдэгдсэн гэмт хэргийн ул мөр хурдан устах эрсдэлтэй байдаг. Иргэд хохирол амссан тухайгаа хугацаа алдаж мэдээлэх нь нотлох баримтыг цуглуулахад хүндрэл учруулдаг.
- **Хүний нөөц, техник технологийн дутмаг байдал:** Мөрдөн шалгах чиг үүрэг бүхий алба хаагчдын ажлын ачаалал их, техник технологийн хангамж, мэргэшсэн байдал

хангалтгүй, цахим ул мөр тогтоох тусгай мэдлэг бүхий ажилтан дутмаг байгаа нь шуурхай, бүрэн нотолгоо цуглуулах боломжийг хязгаарлаж байна.

- **Байгууллага хоорондын уялдаа холбоо:** Банк, холбооны оператор зэрэг байгууллагаас шаардсан лавлагаа, мэдээлэл хугацаанд нь ирдэггүйгээс хэрэг бүртгэл удааширч, нэмэлт ачаалал үүсдэг. Мөн прокурор, шүүхийн шатанд таслан сэргийлэх арга хэмжээг хангалттай авдаггүй нь гэмт хэрэгтнүүдийг оргон зайлах, дахин гэмт хэрэг үйлдэх боломжийг бүрдүүлдэг.
- **Олон улсын хамтын ажиллагаа:** Гэмт хэрэгтнүүд гадаадын IP хаяг, сервертэй платформ (Facebook, Telegram) ашиглаж байгаа нь мөрдөн шалгах ажиллагаанд хүндрэл учруулж байна. Олон улсын платформууд хөнгөн гэмт хэргийн үед хэрэглэгчийн мэдээлэл гаргаж өгөх боломжгүй гэдэг нь мөрдөн шалгалтыг удаашруулдаг.
- **Мөнгө угаах:** Гэмт хэрэгтнүүд хууль бусаар олсон мөнгөө олон улсын болон цахим мөрийтэй тоглоомын данс руу шилжүүлэх, гадаад улсын банкны дансанд байршуулах, виртуал хөрөнгө болгон хувиргах нь мөнгөний урсгалыг мөрдөх, хохирлыг нөхөн төлүүлэхэд хүндрэл учруулж буй практик жишээ юм. Гадаад улсын хууль сахиулах байгууллагуудтай мэдээлэл солилцох эрх зүйн орчин дутмаг байгаа нь мөрдөн шалгах ажиллагааг удаашруулж байна.

V. ХЭЛЭЛЦҮҮЛЭГ

Цахим залилангийн гэмт хэргийн Монгол Улс дахь өсөлт нь дэлхийн чиг хандлагатай нийцэж байгаа бөгөөд энэ нь иргэдийн цахим хэрэглээ нэмэгдэж, гэмт хэрэгтнүүдийн технологийн мэдлэг дээшилж байгаатай шууд холбоотой. Судалгааны үр дүнгээс харахад, энэ төрлийн гэмт хэрэг нь зөвхөн тоон үзүүлэлтээр бус, үйлдлийн арга барилаараа ч улам нарийсч, хууль сахиулах байгууллагуудад шинэ сорилтуудыг бий болгож байна.

Монгол Улсын цагдаагийн байгууллага энэ төрлийн гэмт хэрэгтэй тэмцэхэд олон талын хүндрэлтэй тулгарч байна. **Нэгдүгээрт**, иргэдийн кибер аюулгүй байдлын мэдлэг дутмаг байдал нь гэмт хэрэгтнүүдэд ашиглагдах эмзэг цэг болж байна. **Хоёрдугаарт**, мөрдөн шалгах ажиллагааны чадавхи нь технологийн хөгжлийн хурдыг гүйцэхгүй байгаа нь үр дүн бага байгаагийн гол шалтгаан юм. **Гуравдугаарт**, олон улсын цахим платформ, криптовалют ашиглан үйлдэгдэх гэмт хэрэг нь үндэсний хэмжээний хууль сахиулах байгууллагын эрх хэмжээнээс хэтэрсэн асуудал үүсгэж, олон улсын хамтын ажиллагааг сайжруулах зайлшгүй шаардлагатай байгааг харуулж байна.

