МОНГОЛ УЛСЫН ШИНЖЛЭХ УХААН,ТЕХНОЛОГИЙН ИХ СУРГУУЛЬ
МЭДЭЭЛЭЛ, ХОЛБООНЫ ТЕХНОЛОГИЙН СУРГУУЛЬ

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

2023/2024 ОНЫ НАМРЫН УЛИРЛЫН ЭРДЭМ ШИНЖИЛГЭЭНИЙ ХУРЛЫН ЭМХЭТГЭЛ

№24(02)326

УЛААНБААТАР 2023

ISSN 1560-8794

Хянасан: Х.Загарзүсэм /МХТС-ийн ЭНБД/

Эмхэтгэсэн: М.Сэлэнгэ /ЭШИХ ажилтан/

Хэвлэлийн хуудас: 8.33 х.х

Хэвлэсэн тоо: Онлайн

Цаасны хэмжээ: А4

Улаанбаатар 2023.12.18

MONGOLIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

SCIENTIFIC TRANSACTIONS

№24(02)326

ULAANBAATAR 2023

Өмнөх үг

Мэдээлэл, Холбооны Технологийн Сургуулийн 2023/2024 оны хичээлийн жилийн намрын улирлын бакалавр, магистр, доктор оюутнуудын судалгаа шинжилгээний ажлын үр дүнг тусгасан эрдэм шинжилгээний өгүүллийг энэхүү эрдэм шинжилгээний бичигт эмхэтгэн гаргаж байна.

2023/2024 оны хичээлийн жилийн намрын улирлын бакалавр, магистр, доктор оюутны хурлыг "Мэдээлэл Холбооны салбарын хөгжилд бидний гүйцэтгэх үүрэг-2024" сэдвийн хүрээнд зохион байгуулсан бөгөөд салбаруудын ЭШХ-д хэлэлцэгдсэн илтгэлээс шалгарсан бакалавр оюутны 11, магистр оюутны 8 илтгэлийг 2-р шатанд хэлэлцүүлж доктор (Ph.D) Х.Загарзүсэм, доктор (Ph.D) П.Уганбаяр, доктор (Ph.D) Б.Долгорсүрэн, доктор (Ph.D) Ж.Оргил, доктор (Ph.D) Р.Баярмаа, доктор (Ph.D) Б.Дэнсмаа нар бакалавр оюутнуудын илтгэлийг сонсож, доктор (Ph.D) Х.Загарзүсэм, доктор (Ph.D) Г.Ганчимэг, доктор (Ph.D) Б.Дорж, доктор (Ph.D), Б.Долгорсүрэн, доктор (Ph.D), Р.Баярмаа, доктор (Ph.D), Ж.Оргил, доктор (Ph.D) Ц.Энхтөр нар магистр оюутны илтгэлүүдийг сонсож, тус бүр 3 байр шалгаруулав. Хурлын өгүүллийн редакцаар доктор (Ph.D) Х.Загарзүсэм, доктор (Ph.D), дэд профессор Г.Ганчимэг доктор (Ph.D) Ц.Тэнгис, доктор (Ph.D), дэд профессор Ж.Жавзансүрэн, доктор (Ph.D) Д.Бямбадорж, доктор (Ph.D), дэд профессор Б.Туяацэцэг, доктор (Ph.D), дэд профессор П.Нямсүрэн нар ажиллан тунгаан дүгнэлт өгсний дагуу өгүүллүүдийг засварлан эмхэтгэв.

МАГИСТР ОЮУТНЫ АНГИЛАЛД:

I-р байр **"Fisheye8k: A benchmark and dataset for fisheye camera object detection"**
Илтгэгч: О.Мөнх-Эрдэнэ */Электроник хөтөлбөрийн магистрант/*
Удирдагч: Доктор (Ph.D) Г.Мөнхжаргал */АНЭУ-ын их сургуулийн дэд профессор/*

II-р байр **"Дүрс боловсруулалт, хиймэл оюун ухаан ашиглан нисгэгчгүй нисэх хэрэгсэл илрүүлэх аргын судалгаа"**
Илтгэгч: Б.Мөнх-Учрал */ Электроник хөтөлбөрийн магистрант /*
Удирдагч: Доктор (Ph.D) Б.Дорж */ЭС-ын дэд профессор/*

III-р байр **"Роботод зориулсан байршил тогтоох болон газрын зураг үүсгэх аргачлал"**
Илтгэгч: Ц.Хас-Очир */ Электроник хөтөлбөрийн магистрант /*
Удирдагч: Доктор (Ph.D) Б.Дорж */ЭС-ын дэд профессор/*

БАКАЛАВР ОЮУТНЫ АНГИЛАЛД:

I-р байр **"Машин сургалтын dnn+resnet хосолсон алгоритм ашиглан өвчнийг ангилах нь"**
Илтгэгч: Т.Түвшинсайхан, Х.Ариунзаяа, Н.Дуламсүрэн */Мэдээллийн технологи хөтөлбөр, III курс/*
Удирдагч: Доктор (Ph.D) Б.Долгорсүрэн */МТС-ын дэд профессор/*

II-р байр **"220V төхөөрөмжид зориулсан IoT алсын удирдлагатай унтраалга"**
Илтгэгч: Б.Энхбаяр */ Электроникийн инженерчлэл хөтөлбөр, III курс/*
Удирдагч: Ц.Сугир */ЭС-ын ахлах багш/*

III-р байр **"Хортой URL-г машин сургалтын арга ашиглан илрүүлэх"**
Илтгэгч: Т.Шижир-Алт, Ж.Өнөболд, М.Жүгдэрнамжил, Н.Даваадорж */Кибер аюулгүй байдал хөтөлбөр, III курс/*
Удирдагч: Доктор (Ph.D) Б.Мөнхбаяр */МСАБ-ын салбарын эрхлэгч/*

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

НОМЫН ЦАГААН БУЯН ДЭЛГЭРЭХ БОЛТУГАЙ

ГАРЧИГ

I. МАГИСТР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

II. БАКАЛАВР ОЮУТНЫ ЭРДЭМ ШИНЖИЛГЭЭНИЙ ӨГҮҮЛЛҮҮД

FISHEYE8K: A BENCHMARK AND DATASET FOR FISHEYE CAMERA OBJECT DETECTION

Munkhjargal Gochoo[1,2] Munkh-Erdene Otgonbold[1,2] Erkhembayar Ganbold[1,2] Jun-Wei Hsieh[3]
Ming-Ching Chang[4] Ping-Yang Chen[5] Byambaa Dorj[6] Hamad Al Jassmi[1,2]
Ganzorig Batnasan[1] Fady Alnajjar[1] Mohammed Abduljabbar[1] Fang-Pang Lin[7]

[1] Department of Computer Science and Software Engineering, United Arab Emirates University, UAE
[2] Emirates Center for Mobility Research, United Arab Emirates University, UAE
[3] College of AI and Green Energy, National Yang Ming Chiao Tung University, Taiwan
[4] University at Albany — State University of New York, NY, USA
[5] Department of Computer Science, National Yang Ming Chiao Tung University, Taiwan
[6] Mongolian University of Science and Technology, Mongolia
[7] National Center for High-Performance Computing, Taiwan

mgochoo@uaeu.ac.ae, omunkuush@uaeu.ac.ae, eganbold@uaeu.ac.ae, jwhsieh@nctu.edu.tw,
mchang2@albany.edu, pingyang.cs08@nycu.edu.tw, dorj@must.edu.mn, h.aljasmi@uaeu.ac.ae,
gbatnasan@uaeu.ac.ae, fady.alnajjar@uaeu.ac.ae, 201970087@uaeu.ac.ae, fplin@narlabs.org.tw

Abstract

With the advance of AI, road object detection has been a prominent topic in computer vision, mostly using perspective cameras. Fisheye lens provides omnidirectional wide coverage for using fewer cameras to monitor road intersections, however with view distortions. To our knowledge, there is no existing open dataset prepared for traffic surveillance on fisheye cameras. This paper introduces an open FishEye8K benchmark dataset for road object detection tasks, which comprises 157K bounding boxes across five classes (Pedestrian, Bike, Car, Bus, and Truck). In addition, we present benchmark results of State-of-The-Art (SoTA) models, including variations of YOLOv5, YOLOR, YOLO7, and YOLOv8. The dataset comprises 8,000 images recorded in 22 videos using 18 fisheye cameras for traffic monitoring in Hsinchu, Taiwan, at resolutions of 1080×1080 and 1280×1280. The data annotation and validation process were arduous and time-consuming, due to the ultra-wide panoramic and hemispherical fisheye camera images with large distortion and numerous road participants, particularly people riding scooters. To avoid bias, frames from a particular camera were assigned to either the training or test sets, maintaining a ratio of about 70:30 for both the number of images and bounding boxes in each class. Experimental results show that YOLOv8 and YOLOR outperform on input sizes 640×640 and 1280×1280, respectively. The dataset will be available on the GitHub link with PASCAL VOC, MS COCO, and YOLO annotation formats. The FishEye8K benchmark will provide significant contributions to the fisheye video analytics and smart city applications.

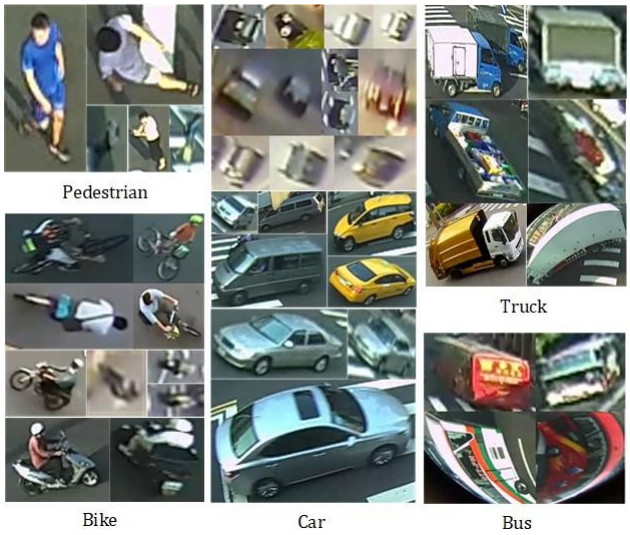


Figure 1. Sample of the 5 classes in the FishEye8K dataset: Pedestrian (all visible people on the streets), Bike (people riding bicycles, motorcycles, or scooters), Car (light vehicles such as sedans, SUVs, Vans, *etc.*), Bus, and Truck (dump-truck, semi-trailers, *etc.*)

1. Introduction

Fisheye lenses have gained popularity owing to their natural, wide, and omnidirectional coverage, which traditional cameras with narrow fields of view (FoV) cannot achieve. In traffic monitoring systems, fisheye cameras are advantageous as they effectively reduce the number of cameras required to cover broader views of streets and intersections.

Dataset	Frame	Boxes	Task	Vehicles	Pedestrian	Weather	Occlusion	Altitude	View	Classes	Location	Type
MIT-Car 2000 [15]	1.1K	1.1K	D	+						-	Surveillance	2D
KITTI-D 2014 [4]	15K	80.3K	D	+	+		+			3	Car	2D
UA-DETRAC 2015 [21]	140K	1210K	D,T	+		+	+			4	Surveillance	2D
Detection in LLC 2017 [9]	7.5K	15K	D	+		+				12	Car	2D
CARPK 2017 [5]	1.5K	90K	D	+						-	Drone	2D
UAVDT 2017 [2]	80K	841.5K	D,T	+		+	+	+	+	-	Drone	2D
NEXET 2017 [6]	50K	-	D	+		+				5	Car	2D
BDD100k 2018 [22]	5.7K	-	D,T	+	+	+				10	Car	2D
AAU RainSnow 2018 [1]	2.2K	13297	D,Seg	+		+					Surveillance	RGB&Thermal
MIO-TCD CCTV 2018 [12]	113K	200K	D	+		+				5	Surveillance	2D
BDD100k Adas 2018 [24]	100K	250K	D,Seg	+		+				10	Car	2D
Woodscape 2018/2019 [23]	10K	-	D,3D,T	+		+				7	Car	Fish-Eye
CityFlow2D 2021 [14]	-	313.9K	D,T	+							Surveillance	2D
FishEye8K 2023 [**our**]	8K	157.0K	D	+	+				+	5	Surveillance	Fish-Eye

Table 1. Summary of existing road traffic datasets. The second and third columns ($1K = 10^3$) indicate the number of images containing at least one object on them and the unique object bounding boxes. Remaining columns: additional attributes for each dataset, i.e., "D": target is a detection task, "$3D$": target is a three-dimensional detection task, "T ": target is a tracking task, and the "Seg": target is a segmentation task.

Despite these benefits, fisheye cameras present distorted views that necessitate a non-trivial design for image undistortion and unwarping or a dedicated design for handling distortions during processing. It is worth noting that, to the best of our knowledge, there is no open dataset available for fisheye road object detection for traffic surveillance applications. The WoodScape dataset [23] was collected using an in-car fisheye dash camera; however, it was intended for self-driving scenarios.

In this paper, we present a new open **FishEye8K** benchmark dataset for the training and evaluation of 2D road object detection tasks. The FighEye8K dataset consists of 8,000 image frames with 157K bounding box annotations of 5 object classes, namely, Pedestrian, Bike, Car, Truck, Bus, and Truck; see Figure 1. A total of 22 short (8 to 20 minutes) videos were extracted from many hour-long videos collected from 35 fisheye cameras. These traffic surveillance cameras are properties of the police department of Hsinchu City, Taiwan, and our data collection is free from user consent agreements or license issues. However, efforts are performed in blurring out visible faces and license plates in the video frames. The dataset comprises different traffic patterns and conditions, including urban highways, road intersections, various illumination, and shooting angles of the five road object classes in various scales.

The labeling of objects of interest is meticulous. Specifically, we labeled all visible and recognizable objects even if they are located far away. The FishEye8K sample images are split into the training and test sets, with a ratio of about 70:30. Efforts are made to keep a similar ratio for each class of road objects. To avoid bias, the train and test sets do not share frames from the same camera. Annotations are provided in several standard formats, including Pascal-VOC [3], MS COCO [11], and YOLO [18].

We also provide benchmarking results of the latest State-of-The-Art (SoTA) two-stage object detection models, including YOLOv5x [7], YOLOR [19], YOLOv7 [20], and YOLOv8, and report in standard metrics including $Precision$, $Recall$, mAP s, AP_S, AP_M, AP_L, $F1\_score$, and their inference time.

The FishEye8K benchmark dataset will be available at https://github.com/MoyoG/FishEye8K upon paper acceptance.

2. Related Works

Road datasets. High-resolution, diverse, and large-scale road datasets play a critical role in advancing and enhancing traffic monitoring systems. In the last decade, the number of open road datasets [1, 2, 4–6, 9, 12, 14, 15, 21–24] for 2D and 3D road object detection, single and multiple object tracking, object segmentation tasks have significantly increased. Table 1 provides a summary of popular road datasets that are used in both model development as well as for benchmarking and public contests. In terms of camera locations, the following datasets are captured using fixed surveillance cameras: MIT-Car [15], UA-DETRAC [21], AAU RainSnow [1], MIO-TCD [12], and AI-City [14] datasets. The CARPK [5] and UAVDT [2] dataasets are captured using drones. The KITTI [4], Detection in LLC [9], NEXET [6], BDD100K [22], and Woodscape [23] datasets are captured using in-dash cameras mounted on a car. In terms of FoV, all the datasets were constructed using standard perspective cameras, with the drawback of narrow FoV. The only exception is the WoodScape dataset [23] that are captured using an in-dash 180° fisheye camera. To our knowledge, the proposed FishEye8K dataset is the first of the kind among the open datasets, that are designed and constructed specifically for the development and evaluation of road object detection using fisheye traffic surveillance cameras.

Fixed perspective traffic camera-based datasets. Table 1 shows that most datasets are captured using fixed,

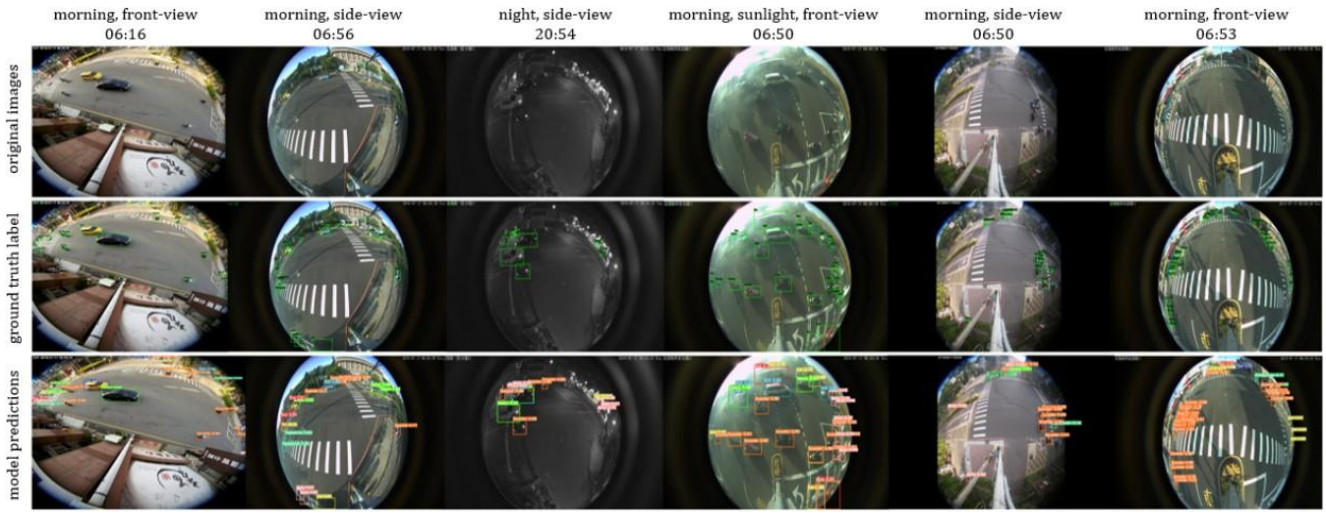


Figure 2. Sample images of FishEye8K dataset: (Top) the original unlabelled images, (Middle) the labeled ground truths, (Bottom) the YOLOv5x6 [7] detected objects. The columns illustrate several viewing angles, time of day, various intersections and road participants in the dataset.

perspective cameras, which are limited by the narrow FoV. All the datasets have annotations for 2D road object detection task; on top of it, a few datasets [2, 14] have multiple objects tracking annotation, and one [1] has segmentation mask annotation. In 2000, MIT-Car dataset [15] was publicly offered as a flagship dataset pioneering the road automation research field. The dataset has 1.1K frames, including 1.1K bounding boxes for the vehicle detection task. In 2016, UA-DETRAC [21] dataset was offered with 140K frames, including rich annotations of illumination, vehicle type, occlusion, and 1210K bounding boxes. The dataset has four classes (car, van, bus, and others) for detection and multiple object detection tasks. In the same year, similarly, MIO-TCD CCTV [12] dataset is offered with 113K frames, including 200K bounding boxes for the detection task. In 2018, the AAU RainSnow [1] dataset was offered as a benchmark for evaluating state-of-the-art rain removal algorithms. The dataset has 22 five-minute real-world camera video sequences collected from 7 urban intersections covering various weather conditions, i.e., snow, rain, haze, and fog. They have extracted 100 frames from each five-minute video to construct 2200 frames, including 13297 bounding boxes. Recently, in 2021, AI-City Challenge [14] was held, including vehicle detection and re-identification on CityFlowV2-ReID dataset and multi-target multi-camera vehicle tracking challenge on CityFlow2D dataset. CityFlow2D dataset has 313.9K bounding boxes for 880 distinct vehicles.

Drone based datasets. Lately, drone road datasets have been publicly offered in the literature, namely CARPK [5] and UAVDT [2]. Both datasets were captured from a high altitude with a viewing angle of the top by narrow FOV cameras for the drone-based road monitoring systems. Thus they are not suitable for fixed surveillance camera-based traffic monitoring.

3. The FishEye8K Dataset

We provide detailed information on the new FishEye8K road object detection dataset. The dataset consists of 8,000 annotated images with 157K bounding boxes of five object classes. Figure 2 shows sample images of the wide-angle fisheye views, which provide new opportunities for large coverage, but also new challenges of large distortions of the road objects.

3.1. Video Acquisition

We have acquired a total of 35 fisheye videos captured using 20 traffic surveillance cameras at 60 FPS in Hsinchu City, Taiwan. Among them, the first set of 30 videos (**Set 1**) was recorded by the cameras mounted at Nanching Hwy Road on July 17, 2018, with 1920×1080 resolution, and each video lasts about 50-60 minutes. The second set of 5 videos (**Set 2**) was recorded at 1920×1920 resolution, and each video lasts about 20 minutes.