Олон улсын туршлагаас харахад цахим залилантай тэмцэхэд зөвхөн гэмт хэргийг мөрдөн шалгахаас илүүтэйгээр, таслан зогсоох, урьдчилан сэргийлэх арга хэмжээг цогцоор хэрэгжүүлэх нь илүү үр дүнтэй байдаг. Үүнд:

- **Шуурхай хариу үйлдэл:** Залилангийн гомдлыг хүлээн авсан даруйд, ялангуяа 30 минутын дотор, санхүүгийн гүйлгээг царцаах механизм нь хохирлыг бууруулах хамгийн чухал арга юм. Үүнийг 24/7 ажиллагаатай шуурхай нэгжээр дамжуулан хэрэгжүүлдэг.
- **Технологийн шийдэл:** Хиймэл оюун ухаанд суурилсан сэжигтэй гүйлгээг илрүүлэх систем, сэжигтэй дансны нэгдсэн хайлтын систем зэрэг нь гэмт хэргийг эхэн үед нь таслан зогсооход үр дүнтэй.
- **Хамтын ажиллагаа:** Банк, мобайл операторууд болон бусад төрийн болон төрийн бус байгууллагуудтай нягт хамтран ажиллаж, мэдээлэл солилцох, сэжигтэй сувгуудыг хаах нь гэмт хэргийн тархалтыг зогсооход чухал үүрэгтэй.
- **Иргэдийн боловсрол:** Олон нийтэд чиглэсэн танин мэдэхүйн сургалт, сэрэмжлүүлэг нь иргэдийг цахим аюулаас өөрийгөө хамгаалах чадварыг дээшлүүлж, гэмт хэргийн хохирогч болохоос урьдчилан сэргийлдэг.

Эдгээр туршлагыг Монгол Улсын нөхцөл байдалд нутагшуулж, цагдаагийн байгууллагын үйл ажиллагаанд нэвтрүүлэх нь цахим залилангийн гэмт хэргийн өсөлтийг бууруулах, нийгмийн аюулгүй байдлыг хангах үндсэн шийдэл болох юм. Цаашид гэмт хэрэг бүрийг мөрдөн шалгах гэхээсээ илүүтэйгээр, таслан зогсоох, урьдчилан сэргийлэх арга хэмжээг онцгойлон анхаарах нь илүү өндөр үр дүнтэй байх болно.

ДҮГНЭЛТ

Монгол Улсад цахим залилангийн гэмт хэрэг нь хурдацтай өсөж, нийгэм, эдийн засагт ноцтой үр дагавар учруулж байна. Судалгаагаар энэ гэмт хэргийн шалтгаан нөхцөлүүд нь иргэдийн цахим мэдлэг дутмаг байдал, гэмт хэрэгтнүүдийн технологийн дэвшил, хууль сахиулах байгууллагын чадавхийн хязгаарлалт, олон улсын хамтын ажиллагааны сул талуудтай салшгүй холбоотой болохыг тогтоов. Мөрдөн шалгах ажиллагаанд ул мөр баримт хурдан устах, гэмт хэрэгтнүүд олон улсын платформыг ашиглах, мөнгөн гүйлгээг далдлах зэрэг нь томоохон хүндрэл учруулж, хохирлыг нөхөн төлүүлэх үр дүнг бууруулж байна.

Олон улсын шилдэг туршлагаас харахад цахим залилантай тэмцэхэд зөвхөн гэмт хэргийг илрүүлж,

шийдвэрлэхээс илүүтэйгээр, таслан зогсоох, урьдчилан сэргийлэх чиглэлийн арга хэмжээг цогцоор нь авч хэрэгжүүлэх нь хамгийн үр дүнтэй болохыг харуулж байна. Үүнд шуурхай хариу үйлдэл үзүүлэх нэгж байгуулах, хиймэл оюун ухаанд суурилсан илрүүлэлтийн системийг нэвтрүүлэх, банк болон мобайл операторуудтай хамтран ажиллах, иргэдийн кибер аюулгүй байдлын боловсролыг дээшлүүлэх зэрэг нь чухал ач холбогдолтой юм.

Судалгааны үр дүнд үндэслэн боловсруулсан зөвлөмжүүдийг хэрэгжүүлснээр цагдаагийн байгууллага цахим залилангийн гэмт хэрэгтэй тэмцэх чадавхийг дээшлүүлж, иргэдийг хохирохоос урьдчилан сэргийлэхэд тодорхой үр дүнд хүрнэ гэж үзэж байна.