All cameras are the property of the local police department, so there is no issue of user consent or license issues. All images in the dataset will be made available to the public for academic and R&D use.

3.2. Dataset Preparation and Characteristics

Sampling. We chose 18 videos from the recorded footage, with 15 videos coming from Set 1. These were cropped into shorter videos, each lasting approximately 8 to 10 minutes, except for one that lasted 16 minutes. Using a sampling method of one frame per 50 and 200 frames for Set 1 and Set 2 videos, respectively, we extracted over

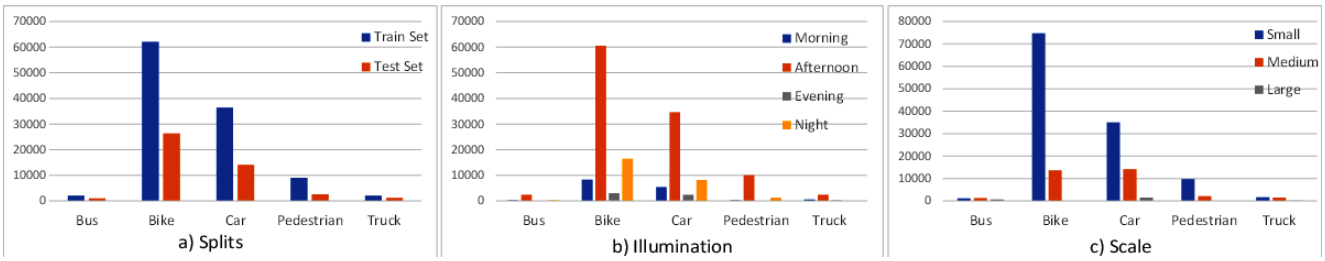


Figure 3. The class distributions of objects in terms of (a) Splits for FishEye8K dataset; (b) Illumination; and (c) Scale.

10,000 frames. The resulting images were then resized to 1080 × 1080 and 1280 × 1280 for Set 1 and Set 2, respectively.

To incorporate a wide range of perspectives on road conditions, we carefully selected videos for our dataset that feature diverse camera angles, including side-view and front-view shots, as well as varying video quality. The dataset also includes images from different intersection types, such as T-junctions, Y-junctions, cross-intersections, midblocks, pedestrian crossings, and non-conventional intersections. The videos were captured under various lighting conditions, including morning, afternoon, evening, and night, and diverse traffic congestion levels ranging from free-flowing to steady and busy. Figure 2 illustrates some of the wide-ranging road conditions with ground truth annotations of road objects and detection results obtained from YOLOv5x6 [7].

Object classes: We annotate 5 major classes for road objects, namely, **Pedestrian** (all visible people on the streets), **Bike** (riders on bicycles, motorcycles, or scooters), **Car** (light vehicles such as sedans, SUVs, vans, *etc.*), **Bus**, and **Truck** (dump-truck, semi-trailers, *etc.*).

Distant objects: The wide fisheye lens creates a wide FoV but also results in a panoramic hemispherical image that is notably distorted with a barrel effect. Additionally, the camera has a tendency to produce blurred images of objects located around the edges of the lens. As a consequence, distant objects can appear minuscule and indistinct. Annotating these distant objects can be an arduous or even impossible task due to their lack of clarity.

Illumination: Four categories of illumination conditions were identified, namely morning (sunrise), afternoon (sunny), evening (sunset), and night. The distribution of video sequences based on their respective illumination attributes is illustrated in Figure 3(b), with the majority of bounding boxes falling under the afternoon category. Nighttime sequences follow in second place, with morning and evening categories trailing behind respectively. Notably, the distribution of classes across all times of day is remarkably similar

Object scale: We define the scale of the bounding boxes of road participants based on their size (length and width) in pixels. The MS COCO evaluator is employed for small and medium, and large scaled objects. However, as the size of the image grows toward 1080 × 1080 or 1280 × 1280, respectively for Sets 1 and 2, we doubled the size of standard scales, i.e., *small* (pixels ≤ 64 × 64), *medium* (64 × 64 < pixels ≤ 192 × 192), and *large* (pixels > 192 × 192). The distribution of road participants in the dataset in terms of scale is presented in Figure 3 (c), where small and medium-scaled objects make the most of the dataset. Bus and Truck classes have a similar number of small and medium scaled objects. On the contrary, other classes have a comparatively high number of small-scaled objects than medium and large-scale objects.

3.3. Annotation

Annotation Rule. The road participants were annotated based on their clarity and recognizability to the annotators, regardless of their location. In some cases, distant objects were also annotated based on this criterion.

Annotation. Two researchers/annotators manually labeled over 10,000 frames using the DarkLabel annotation program over a period of one year. After cleaning the dataset, a total of 8,000 frames containing 157012 bounding boxes remained. Unsuitable frames were removed, including those featuring road participants outside the five classes of interest.

The distribution of objects per class for each video is depicted in Figure 4. Notably, the night video captured by Camera 3 has the highest number of objects. In this dataset, the dominant classes are Bike (88,373) and Car (50,597), which can be attributed to the semi-tropical location of the country where the videos were recorded. On the other hand, the classes of Truck (3,317) and Bus (2,982) have the lowest number of objects, rendering the dataset highly imbalanced. Figure 1 displays a selection of samples from all classes, showcasing various scales. Furthermore, the distributions of classes are depicted as bar graphs in Figure 3.

For the sake of convenience, we provide three different formats for the annotations of FishEye8K datasets, i.e., Pascal-VOC [3], MS COCO [11], and YOLO [18].

3.4. Validation

Given the complexity and effort required for the labeling task, human errors were inevitable, and it was necessary to

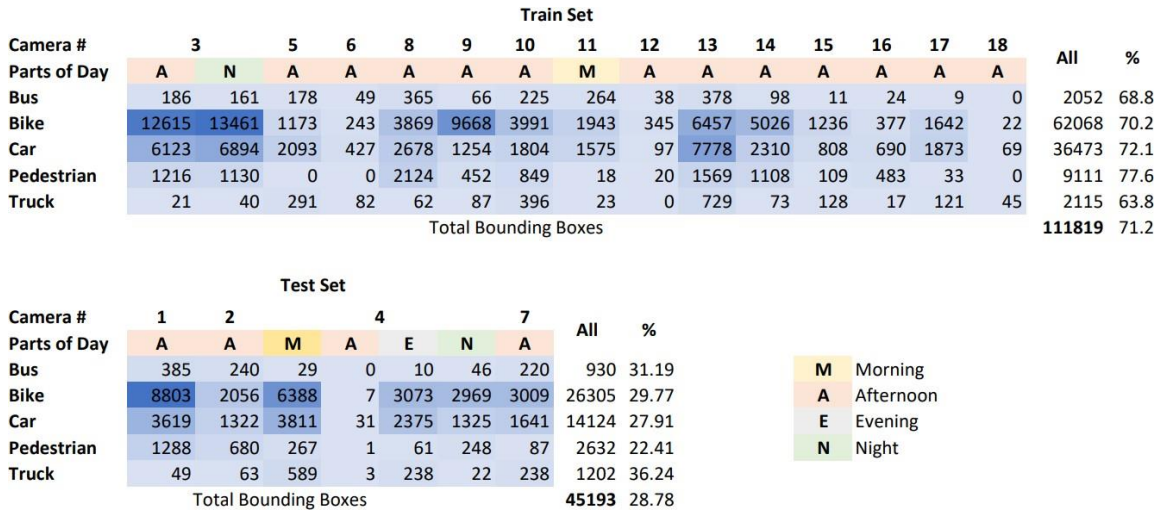


Figure 4. Heat maps represent the number of extracted objects per class from all 22 short videos recorded by 18 cameras for training and test sets of the FishEye8K dataset. For the training set, the darkest blue color refers to 13461 labeled bikes from the video recorded at night with Camera 3.

correct them to avoid inaccurate results. Therefore, in order to minimize human error, we employed two semi-automatic approaches to validate all bounding boxes.

In the case of mislabeled objects, we followed a two-step approach. Firstly, we cropped and copied the objects based on their respective bounding boxes into the corresponding directories. Secondly, our annotators manually verified if the objects were correctly placed in their designated directories through simple inspection, which is highly accurate and requires less time and effort. However, this approach is blind to objects that were not labeled in the first place, which is known as a missing label error. To address this issue, we inspected the False Positives generated by the YOLOv7 model [20] trained on FishEye8K, which helped identify numerous missing label errors. This approach was especially effective in identifying errors in distant areas and regions with high traffic density of vehicles and bikes.

3.5. Dataset Splits

In order to minimize dataset bias, we ensured that frames from the same camera were not included in both the train and test sets. Specifically, all frames from a given camera were assigned to either the train or test set. Figure 4 illustrates the heat maps of 22 videos (captured during morning, afternoon, evening, and night) recorded by Cameras 1-18, from which all images were extracted to create the FishEye8K dataset. To satisfy the criteria, we selected Cameras 1, 2, 4, and 7 for the test set and the remaining cameras for the training set. This division resulted in a training set that constitutes 66.07% of the dataset, while the test set constitutes 33.93%.

In order to maintain a roughly 70:30 ratio of objects for each class, the training set was composed of 111,835 objects and the test set contained 45,193 objects, which correspond to 71.28% and 28.78% of all objects, respectively. The classes Bike, Bus, and Car follow this ratio in both sets.

3.6. Data Anonymization

The identification of road participants such as people's faces and vehicle license plates from the dataset images was found to be unfeasible due for various reasons. The cameras used for capturing the images were installed at a higher ground level, making it difficult to capture clear facial features or license plates, especially when they are far away. Additionally, the pedestrians are not looking at the cameras, and license plates appear too small when viewed from a distance. However, to maintain ethical compliance and protect the privacy of the road participants, we blurred the areas of the images containing the faces of pedestrians and the license plates of vehicles, whenever they were visible.

4. Benchmark

4.1. One-Stage 2D Object Detection Methods

In order to assess the performance of 2D object detection methods, particularly for pedestrian and vehicle detection, we conducted a benchmark of the latest state-of-the-art one-stage detectors. Our selection process involved reviewing the literature and identifying the best-performing models, including YOLOv5 [7], YOLOR [19], YOLOv7 [20], and the latest YOLOv8. One-stage detectors predict bounding boxes on images without requiring a region proposal step, which results in faster processing times and makes them suitable for real-time applications. However, these detectors prioritize inference speed and may not perform as well for recognizing irregularly shaped objects or groups of small

objects. Table 2 presents the results of our benchmark of the one-stage detectors.