Энэхүү судалгаа нь Монгол Улсын цагдаагийн байгууллагын цахим гэмт хэрэгтэй тэмцэх стратеги, бодлогыг боловсруулахад чухал суурь мэдээлэл болж өгөх бөгөөд цаашид энэ чиглэлээр хийгдэх судалгаа, практик үйл ажиллагаанд хувь нэмэр оруулах юм.

НОМ ЗҮЙ

[1]. Залилах гэмт хэргийн нөхцөл байдалд хийсэн дүн шинжилгээ, ЦЕГ-ын Мэдээлэл, дүн шинжилгээ, шуурхай удирдлагын алба, 2023 он, 13 дахь тал.

[2]. Өмнөговь аймаг дахь сум дундын эрүүгийн анхан шатны шүүхийн шийтгэх тогтоол, 2025 оны 08 сарын 14 өдөр, №2025/ШЦТ/145.

[3]. Баянзүрх, Сүхбаатар, Чингэлтэй дүүргийн Эрүүгийн хэргийн анхан шатны тойргийн шүүхийн Шийтгэх тогтоол, 2025 оны 07 сарын 28 өдөр, № 2025/ШЦТ/1825.

[4]. Улсын дээд шүүхийн Тогтоол, 2025 оны 05 сарын 28 өдөр, №2025/ХШТ/73.

[5]. Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The Development of Phishing During the COVID-19 Pandemic. *Journal of Cybersecurity, 9*(1). (Жишээ)

[6]. Al-Qahtani, A. F., & Cresci, S. (2022). COVID-19 Frauds: An Exploratory Study of Victimization During a Global Crisis. *International Journal of Cyber Warfare and Terrorism, 12*(3), 23-45. (Жишээ)

[7]. Rand EU Research Agency, Zürcher, E., Eekelschot, L., Wolcke, A., & Strang, L. (2023). International approaches to police performance measurement. *Rand Research Reports*. (Жишээ)

[8]. http://daily.police.gov/

МАШИН СУРГАЛТ АШИГЛАН ДРОНЫ КИБЕР ХАЛДЛАГЫГ ИЛРҮҮЛЭХ НЬ

Бямбанямийн ТЭМҮҮЛЭН[1], Лхагваагийн ОДОНЧИМЭГ[2], Мөнхсайханы АНАР[3]

[1,2]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Кибер аюулгүй байдлын тэнхим

Холбоо барих зохиогчийн е-мэйл хаяг: temka9944@gmail.com[1]

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

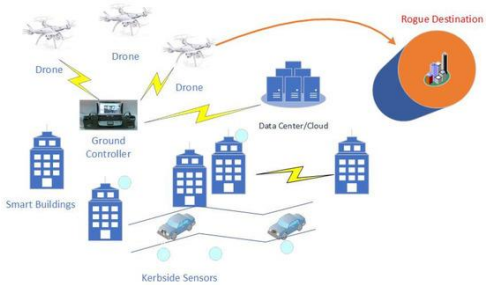
Түлхүүр үг: hijacking, GPS jamming, DoS, машин сургалт, Random Forest.

I. ОРШИЛ

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

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

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



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

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

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

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

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

II. ДРОНЫН (UAV) ТАНИЛЦУУЛГА

Дрон буюу ***Unmanned Aerial Vehicle (UAV)*** нь хүнгүйгээр алсаас удирдлагад ажилладаг агаарын төхөөрөмж бөгөөд ухаалаг хотын экосистемд өгөгдөл цуглуулах, ажиглалт хийх, хүргэлт гүйцэтгэх зэрэг үүрэгтэй [1]. Эдгээр төхөөрөмжүүд нь ухаалаг хотын дэд бүтэцтэй уялдан ажиллаж, байршил, орчны төлөв, хөдөлгөөний талаарх бодит цагийн өгөгдлийг цуглуулж edge эсвэл cloud сервер рүү дамжуулдаг [1].

A. Архитектур ба бүрэлдэхүүн

Дроны архитектур дараах үндсэн хэсгүүдээс бүрдэнэ [1]:

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

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

B. Өгөгдөл дамжуулалт ба нислэгийн лог

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

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

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

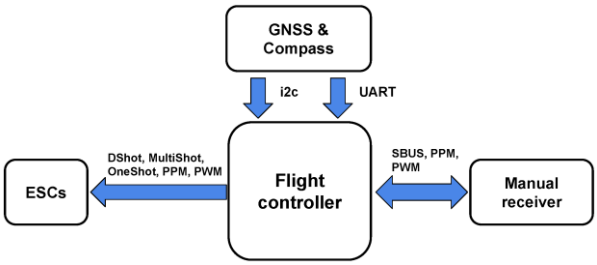
C. Өгөгдлийн урьдчилсан боловсруулалт

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

D. Дүгнэлт

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

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



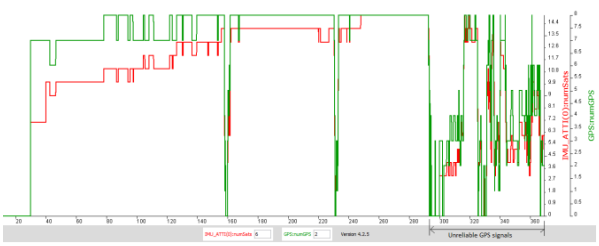
2-р зураг. Дрон системийн архитектур

III. ДРОНЫ ХАЛДЛАГЫН ТӨРӨЛ БА ЛОГ ДЭЭР СУУРИЛСАН ИЛРҮҮЛЭЛТИЙН АРГУУД

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

- *GPS Spoofing ба Jamming*

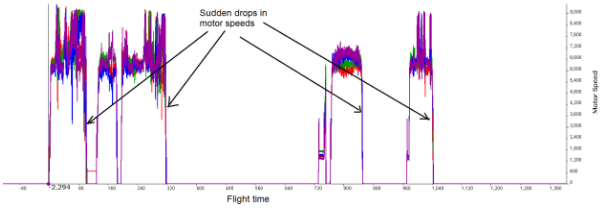
GPS spoofing нь дрон руу хуурамч байрлалын мэдээлэл илгээж, буруу чиглэлд нисэхэд хүргэдэг. Энэ халдлагыг радио долгион дамжуулагч ашиглан хийдэг бөгөөд дронуудын GPS систем шифрлэлгүй дохио хүлээн авдаг учраас халдагчид үүнийг амархан ашигладаг. GPS jamming нь GPS дохиог радио долгионоор дарах замаар дроны навигацийн системийг тасалдуулдаг . Иймт халдлагын үед дроны navHealth лог утга 0 болж, хиймэл дагуулын холболт алдагддаг [1,6]. GPS spoofing нь дрон руу хуурамч байрлалын мэдээлэл илгээж, буруу чиглэлд нисэхэд хүргэдэг [1]. Энэ халдлагыг радио долгион дамжуулагч ашиглан хийдэг бөгөөд дронуудын GPS систем шифрлэлгүй дохио хүлээн авдаг учраас халдагчид үүнийг амархан ашигладаг. GPS jamming нь GPS дохиог радио долгионоор дарах замаар дроны навигацийн системийг тасалдуулдаг [1]. Иймт халдлагын үед дроны navHealth лог утга 0 (3-р зураг) болж, хиймэл дагуулын холболт алдагддаг [1,6].



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

- *Удирдлага булаах (Hijacking)*

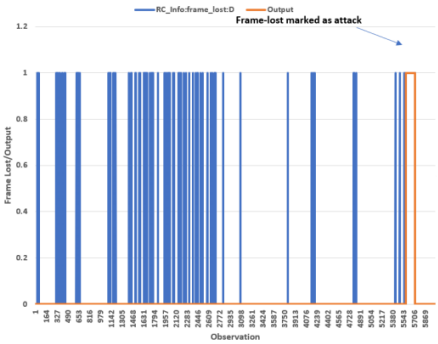
Hijacking буюу удирдлагын булаалт нь халдагч дроны команд ба удирдлагын (C&C) сувгаар орж, системийг алсаас хянах явдал юм. Энэ нь firmware, радио холбоо, эсвэл ground controller-ийн эмзэг байдлыг ашиглан дрон руу шинэ команд оруулах байдлаар хийгддэг [1, 6, 7]. Судалгаанд hijacking үед RC_Info:frame_lost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



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

- *DoS (Denial of Service) халдлага*

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



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

4. *Лог өгөгдлөөр илрүүлэх аргачлал*

Нислэгийн лог өгөгдлийг ашиглан кибер халдлагыг илрүүлэх нь хамгийн үр дүнтэй аргачлалуудын нэг юм. Судалгаанд VTO Labs-ийн нислэгийн лог өгөгдлийг ашиглаж, хэвийн болон халдлагын төлөвийг ялгахын тулд Random Forest, Naïve Bayes, Linear Regression, болон SVM алгоритмуудыг хэрэглэсэн [1,6]. Дрон бүрийн лог файлд дараах шинж чанаруудыг онцолсон:

- IMU_ATTI(0):Longitude, Latitude, Pitch, Roll, Yaw
- Motor:Speed:RFront, LFront, LBack, RBack

- osd_data:navHealth, RC_Info:frame_lost, IMU_ATTI(0):numSats (6-р зураг)

osd_data:compassError	osd_data:connectedToRC	osd_data:lowVoltage
FALSE	Connected	low
FALSE	Connected	low
FALSE	Connected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low
FALSE	DisConnected	low

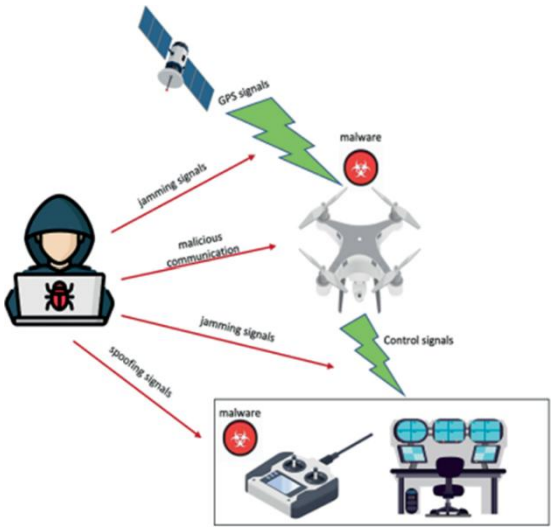
6-р зураг. Машин сургалтын үндсэн шат дамжлагууд: өгөгдөл цуглуулах, шошголох, сургалт ба тест хийх, илрүүлэлт

5. Дүгнэлт

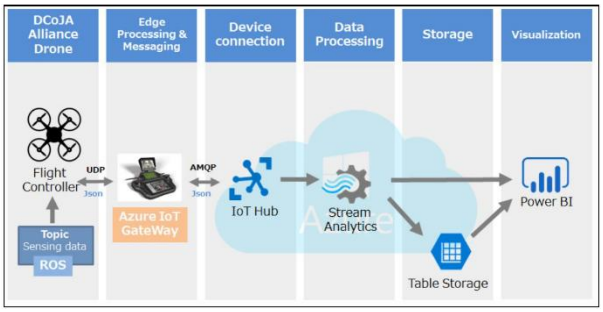
Дроны кибер халдлагууд нь GPS spoofing, hijacking, DoS зэрэг олон хэлбэртэй бөгөөд эдгээр нь системийн лог өгөгдлөөр тодорхой хэмжээнд илэрдэг. Нислэгийн лог-д суурилсан машин сургалтын аргууд нь эдгээр халдлагыг өндөр нарийвчлалтайгаар илрүүлэх боломжийг нээж байна. Судалгааны үр дүнгээр Random Forest ба SVM зэрэг supervised learning алгоритмууд хамгийн үр дүнтэй нь болохыг харуулсан бөгөөд эдгээрийг ухаалаг хотын хамгаалалтын системд нэгтгэх боломжтой гэж үзжээ [1, 5, 7].

IV. СУДЛАГДСАН БАЙДЛЫН ТОЙМ

Дроны кибер аюулгүй байдлын судалгаа сүүлийн жилүүдэд эрчимтэй хөгжиж байгаа бөгөөд судлаачид халдлагын төрөл, илрүүлэлтийн арга, өгөгдлийн онцлог, болон хамгаалалтын архитектурыг олон талаас нь авч үзсэн байдаг. Судалгааны ажлуудыг ерөнхийд нь гурван үндсэн чиглэлд ангилж болно: (1) халдлагын загварчлал ба эрсдэлийн үнэлгээ, (2) машин сургалт дээр суурилсан илрүүлэлт, болон (3) дрон forensic ба лог өгөгдлийн шинжилгээ [1,5]. Singh ба Verma (2017) нь олон дрон (multi-UAV) сүлжээнд үүсэх халдлагын загварыг тодорхойлж, сүлжээний дэд бүтцэд учрах эрсдэлийг *Threat Modeling Framework* (7-р зураг) ашиглан тооцсон [7]. Tran нар (2022) нь UAV системийн кибер эрсдэлийн үнэлгээг *Cybersecurity Risk Framework* (8-р зураг) ашиглан боловсруулсан бөгөөд дрон бүрийн үйл ажиллагааг “Specific Category” ангиллаар эрэмбэлэх аргыг санал болгосон . Эдгээр судалгаанууд нь дроны архитектурын сул талыг илрүүлж, хамгаалалтын арга хэмжээг төлөвлөхөд чухал ач холбогдолтой юм [1].