4.2. Training Procedure

We utilized several frameworks and platforms, i.e., Darknet [17], Pytorch [16], and PaddlePaddle [13], for the model training.

Hyperparameters. All YOLO variations were pre-trained on MS COCO [11] dataset. Among the models, we trained four models (YOLOv7 [20], YOLOv7-X [20], YOLOv8l, and YOLOv8x on the input size 640×640. Six models (YOLOv5x6 [7], YOLOv5l6 [7], YOLOR-W6 [19], YOLOR-P6 [19], YOLOv7-D6 [20], YOLOv7-E6E [20]) on the input size 1280×1280. All models have trained with the same training procedures for 250 epochs, Adam [8] optimizer with the momentum of 0.937 except for YOLOv5 [7] which employed SGD optimizer. The confidence and NMS (Non Max Suppression) IoU (Intersection over Union) thresholds were both 0.5, and a learning rate of 0.01.

Data preprocessing. For the purpose of training and testing, the input images were resized to 640×640 and 1280×1280 for particular models, see Table 2.

Loss Objective. We employed the Focal loss [10] as it is commonly used in the multi-object detection and multi-label image classification domain. The loss function is defined as:

$$FL(p_t) = -\alpha_t(1 - p_t)^{\gamma} log(p_t), \tag{1}$$

where by default $\gamma = 0.5$ and $\alpha = 0.5$, p_t is the predicted probability for the object indexed by t.

4.3. Metrics

All models are analyzed and evaluated with the same metrics, i.e., *Precision*, *Recall*, *mAP* s, AP_S, AP_M, AP_L, $F1$ *score*, and their inference time.

F1-score metric measures the balance between *Precision* and *Recall*. When both *Precision* and *Recall* are high, the $F1$ score is high as well, indicating good model performance. On the other hand, a low $F1$ score indicates that the *Precision* and *Recall* values are imbalanced, and the model is not performing well. The $F1$ score is calculated as below:

$$F_1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{2}$$

Average Precision (*AP*) represents all *Precision* and *Recall* values into a single score. The *AP* is calculated according to:

$$AP = \sum_{k=0}^{n-1} [Recall_{(k+1)} - Recall_{(k)}] * Precision_{(k+1)},$$

where k is an index of the frame, and n is the number of frames for a given class.

Intersection over Union (IoU). The model predicts the bounding boxes of the detected objects; however, it is expected that the predicted box will not match exactly the ground truth box. Intersection over Union (IoU) is employed to quantify the measure to score how the ground truth and predicted boxes match: $IoU = \frac{Intersection\ Area}{Union\ Area}$.

Normalized Confusion Matrix is used to determine the prediction quality of the model by each class. A confusion matrix is made up of 4 components, namely, True Positive (*TP*), True Negative (*TN*), False Positive (*FP*), and False Negative (*FN*).

Mean Average Precision (*mAP* s) is the mean of the *AP* s for all classes. The *mAP* of the object detection model is calculated according to:

$$mAP = \frac{1}{n} \sum_{k=1}^{n} AP_k, \tag{3}$$

where n is the number of classes in the dataset and $AP(k)$ is the average precision (AP) for a given class k.

4.4. Performance

In this subsection, we report the experimental results of variations of YOLOv5 [7], YOLOR [19], YOLOv7 [20], and YOLOv8.

Table 2 presents two sets of models that were trained on the FishEye8K dataset, with input sizes of 1280×1280 and 640×640.

4.4.1 Results on Input Size 640 × 640

For input size 640×640, the highest two $mAP_{0.5}$s of 0.6146 and 0.612 are achieved by YOLOv8x and YOLOv8l, respectively. The lowest $mAP_{0.5}$s of 0.4235 is result of YOLOv7 [20]. In terms of *F1-score* and *Recall*, YOLOv7-X achieved the highest performance with 0.5794 and 0.4888, respectively. Further, in terms of object scale, YOLOv7-X outperformed on all three scales (small, medium, and large) as well.

The confusion matrix for the best-performing model, YOLOv8x, on the input size of 640×640, is presented in Figure 5, and Table 3 tabulates the results. The Car class achieved the highest $mAP_{0.5}$ score of 0.749, followed by Bus, Bike, Truck, and finally Pedestrian with a score of 0.4596. Surprisingly, the Bike class had the highest FP rate of 0.82, with many objects mispredicted as Bike on the background. Additionally, a significant portion of objects across all classes were undetected, with normalized FN s ranging from 0.45 to 0.84. However, the model performed significantly well in terms of *Precision* for all classes, with values ranging from 0.74 to 0.94. The Pedestrian class had

Model	Version	Input Size	*Precision*	*Recall*	$mAP_{0.5}$	$mAP_{.5:.95}$	*F1-score*	AP_S	AP_M	AP_L	Inference [ms]
YOLOv5 [7]	YOLOv5l6	1280×1280	0.7929	0.4076	0.6139	0.4098	0.535	0.1299	0.434	0.6665	22.7
	YOLOv5x6	1280×1280	**0.8224**	0.4313	0.6387	0.4268	0.5588	0.133	0.452	0.6925	43.9
YOLOR [19]	YOLOR-W6	1280×1280	0.7871	0.4718	0.6466	**0.4442**	0.5899	0.1325	0.4707	0.6901	16.4
	YOLOR-P6	1280×1280	0.8019	0.4937	**0.6632**	0.4406	0.6111	0.1419	0.4805	**0.7216**	**13.4**
YOLOv7 [20]	YOLOv7-D6	1280×1280	0.7803	0.4111	0.3977	0.2633	0.5197	0.1261	0.4462	0.6777	26.4
	YOLOv7-E6E	1280×1280	0.8005	**0.5252**	0.5081	0.3265	**0.6294**	**0.1684**	**0.5019**	0.6927	29.8
YOLOv7 [20]	YOLOv7	640×640	0.7917	0.4373	0.4235	0.2473	0.5453	0.1108	0.4438	0.6804	**4.3**
	YOLOv7-X	640×640	0.7402	**0.4888**	0.4674	0.2919	**0.5794**	**0.1332**	**0.4605**	**0.7212**	6.7
YOLOv8	YOLOv8l	640×640	0.7835	0.3877	0.612	0.4012	0.5187	0.1038	0.4043	0.6577	8.5
	YOLOv8x	640×640	**0.8418**	0.3665	**0.6146**	**0.4029**	0.5106	0.0997	0.4147	0.7083	13.4

Table 2. Results of state-of-the-art models trained on FishEye8K datasets. The table consists of two groups of various versions of YOLO object detection models for input sizes 1280×1280 and 640×640.

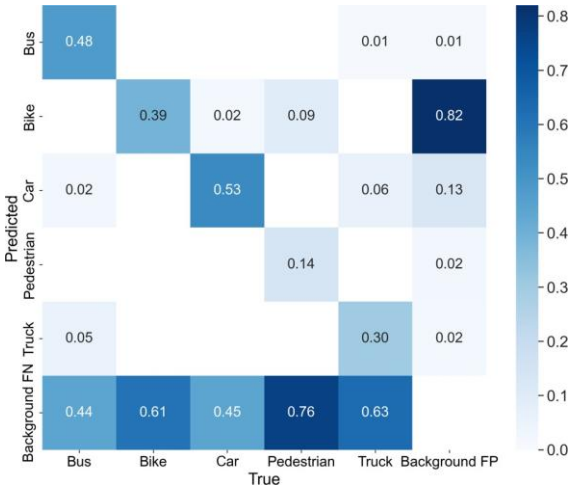


Figure 5. Normalized Confusion Matrix of YOLOv8x model on the input size 640 × 640.

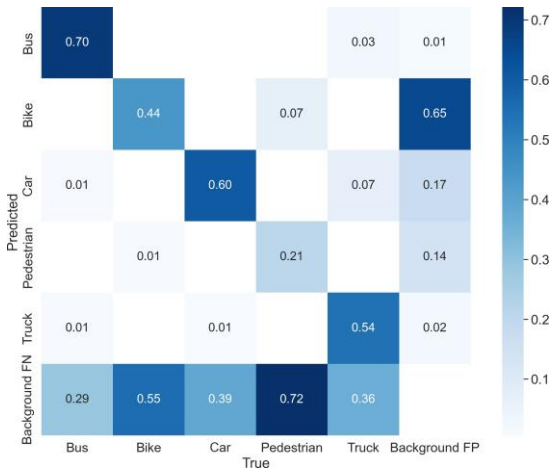


Figure 6. Normalized Confusion Matrix of YOLOR-P6 model on input size 1280 × 1280.

YOLOv8x-640 640					
Classes	***Precision***	***Recall***	× $mAP_{0.5}$	$mAP_{.5:.95}$	***F1-score***
Bike	0.8035	0.377	0.6062	0.3208	0.5132
Car	0.9493	0.5331	0.749	0.5208	0.6827
Pedestrian	0.7785	0.1402	0.4596	0.2168	0.2376
Truck	0.7444	0.3028	0.5424	0.4141	0.4304
All	**0.8418**	**0.3665**	**0.6146**	**0.4029**	**0.5106**

Table 3. Results of YOLOv8x model on the input size 640 × 640.

YOLOR-P6-1280 1280 [19]					
Classes	***Precision***	***Recall***	× $mAP_{0.5}$	$mAP_{.5:.95}$	***F1-score***
Bike	0.8537	0.4316	0.6553	0.3725	0.5733
Car	0.9473	0.6062	0.7876	0.5575	0.7393
Pedestrian	0.4903	0.2014	0.3621	0.2007	0.2855
Truck	0.7753	0.5541	0.695	0.4451	0.6462
All	**0.8019**	**0.4937**	**0.6632**	**0.4406**	**0.6111**

Table 4. Results of YOLOR-P6 model on the input size 1280×1280.

the lowest normalized *TP* rate at 0.14, indicating incorrect predictions of this class as others, mainly as Background which has the maximum normalized *FN* rate at 0.76.

4.4.2 Results on Input Size 1280 × 1280

Table 2 shows that for an input size of 1280 × 1280, YOLOR-P6 [19] and YOLOR-W6 [19] achieved the highest $mAP_{0.5}$ scores of 0.6632 and 0.6466, respectively. In contrast, YOLOv7-D6 [20] yielded the lowest $mAP_{0.5}$ score of 0.3977. YOLOv7-E6E [20] demonstrated the highest performance in terms of *F1-score* and *Recall*, with values of 0.6294 and 0.5252, respectively.

Furthermore, with regard to object scale, YOLOv7-E6E [20] exhibited higher performance over the other models in detecting small and medium-sized objects, achieving AP_S of 0.1684 and 0.5019, respectively. In contrast, YOLOR-P6 [19] demonstrated exceptional accuracy in detecting large objects, with an AP_L of 0.7216.

Figure 6 shows the confusion matrix and Table 4 tabulates the results provided by the best-performing model YOLOR-P6 [19] on the input size of 1280 × 1280. The most accurately predicted class is Bus with an $mAP_{0.5}$ of 0.8161 followed by Car, Truck, Bike and finally Pedestrian with $mAP_{0.5}$ of 0.3621.

The Bike has the maximum normalized FP rate at 0.65 when the background is incorrectly detected as Bike. Ad-

ditionally, a substantial fraction of objects in each class remains undetected, as indicated by their normalized *FN* rates varying between 0.29 to 0.72. Despite this, the model demonstrates comparatively good performance in terms of *Precision* across all classes, with values ranging from 0.77 to 0.95, with the exception of the Pedestrian class, which displays a significantly low *Precision* of 0.49.

4.4.3 Inference Time

The inference time for each model was measured on a workstation featuring an 11^{th} Gen i7 CPU and an Nvidia RTX 3080 GPU, and the results are presented in Table 2. The outcomes demonstrate that all models perform efficiently on this high-end computer, with inference times varying between 4.3 ms to 43.9 ms.

5. Discussions

The majority of the dataset, consisting of images from Cameras 1-15, were derived from fisheye surveillance camera footage captured on a single day in July 2018 in Taiwan. Although the dataset contains images of 5 major road participants captured from varying angles and under different illumination conditions, it lacks diversity in terms of weather conditions, such as fog, rain, snow, and storms. Additionally, the dataset is imbalanced, with the class Bike having the highest number of objects at 88K, while the Bus class has the lowest number at 2.98K.

Hard cases of the best-performing YOLOR-W6 [19] are represented by few samples in Figure 7.

In Figure 7(a), several examples of false positives are shown where the labeled objects are not detected. These instances can be categorized into two groups: parked/stationary vehicles and road participants in motion. In the top left, only two out of nine scooters parked in a row on the sidewalk are correctly detected. On the top right, two partially visible cars parked in a garage are not detected. The presence of numerous parked vehicles in the dataset and the misdetection of such vehicles contribute to the high false negative rates observed across all classes.

The second type of false positives involves road participants in motion, such as a truck, a pedestrian, and a bus shown in the three crops at the bottom of Figure 7(a)

The examples shown in Figure 7(b) illustrate instances where the background is misclassified as one of the object classes, resulting in higher false positive rates. Specifically, in the top left, a road sign is incorrectly detected as a Pedestrian, while in the bottom left, a yellow building is misclassified as a Bus. In the center, a building pillar is erroneously labeled as a Pedestrian, and on the right, a horizontal road sign is detected as a Bike.

In Figure 7(c), we can observe cases where classes are misclassified as other classes. The four images, from the bottom to the top, show how the predictions change as Pedestrians walk away from the camera. We can see that misclassification occurs when the size of the objects gets smaller. Specifically, the objects were initially correctly detected as Pedestrians when they were closer to the camera, but as they moved away and became smaller, they were misclassified as Bikes.

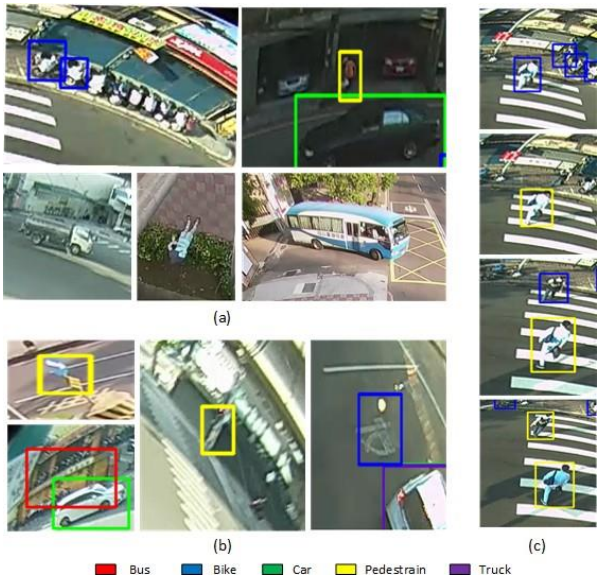


Figure 7. Some samples of hard cases of YOLOR-P6 detections on input size 1280 × 1280.

6. Conclusions

We presented the FishEye8K benchmark dataset along with the evaluation of the SoTA one-stage object detectors for the use of fisheye cameras for road object detection. This dataset fills the gap in the lack of a fisheye surveillance camera dataset for road 2D object detection tasks. The anonymized dataset includes 8000 frames with 157K bounding boxes of 5 different road participants and various aspects of road conditions. Our evaluation results show that YOLOv8 and YOLOR models [19], which are pretrained on MS-COCO [11], outperforms the other models. Therefore the FishEye8K dataset will be a significant contribution to the fisheye video analytics and smart city applications.

Future work includes the creation of a large and more balanced dataset with more diverse street object categories that can be used for object re-identification model training and evaluation.

Acknowledgements. Emirates Center for Mobility Research (EMCR) provided support for our research through Grant 12R012, while SciDM and National Center for High-performance Computing (NCHC) provided necessary storage resources.

References

[1] Chris H Bahnsen and Thomas B Moeslund. Rain removal in traffic surveillance: Does it matter? *IEEE Transactions on Intelligent Transportation Systems*, 20(8):2802–2819, 2018. 2, 3

[2] Dawei Du, Yuankai Qi, Hongyang Yu, Yifan Yang, Kaiwen Duan, Guorong Li, Weigang Zhang, Qingming Huang, and Qi Tian. The unmanned aerial vehicle benchmark: Object detection and tracking. In *ECCV*, pages 370–386, 2018. 2, 3

[3] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman. The PASCAL Visual Object Classes Challenge 2012 (VOC2012) Results. http://www.pascal-network.org/challenges/VOC/voc2012/workshop/index.html. 2, 4

[4] Andreas Geiger, Philip Lenz, and Raquel Urtasun. Are we ready for autonomous driving? the kitti vision benchmark suite. In *CVPR*, pages 3354–3361. IEEE, 2012. 2

[5] Meng-Ru Hsieh, Yen-Liang Lin, and Winston H Hsu. Drone-based object counting by spatially regularized regional proposal network. In *ICCV*, pages 4145–4153, 2017. 2, 3

[6] Itay Klein, Nexar Blog. NEXET - the largest and most diverse road dataset in the world, 2017. https://data.getnexar.com/blog/nexet-the-largest-and-most-diverse-road-dataset-in-the-world, Last accessed on 2021-10-24. 2

[7] Glenn Jocher, Alex Stoken, Jirka Borovec, NanoCode012, ChristopherSTAN, Liu Changyu, Laughing, tkianai, yxNONG, Adam Hogan, lorenzomammana, AlexWang1900, Ayush Chaurasia, Laurentiu Diaconu, Marc, wanghaoyang0106, ml5ah, Doug, Durgesh, Francisco Ingham, Frederik, Guilhen, Adrien Colmagro, Hu Ye, Jacobsolawetz, Jake Poznanski, Jiacong Fang, Junghoon Kim, Khiem Doan, and Lijun Yu. ultralytics/yolov5: v4.0 - nn.SiLU() activations, Weights & Biases logging, PyTorch Hub integration, Jan. 2021. 2, 3, 4, 5, 6, 7

[8] Diederik P. Kingma and Jimmy Ba. Adam: A method for stochastic optimization, 2014. 6

[9] Roman Kvyetnyy, Roman Maslii, Volodymyr Harmash, Ilona Bogach, Andrzej Kotyra, aklin, Aizhan Zhanpeisova, and Nursanat Askarova. Object detection in images with low light condition. In *Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2017*, volume 10445, page 104450W. International Society for Optics and Photonics, 2017. 2

[10] Tsung-Yi Lin, Priya Goyal, Ross B. Girshick, Kaiming He, and Piotr Dollár. Focal loss for dense object detection. *CoRR*, abs/1708.02002, 2017. 6

[11] Tsung-Yi Lin, Michael Maire, Serge J. Belongie, Lubomir D. Bourdev, Ross B. Girshick, James Hays, Pietro Perona, Deva Ramanan, Piotr Dollár, and C. Lawrence Zitnick. Microsoft COCO: common objects in context. *CoRR*, abs/1405.0312, 2014. 2, 4, 6, 8

[12] Zhiming Luo, Frederic Branchaud-Charron, Carl Lemaire, Janusz Konrad, Shaozi Li, Akshaya Mishra, Andrew Achkar, Justin Eichel, and Pierre-Marc Jodoin. Mio-tcd: A new benchmark dataset for vehicle classification and localization. *IEEE Transactions on Image Processing*, 27(10):5129–5141, 2018. 2, 3

[13] Yanjun Ma, Dianhai Yu, Tian Wu, and Haifeng Wang. PaddlePaddle: An open-source deep learning platform from industrial practice. *Frontiers of Data and Domputing*, 1(1):105, 2019. 6

[14] Milind Naphade, Shuo Wang, David C Anastasiu, Zheng Tang, Ming-Ching Chang, Xiaodong Yang, Yue Yao, Liang Zheng, Pranamesh Chakraborty, Christian E Lopez, et al. The 5th ai city challenge. In *CVPR*, pages 4263–4273, 2021. 2, 3

[15] Constantine Papageorgiou and Tomaso Poggio. A trainable system for object detection. *International journal of computer vision*, 38(1):15–33, 2000. 2, 3

[16] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, Alban Desmaison, Andreas Kopf, Edward Yang, Zachary DeVito, Martin Raison, Alykhan Tejani, Sasank Chilamkurthy, Benoit Steiner, Lu Fang, Junjie Bai, and Soumith Chintala. Pytorch: An imperative style, high-performance deep learning library. In *Advances in Neural Information Processing Systems 32*, pages 8024–8035. Curran Associates, Inc., 2019. 6

[17] Joseph Redmon. Darknet: Open source neural networks in C. http://pjreddie.com/darknet/, 2013–2016. 6

[18] Joseph Redmon, Santosh Kumar Divvala, Ross B. Girshick, and Ali Farhadi. You only look once: Unified, real-time object detection. *CoRR*, abs/1506.02640, 2015. 2, 4

[19] Chien-Yao Wang, I-Hau Yeh, and Hong-Yuan Mark Liao. You only learn one representation: Unified network for multiple tasks. *CoRR*, abs/2105.04206, 2021. 2, 5, 6, 7, 8