7-р зураг.. Threat Modeling Framework

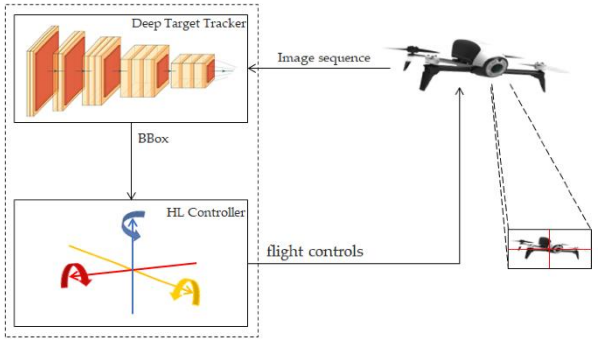


8-р зураг. Cybersecurity Risk Framework

Машин сургалтад суурилсан дрон илрүүлэлтийн судалгаанууд нь сүүлийн жилүүдэд илүү үр дүнтэй болж байгаа. Bronz нар (2020) нь **Real-time fault detection** системийг машин сургалтын аргаар боловсруулж, нислэгийн лог өгөгдлөөр дроны эвдрэл, алдааг илрүүлэх туршилт хийсэн [2]. Lu нар (2017) нь *reinforcement learning* (9-р зураг) ашиглан моторын аномали илрүүлэх системийг хөгжүүлж, UAV-ийн найдвартай байдлыг нэмэгдүүлсэн [1]. Baig нар (2022) нь *drone forensics* болон *machine learning*–ийг хослуулж, drone forensic шинжилгээнд зориулсан cluster загварыг боловсруулсан [3, 5].

Эдгээр судалгаануудын нийтлэг онцлог нь **supervised learning** аргуудыг ашиглан хэвийн ба халдлагын төлөвийг ялгахад чиглэсэн байдаг бөгөөд *Random Forest*, *SVM*, болон *ANN* зэрэг алгоритмууд хамгийн өндөр гүйцэтгэлтэй байжээ [1,5,6].

Reinforcement Learning (RL) нь орчинтой харилцан үйлчилж, туршилт-алдааны зарчмаар хамгийн оновчтой шийдвэр гаргалтыг суралцдаг машин сургалтын арга юм. Дрон RL-ийг ашиглан нислэгийн стратегиа тасралтгүй сайжруулж, сөрөг нөлөө болон халдлагад зөв хариу үйлдэл үзүүлэх чадвартай болдог. (9-р зураг)

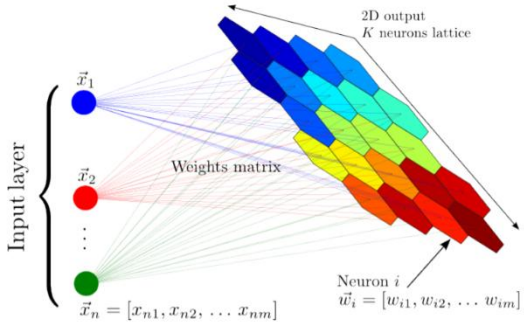


9-р зураг. Reinforcement learning

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

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

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



10-р зураг. Self-Organizing Maps

V. ДРОН ХАЛДЛАГЫГ МАШИН СУРГАЛТААР ИЛРҮҮЛЭХ НЬ

Дроны кибер халдлагын илрүүлэлтийн орчин үед үүсэж буй асуудал нь хурдан хувьсан өөрчлөгдөх хиймэл оюун уур орчин, ухаалаг хотын дэд бүтцийн нэгдэлтэй шууд холбоотой юм. Уламжлалт signature-д суурилсан хандлага нь шинэ төрлийн GPS spoofing, DoS, command hijacking мэтийн халдлагыг амжилттай таних чадваргүй байдаг. Тиймээс машин сургалтын (Machine Learning – ML) загвар ашиглан дроны нислэгийн лог өгөгдлийн үндсэн дээр хэвийн болон халдлагын үйлдлийг ялгах intellectual илрүүлэлтийн системийг боловсруулах нь зүй ёсны шаардлага юм [1,7].