[20] Chien-Yao Wang, Alexey Bochkovskiy, and Hong-Yuan Mark Liao. YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. *arXiv preprint arXiv:2207.02696*, 2022. 2, 5, 6, 7

[21] Longyin Wen, Dawei Du, Zhaowei Cai, Zhen Lei, Ming-Ching Chang, Honggang Qi, Jongwoo Lim, Ming-Hsuan Yang, and Siwei Lyu. DETRAC: A new benchmark and protocol for multi-object tracking. *CoRR*, abs/1511.04136, 2015. 2, 3

[22] Huazhe Xu, Yang Gao, Fisher Yu, and Trevor Darrell. End-to-end learning of driving models from large-scale video datasets. In *CVPR*, pages 2174–2182, 2017. 2

[23] Senthil Yogamani, Ciarán Hughes, Jonathan Horgan, Ganesh Sistu, Padraig Varley, Derek O'Dea, Michal Uricár, Stefan Milz, Martin Simon, Karl Amende, et al. WoodScape: A multi-task, multi-camera fisheye dataset for autonomous driving. In *ICCV*, pages 9308–9318, 2019. 2

[24] Fisher Yu, Haofeng Chen, Xin Wang, Wenqi Xian, Yingying Chen, Fangchen Liu, Vashisht Madhavan, and Trevor Darrell. Bdd100k: A diverse driving dataset for heterogeneous multitask learning. In *CVPR*, pages 2636–2645, 2020. 2

ДҮРС БОЛОВСРУУЛАЛТ, ХИЙМЭЛ ОЮУН УХААН АШИГЛАН НИСГЭГЧГҮЙ НИСЭХ ХЭРЭГСЭЛ ИЛРҮҮЛЭХ АРГЫН СУДАЛГАА

Б.Мөнх-Учрал[1], О.Мөнх-Эрдэнэ[1] Б.Дорж[1]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбоо технологийн сургууль, Элетроникийн салбар[1]
uchraluchral1119@gmail.com, omunkhuush01@gmail.com, dorj@must.edu.mn

Хураангуй—Энэ нийтлэлд нисгэгчгүй нисэх хэрэгслийг илрүүлэх аргын судалгааг толилуулж байна. Техник технологийн дэвшил хурдацтай хөгжиж буй эрин үед нисгэгчгүй нисэх хэрэгсэл нь хүмүүсийн сонирхлыг ихэд татаж хүмүүс өдөр тутмын амьдралдаа тогтмол ашиглах болсон. Бүх төрлийн ашуулгүй байдлын үүднээс нисгэгчгүй нисэх хэрэгсэл объект руу ойртож буйг илрүүлэх нь нэн чухал. Дүрс боловсруулалт, хиймэл оюун ухаан ашиглан нисгэгчгүй нисэх хэрэгсэл илрүүлэх арга нь видео дүрсэнд боловсруулалт хийн машин сургалт дээр үндэслэн объектыг илрүүлэх зориулалттай. Нисгэгчгүй нисэх хэрэгслийн загвар хийц, хөдөлгөөн зэргээс хамааран дүрсэн дээрх объектын байршлыг үнэн зөв бодит цагт хугацааны хоцрогдолгүй харуулахыг зорьсон. Үүний тулд машин сургалтыг явуулахад шаардагдах өгөгдлийн санг монгол орны цаг агаар, орчин нөхцөл, газар зүйн онцлогт тохируулан нисгэгчгүй нисэх хэрэгслийн бичлэг, зургаар бүрдүүлсэн. Уг судалгааны үр дүнд өндөр өртөг бүхий радарын системийн оронд өөрийн улсын онцлогт тохируулан дүрс боловсруулалт, хиймэл оюун ухаан ашиглан нисгэгчгүй нисэх хэрэгсэл илрүүлэх аргыг хэрэглээнд нэвтрүүлэх боломжтойг харууллаа.

Түлхүүр үг— Нисгэгчгүй нисэх хэрэгсэл, суралцах, камер, нисгэгчгүй нисэх хэрэгсэл илрүүлэх, машин сургалт

V УДИРТГАЛ

Нисгэгчгүй нисэх хэрэгсэл гэгддэг бичил агаарын тээврийн хэрэгслийн дэвшил нь аж ахуйн инженерчлэлээс эхлээд дайны голомтын гол хэрэгсэл хүртлээ өргөжин тэлж цаг минутаар хөгжсөөр байна. Нисгэгчгүй нисэх хэрэгсэл үйлдвэрлэлийн хурдацтай тэлэлт нь зарим тал дээр хууль бус тээвэрлэлт, хадлага болон гэмт хэргийн томоохон хэрэгсэл болж байна[1]. Үүнтэй зэрэгцэн Монгол улсын хэмжээнд нисгэгчгүй нисэх хэрэгсэл хэрэглэгчдийн тоо эрс нэмэгдсэн.

Их Британийн хоёр дахь том нисэх онгоцны буудал болох Гатвик нисэх онгоцны буудал 2018 оны 12-р сард хууль бус нисгэгчгүй нисэх хэрэгслүүд хөөрөх зурвасын ойролцоо агаарын орон зайд 15 цагийн турш 50 гаруй удаагийн давтамжтай нислэг үйлдсэн.

Германы Франкфуртын нисэх онгоцны буудлын ойролцоо 2019 оны 05-р сард нэг цагийн турш онгоцны буух хэсэгт ойрхон гарч ирсэн.

2011 оны 09-р сард С-4 бөмбөгөөр тоноглогдсон нисгэгчгүй нисэх хэрэгсэл АНУ-ын Батлан хамгаалах яам болон Капитол толгод руу халдага үйлдэх ородлого үйлдсэн.

ОХУ-ын Агаарын довтолгооны хамгаалах хүчин 2018 оны 1-р сард нисгэгчгүй нисэх хэрэгслийн анхны дайралтыг хамгаалсан түүхтэй. Агаарын довтолгооны хамгаалах хүчний бааз болон Тартусын тэнгисийн цэргийн байгууламж руу довтлохоор 13 зэвсэглэсэн нисгэгчгүй нисэх хэрэгслүүдийг байрлуулсан боловч Оросын цэргийн радио электрон тэмцэгч технологийн тусламжтайгаар няцаав. 10 нисгэгчгүй нисэх хэрэгслийг пуужингаар харваж, үлдсэн гурвыг нь ОХУ-ыг онгоц барьцаалах технологиор саатуулсан.

2019 оны 09-р сард Саудын Арабын үндэсний хамгийн томд тооцогдох газрын тосны компани болох Aramco нь нисгэгчгүй нисэх хэрэгслийн дайралтад өртөн хаагдсан. Арван нисгэгчгүй нисэх хэрэгсэл тус байгууламж руу довтолж, нэг нэгжид 3 кг тэсрэх бодис ачсан байсан [1].

Дэлхий дахинд өрнөж буй Израиль Палестин, Орос Украйны дайны бүх үйл ажиллагаанд дрон болон нисгэгчгүй нисэх хэрэгсэл өндөр үүрэг гүйцэтгэлтэйгээр оролцож байна. Өдөр тутмын дайралтад нисгэгчгүй нисэх хэрэгслээр мэдээлэл цуглуулах, байршил тогтоох, бөмбөгдөх, цэрэг тээвэрлэх, камиказе дроноор дайралт хийх мөргөлдөөнийг эхлүүлэхэд ашиглагдаж байна. Энэхүү дайнд дрон нь тулааны гол түлхүүр болж байна. Хоёр талын аль аль нь дрон ашиглан дайралтыг хийж байгаа юм. Мөн 2020 онд өрнөсөн Азербайжан, Армен улсуудын хоорондох зэвсэгт мөргөлдөөнд нисгэгчгүй нисэх хэрэгсэл нь гол хүчийг бүрдүүлж байсан юм.

Энэхүү нийтлэлд дурдсан асуудлыг шийдэх энгийн нэг шийдэл нь дүрс боловсруулалт, машин сургалт ашигласан дрон илрүүлэх арга юм.

Энэхүү арга нь камерт буусан нисгэгчгүй нисэх хэрэгслийн дүрсийг объект болгон тэмдэглэж машин сургалтын Pandas сангийн тусламжтайгаар нисгэгчгүй нисэх хэрэгслийг тодорхойлсон.

Уг судалгаанд өгөгдлийг санг Монгол орны орчин нөхцөл, байгаль цаг уурт тохируулан видео дүрснүүд хийгдсэн ба нэмэлтээр цахим орчноос татан авч ашигласан. Мөн машин сургалтаар 45 орчим төрлийн нисгэгчгүй нисэх хэрэгслийн загварт суралцуулсан нь объектыг ялгах чадвар нэмэгдсэн.

Тус судалгааны ажлыг өмнө нь Монгол улсын хэмжээнд хийж байсан илэрцгүй ба бусад орны ижил төстэй судалгаатай харьцуулахад илрүүлэх чадамж илүү гэж үзэж байна.

II НИСГЭГЧГҮЙ НИСЭХ ХЭРЭГСЛИЙГ ИЛРҮҮЛЭХ АРГА

Нисгэгчгүй нисэх хэрэгслүүдийн илрүүлэх систем нь зөвхөн нисгэгчгүй агаарын тээврийн хэрэгслийг илрүүлэх, нутаг дэвсгэрт нэвтэрч буй дронуудаас хамгаалах зориулалттай.

- Дулааны илрүүлэлт
- RF Сканер илрүүлэлт
- Радарт суурилсан илрүүлэлт
- Оптик камерын илрүүлэлт
- Акустик дохио илрүүлэлт

Хүснэгт 1: Нисгэгчгүй нисэх хэрэгслүүдийн илрүүлэх аргууд.

Аргууд	Мэдрэгч төхөөрөмж	Давуу тал	Сул тал	Илрүүлэх алс
Дулаан	Хэт улаан туяны камер	Цаг агаарын нөлөөнд бага өртдөг Холын зайнд ашиглах боломжтой	Нарийвчлал бага	1-15 км
Радио давтамжийн дохио	Радио давтамжын хүлээн авагч	Саад бэрхшээлгүй Дрон илрүүлдэг	Давтамж таарахгүй байх магадлал бага	1-20 км
Радар	Радар	Цаг агаарын нөлөөнд бага өртдөг Холын зайнд ашиглах боломжтой	Өндөр зардалтай	1-20 км
Камер	Оптик	Бага зардалтай Харагдах байдлыг сайн тодорхойлдог	Цаг агаарын нөхцөл байдлаас хамааралтай	0.5-3 км
Акустик дохио	Акустик (дуу чимээ) хүлээн авагч	Радио давтамж дээр суурилсан мэдрэгчтэй нийцдэг Жижигрүүрлэсн	Илрүүлэх хүрээ маш муу Нарийвчлал бага	<0.2 км

Радарын тандалт, хяналт нь хэд хэдэн давтамжийн зурвасыг ашигладаг бөгөөд бид үүнийг доор тоймлон харуулав[15], [16].

- X зурвас, 8-12 GHz. Цэргийн тагнуулын болон синтетик диафрагмын радарын агаарын системд өргөн хэрэглэгддэг.
- C зурвас, 4–8 GHz. Агаарын судалгааны олон систем (жишээ нь CCRS Convair-580 ба NASA Air SAR) болон сансрын системд түгээмэл байдаг.
- S зурвас, 2–4 GHz. Оросын ALMAZ хиймэл дагуул, цаг агаарын радарт ашигладаг.
- L зурвас, 1–2 GHz. АНУ-ын SEASAT болон Японы JERS-1 хиймэл дагуул, НАСА-гийн агаарын системд ашигладаг.
- P зурвас, 300 kHz-ээс 1 GHz хүртэл. НАСА-гийн туршилтын агаарын судалгааны системд ашигладаг хамгийн урт радарын долгионы урт.

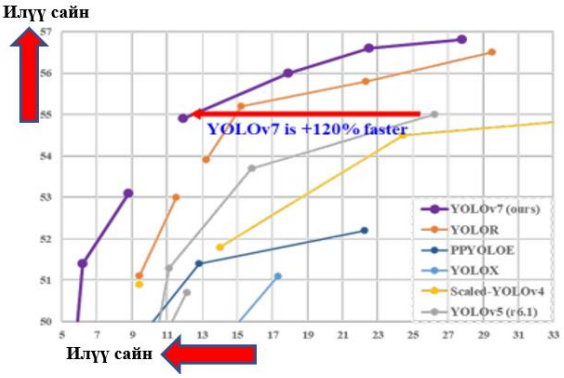
Дүрс боловсруулалтын аргаар нисгэгчгүй нисэх хэрэгсэл илрүүлэх арга

Дүрс боловсруулалтын (камер) арга нь хөдөлгөөнт агаарын объектын байршлыг тогтооход хяналтын камер ашиглан нисгэгчгүй нисэх хэрэгслүүдийн хэмжээ хийц, нислэгийн зам, хөдөлгөөний хэв маягаар илрүүлэх боломжтой.

Видео дүрсэндэх нисгэгчгүй нисэх хэрэгслийг илрүүлэхийн тулд дүрс болгонд объект илрүүлэх алгоритмыг ашигладаг. Ялангуяа каскадын ангилал нь объект илрүүлэхэд тохиромжтой. Урьдчилан бэлдсэн төрөл бүрийн нисгэгчгүй нисэх хэрэгслийн дүрс дээр суурилсан машин сургалтын тусламжтайгаар систем нь дүрснээс дроныг үнэн зөв нарийвчлалтай илрүүлэх талаар суралцдаг.

1-р зураг. Дрон илрүүлэх, таних системийн үйл явц.

Машин сургалт бол компьютерт суралцах боломжийн заадаг хиймэл оюун ухааны арга юм. YOLOv7 нь өнөөг хүртэл хамгийн хурдан бөгөөд бодит цагийн объект илрүүлэгч юм.

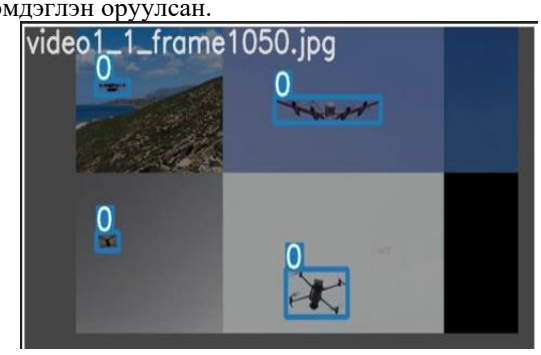


2-р зураг. Бусад объект илрүүлэгчтэй харьцуулбал YOLOv7 нь хамгийн сүүлийн үеийн гүйцэтгэлтэй .

III СУДАЛГАА ТУРШИЛТ, УР ДҮН

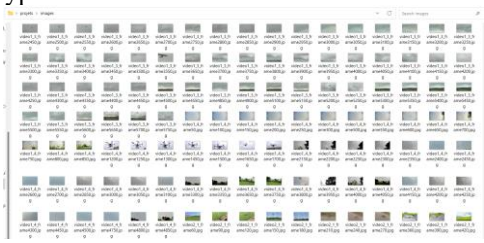
Машин сургалтаар сургахдаа нийт 3924 дүрс цуглуулсны 80% буюу 3137 сургалт явуулахад, 20% буюу 787 дүрсийг тест явуулахад ашигласан.

Судалгааны өгөгдлийн санг бүрдүүлэхдээ орчин нөхцөл, байгаль цаг уурт тохируулан видео дүрснүүд хийгдсэн ба нэмэлтээр цахим орчноос татан авсан төрөл бүрийн ойролцоогоор 45 ялгаатай нисгэгчгүй нисэх хэрэгслийн жишээнүүдээр бүрдүүлэн, зураг бүрээс нисгэгчгүй нисэх хэрэгслийн гараар тэмдэглэн оруулсан.

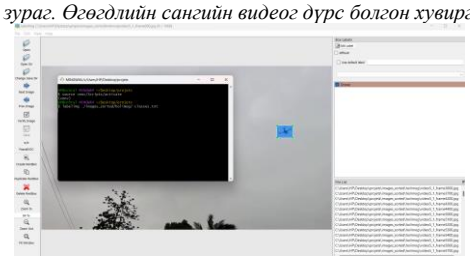


3-р зураг. Дүрснээс нисгэгчгүй нисэх хэрэгсэл илрүүлэх.

Нийт 5 хэсэгт (цастай, бүрхэг бороотой, нартай, улирлууд, холимог) ангилан видео дүрсээ Python ашиглан *.jpg өргөтгөлтэй зураг болгосон. /4-р зураг -6-р зураг/.

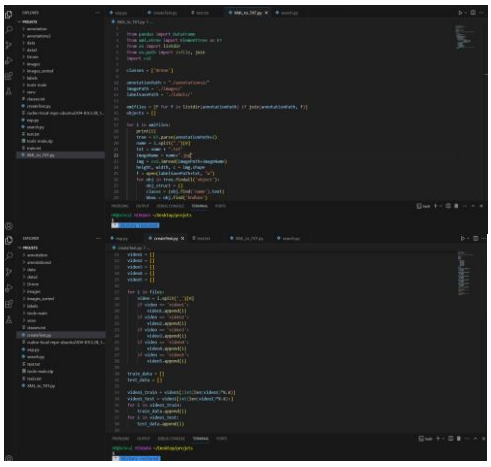


4-р зураг. Өгөгдлийн сангийн видеог дүрс болгон хувиргалт



5-р зураг. Дүрснүүдээ тэмдэглэн .xml файл болгон хувиргаж буй байдал.

Дүрснүүдийн тус бүрийн объекттой хэсгээ тэмдэглэн *.xml файл үүсгэн лабел хийхэд бэлтгэсэн. Бүх дүрсээ Python-ний тусламжтайгаар *.txt файл /XML_to_TXT/ болгон хувиргалт хийн лабел үүсгэхэд бэлтгэсэн.



6-р зураг. XML_to_TXT үүсгэн сургалт болон тест хийх файлын бэлдэц.

Бэлэн болсон *.txt файлынхаа 80%-ийг сургалт явуулахад, 20%-ийг тест явуулахад ашиглах зорилгоор ангилан машин сургалт хийхэд бэлэн болгосон.

Сургалт: 2023.11.07-нооc 11.08-ны өдрийн хооронд Yolov7 сан ашиглан 21 цагийн хугацаатай нисгэгчгүй нисэх хэрэгсэл таниулах сургалтыг явуулсан.

7-р зураг Нисгэгчгүй нисэх хэрэгсэл таниулах анхны туршилт амжилттай явагдсан.

Машин сургалт явуулахад Lambda супер компьютерийн тусламжтайгаар илүү богино хугацаанд явуулсан.

Сургалт болон тест явуулахад ашиглаагүй шинэ дүрсээр туршилт хийж машин сургалтаар явуулсан туршилтаа баталгаажуулав.

9-р зураг. Бүрхэг болон цастай үед утасны камераар хийсэн туршилт.

2023.11.15-ны өдөр 365˚ PTZ 5MP 30x Zoom хяналтын камер ашиглан туршилт явуулсан ба үр дүнд ойролцоогоор 700м алсад нисгэгчгүй нисэх хэрэгслийг уг камерыэ тусламжтайгаар томруулж, жижигрүүлсэн (zoom in, zoom out) дүрсийг амжилттай таньсан.

10-р зураг 365˚*PTZ 5MP 30x Zoom хяналтын камер ашиглан хийж буй туршилт.*

IV ДҮГНЭЛТ

Энэ нийтлэлд бид видео фрейм дээр үндэслэн шийдвэр гаргах нисгэгчгүй нисэх хэрэгсэл илрүүлэх, таних системийг санал болгож байна. Энэхүү систем нь энгийн YOLOv7 ашиглан сургалтаа явуулсан боловч гүйцэтгэл сайн, маш их ирээдүйтэй гэдгийг харуулсан. Бүх системийг бодитоор хэрэгжүүлж, сургалтын мэдээллийг цуглуулсан.

Уг судалгааны туршилтын үр дүн дээр үндэслэн дүрс боловсруулалтын аргаар машин сургалт ашиглан нисгэгчгүй нисэх хэрэгсэл илрүүлсэн нь цаашид хөгжүүлэх боломжтой гэж үзэж байна. Үүнд:

- Хяналтын 360˚ PTZ камертай холбон ажиллуулах;
- Дулааны камертай хослуулан ажиллуулах;
- Нисэж өнгөрсөн замын тэмдэглэгээг (tracking) харуулах;
- Нисэж буй объектын зайг 2 болон түүнээс дээш оптик камер ашиглан тооцоолох.

Цаашид өгөгдлийн сангаа цаг агаар илүү өргөн нөхцөл байдалд (бороотой, шуургатай, нар мандах) олон төрлөөр цуглуулан нисгэгчгүй нисэх хэрэгсэл илрүүлэлтийг сайжруулах боломжтой гэж үзэж байна.