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

Архитектурын үндсэн үе шатууд

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

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

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

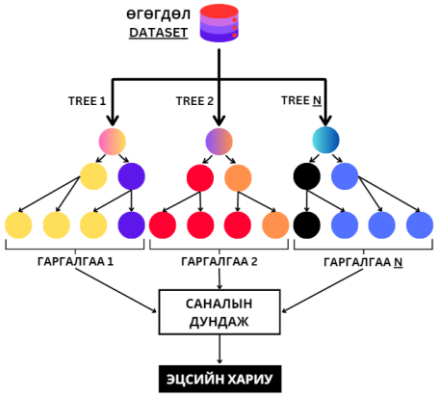
Algorithm	Гол параметрүүд	Тайлбар
Random Forest	n_estimators (9), max_depth (9), criterion (Gini)	Олон ангиллын шийдвэр мод бүрдүүлдэг ensemble арга
Naïve Bayes	Probability smoothing (1.0)	Хурдан ба хөнгөн performance үзүүлэлттэй
Linear Regression	Penalty (L2), tolerance (0.0001)	Логистик ангилалд суурилсан

		таамаглал загвар
SVM	Kernel (RBF), C (1.0), gamma (scale)	Өндөр хэмжээст орон зайд анги задлах арга

1-р хүснэгт. Машин сургалтын загваруудын параметрийн тодорхойлолт

Шийдвэрийн мод ба Random Forest

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



12-р зураг. Random forest алгоритм.

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

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

VI. СУДАЛГААНЫ АРГА ЗҮЙ БОЛОН ҮР ДҮН

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

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

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

Судалгаанд ашигласан машин сургалтын алгоритмууд нь Random Forest (RF), Support Vector Machine (SVM), Naïve Bayes (NB), Linear Regression (LR) гэсэн дөрвөн өөр төрлийн ангиллын модел байв. Random Forest алгоритм нь шийдвэрийн модон бүтэц дээр тулгуурласан ensemble арга бөгөөд олон ангилллын гүйцэтгэлийг дундажлан, хэт сургалтаас хамгаалдаг. SVM загвар нь RBF kernel ашиглан

өгөгдлийн онцлогийг илүү сайн ялгах чадвартай боловч тооцооллын хувьд илүү хүнд байв. Naïve Bayes болон Linear Regression нь суурь хэмжүүрийн зорилгоор ашиглагдсан бөгөөд бусад загваруудын харьцуулалт хийхэд тусалсан [7].

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

13-р зураг. Random forest алгоритм

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

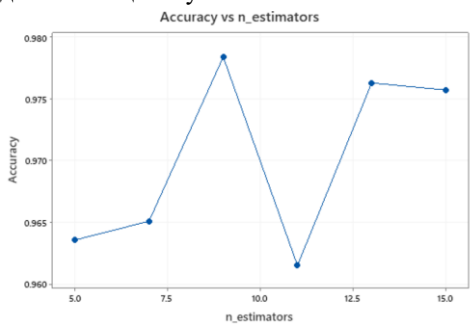
max_depth	Accuracy	Precision	Recall	Training Time
2	0.9517	0.8767	0.7518	0.2288
3	0.9796	0.9818	0.8666	0.2599
4	0.9782	0.9979	0.8421	0.3401
5	0.9914	0.9930	0.9436	0.3846
6	0.9947	0.9960	0.9653	0.4455

14-р зураг. Random forest алгоритм.

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

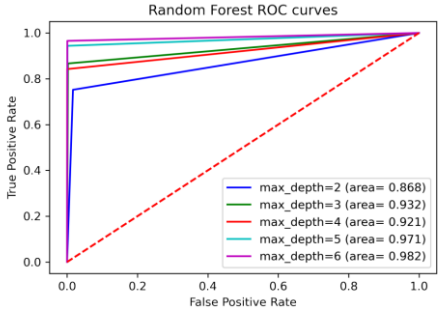
15-р зураг. Дроны өгөгдлийн багц дээрх машин сургалтын загваруудын гүйцэтгэл.

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

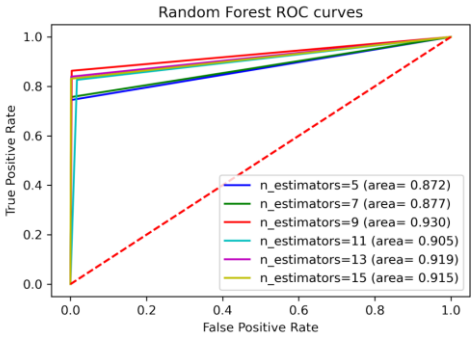


16-р зураг. Random Forest загварын сургалт ба баталгаажуулалтын нарийвчлалын муруй

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



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



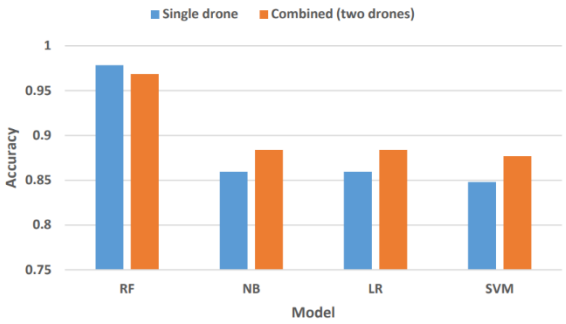
18-р зураг. Random Forest (n_estimators) параметрийн ROC муруй

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

Судалгааны дараагийн шатанд олон төрлийн дрон өгөгдлийг (Phantom 3, Inspire 1, Mavic Pro) нэгтгэн туршилт хийж, нэг төрлийн дрон өгөгдөл дээрх үр дүнтэй харьцуулсан. Хүснэгт 6 болон Зураг 13-д харуулсанчлан Random Forest загвар олон төрлийн өгөгдөлд 97.8% нарийвчлалтай байсан нь өмнөх туршилтаас ≈ 10%-иар сайжирсан. Энэ нь RF загварын generalization буюу ерөнхий чадвар илүү сайн болсон, өөр өөр дроны өгөгдөлд дасан зохицох боломжтойг харуулж байна.

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

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



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

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

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

Эдгээр үр дүнгүүдийн дүн шинжилгээ нь дараах гол дүгнэлтэд хүргэж байна. Нэгдүгээрт, Random Forest алгоритм нь хамгийн өндөр гүйцэтгэлтэй буюу нарийвчлал 97%, AUC 0.97 үзүүлсэн нь нислэгийн лог өгөгдлийн динамик өөрчлөлтийг сайн ялгаж байгааг нотолсон. Хоёрдугаарт, цаг хугацааны хамааралтай өгөгдөл суурилсан feature extraction арга нь GPS, мотор, RC өгөгдлийг уялдуулан халдлагын шинж тэмдгийг илүү сайн илрүүлж өгсөн. Гуравдугаарт, ROC муруйн шинжилгээ нь моделийн overfitting-ийг багасгаж, хамгийн оновчтой параметрүүдийг тодорхойлоход тусалсан. Дөрөвдүгээрт, олон төрлийн дрон өгөгдлийн туршилтаар моделийн generalization чадвар сайжирсан нь дроны төрөл бүрийн өгөгдөлд дасан зохицох чадвартай болохыг харуулсан. Тавдугаарт, энэхүү системийг бодит цагийн илрүүлэлтэд хэрэгжүүлэхэд Google Colab, Raspberry Pi, эсвэл edge AI платформ ашиглах боломжтой гэдгийг судалгаа харуулж байна.

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

ДҮГНЭЛТ

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

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

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

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Singh, M., Baig, Z., & Verma, A. (2022). *Drone Cyber Attack Detection through Machine Learning.* Future Internet, 14(7), 205. https://doi.org/10.3390/fi14070205

[2] DJI (2018). Flight Records Analysis Tutorial. DJI Official Documentation. https://www.dji.com/

[3] VTO Labs (2020). *Drone Forensics Dataset*.

[4] You, Il., Yim, K., Sharma, V., & Cho, J.-H. (2018). *AI-Driven Cybersecurity: Opportunities and Challenges.* In Proceedings of the IEEE Pacific Rim Dependable Computing Conference (PRDC) (pp. 45–52). IEEE.

[5] Mekala, S. H., & Baig, Z. (2019). *Digital Forensics for Drone Data — Intelligent Clustering Using Self-Organizing Maps.* Digital Investigation, 29, S78–S87.

[6] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., … Duchesnay, E. (2011). *Scikit-learn: Machine Learning in Python.* Journal of Machine Learning Research, 12, 2825–2830. https://jmlr.org/papers/v12/pedregosa11a.html

[7] Liu, C., Zhou, Z., & Wang, H. (2017). *Generalising Random Forest Parameter Optimisation to Include Stability and Cost.* In Proceedings of ECML PKDD 2017. Springer.