ТАЛАРХАЛ

Энэхүү судалгааны ажлыг удирдан чиглүүлсэн багш доктор Б.Дорж, машин сургалтыг сургахад туслалцаа үзүүлсэн магистрант О.Мөнх-Эрдэнэ нарт талархал илэрхийлье.

НОМ ЗҮЙ

[1]. Seongjoon Park, (Graduate Student Member, Ieee), Hyeong Tae Kim, Sangmin Lee, Hyeontae Joo, And Hwangnam Kim, (Member, IEEE) “Survey on Anti-Drone Systems: Components, Designs, and Challenges” March 2018.

[2]. Dongkyu ’Roy’ Lee, Woong Gyu La, and Hwangnam Kim School of Electrical Engineering, Korea University, Seoul, Rep. of Korea “Drone Detection and Identification System using Artificial Intelligence”

РОБОТОД ЗОРИУЛСАН БАЙРШИЛ ТОГТООХ БОЛОН ГАЗРЫН ЗУРАГ ҮҮСГЭХ АРГАЧЛАЛ

Ц.Хас-Очир[1], Б.Дорж[1]
Монгол Улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбооны Технологийн Сургууль, Электроникийн салбар[1]
hasochir1126@gmail.com, dorj@must.edu.mn

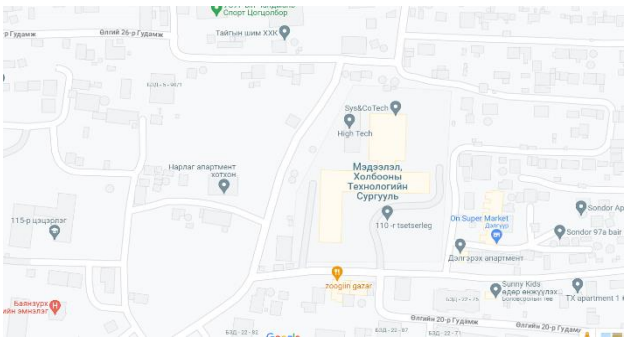
Хураангуй-Дэлхийн улс орнууд автомат машин буюу роботын талаарх янз бүрийн туршилт, судалгаа хийж зарим нь хэрэглээндээ нэвтрүүлээд эхэлсэн билээ. Харин Монгол улсын зам төлөвлөлт, дэд бүтэц зэргээс хамаарч дээрх судалгааны ажлыг үндэслэв. Энэхүү өгүүлэл нь EKF-SLAM ашиглах роботын байршилыг тогтоох болон газрын зураг үүсгэх аргачлалыг танилцуулна. Ул мэдэгдэх орчинд байршил тогтоох болон газрын зураглалыг нэгэн зэрэг хийж уг орчны шинж чанарыг дүрслэн харуулахын тулд Simultaneous Localization and Mapping [SLAM] хийнэ. Учир нь Робот болон өөрийгөө жолооддог автомашины хувьд байршил тогтоох, замчлах нь маш чухал байдаг. Гар удирдлагатай робот дээр байрлуулсан компьютер нь RVIZ программын тусламжтай лазер сканнераас авсан өгөгдлөөр газрын зураглалыг дүрслэнэ. Үр дүнд нь роботод зориулсан газрын зурагийг үүсгэж, байршилыг тогтоосон. Энэ аргачлалыг цэрэг цагдаа болон, уул уурхайн салбар гэх мэт байгууллагуудад ашиглаж болно.

Түлхүүр үг – EKF-SLAM, робот, газрын зураг, лазер сканнер, RVIZ, байршил тогтоох

I. УДИРТГАЛ

Автоматжуулсан буюу хүний хөдөлмөрийг хялбарчилсан, илүү найдвартай ажиллагааг хангасан, тухайн хүний бие махбод, оюун санааны өөрчлөлтөөс үл хамааран өөрийн үүрэгт ажлаа найдвартай гүйцэтгэдэг техникүүдийг дэлхий дахинд өргөнөөр ашиглаж байна. Орчин үед Монгол улсын инженерчлэлийн салбарт автоматжуулах, технологид суурилан үйл ажиллагаагаа зохион явуулах зэрэг шаардлагууд гарч ирдэг. Уг шаардлагууд дээр үндэслэн хүний хэрэгцээ, найдвартай ажиллагаа болон бусад хүчин зүйлүүдийг хангасан төхөөрөмж зохион бүтээхийг зорьж эхний загварыг боловсруулсан. Энэхүү загвар нь механик, электроник, програм хангамж гэсэн үндсэн 3 хэсгээс бүрдсэн ба роботын бүтэц болон зохион бүтээх үйл явцыг үндсэн дараалаллын дагуу хийж гүйцэтгэгэн туршиж байна.

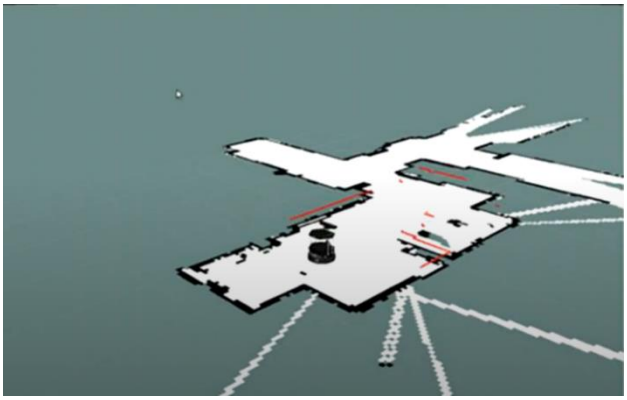
Өнөөдрийн байдлаар Монгол улсын газрын зурагийг Google map, Google earth, бүх төрлийн GPS зэрэг гадны болон дотоодын хүмүүсийн зохион бүтээсэн програм хангамж дээрээс харах, байршлыг тогтоох зэрэг арга хэмжээнүүдийг авдаг. Тэгвэл эдгээр програм нь хиймэл дагуулаас байршилийн мэдээллээ авдаг юм.



Зураг. 1. “Google map” программ дээр дүрслэгдэх 2 хэмжээст зураг

Зураг. 2. “Google earth” программ дээр дүрслэгдэх зураг

SLAM хийх үйл явц нь гар удирдлагатай робот дээр суурьлагдсан лазер сканнераас ашиглан орчин тойрны зайны хэмжилт хийнэ. SLAM гэдэг нь байршил тогтооох болон газрын зурагийг нэгэн зэрэг хийх, нэгэн зэрэг тооцоолохын зэрэгцээ үл мэдэгдэх орчинд ажиллах арга юм [1]. Энэ арга нь гадаа орчинд ашигладаг GPS, Glanoss зэрэг уламжлалт навигацын системээс ялгаатай. SLAM нь өөрөө ямар ч гадны систем, төхөөрөмжгүйгээр зөвхөн LIDAR болон IMU энкодер зэрэг мэдрэгчүүд ашигладаг. Тиймээс хөдөлгөөнт роботуудад ашиглахад тохиромжтой. Үүнд: нисгэгчтэй болон нисгэгчгүй янз бүрийн тээврийн хэрэгсэл, усан доорх робот, сансарын роботууд зэрэг багтдаг бөгөөд үндсэн хэрэгсэл нь



болсон.

Зураг. 3. RVIZ програм дээр дүрслэгдсэн 3 хэмжээст зураг

SLAM хийхийн тулд үндсэн 2 төрлийн аргыг ашигладаг. Эхнийх нь уялдуулах арга бөгөөд үүнд робот нийт туулах замын хэмжилтээр тооцдог. Алдааг багасгаж асуудлыг шийдэх нь харьцангуй нарийн, төвөгтэй байдаг тул графикт суурилсан SLAM оффлайн алгоритмыг шаарддаг. Хоёр дахь нь шүүлтүүрийн аргууд юм. Энэ нь SLAM хийхийн тулд роботын одоогийн байрлал, газрын зураг зэргээс бүрдсэн онлайн ангилалд багтдаг арга юм. Энэ ангилалд багтдаг шүүлтүүрийн аргууд нь:

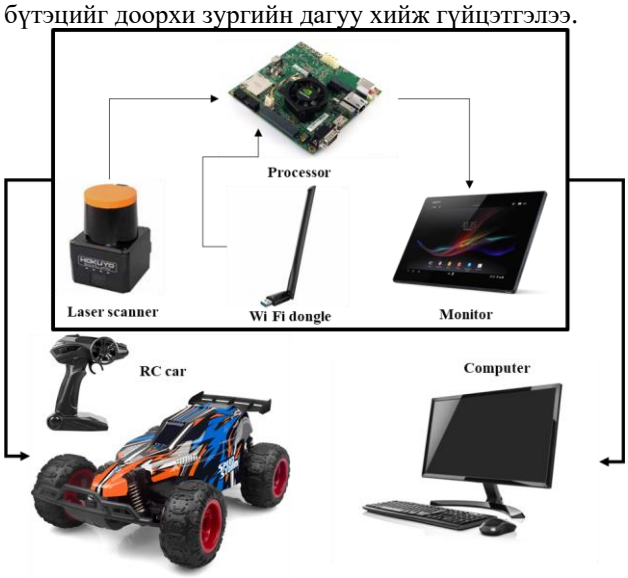
- Калман шүүлтүүр (EKF);
- Мэдээллийн шүүлтүүр;
- Жижиг хэсгүүдийн шүүлтүүр дээр суурилсан аргууд ордог

Ихэнх өндөр үзүүлэлт харуулдаг SLAM систем нь EKF-г ашигладаг бөгөөд янз бүрийн хэрэглээнд зориулан боловсруулдаг [2-4]. Гэсэн хэдий ч EKF аргыг Гаусын бус асуудлуудыг шийдвэрлэхэд ашиглаж болохгүй. Мэдээллийн шүүлтүүр ашигладаг SLAM систем нь Гаусын тархалтын тогтвортой байдлыг болон мэдээллийн матрицыг хадгаладаг [5,6]. Жижиг хэсгүүдийн шүүлтүүр ашигладаг SLAM систем (PF-SLAM) нь хамгийн үр дүнтэй систем (Fast SLAM) юм. Энэ систем дээр роботын байршил тогтоох болон зам зааж тооцоолох асуудалууд гарч ирдэг. Гэхдээ дээр дурдсан аргууд бүгд нэгдсэн шүүлтүүр дээр суурилсан системийн бүтцэд тулгуурладаг.

Мөн газрын зурагийг үүсгэснээр роботын явах замыг урьдчилан таамаглах, роботын зам төлөвлөлтийг дэмжих, газрын зураг дээр байршил тогтоох зэрэг хэрэгцээнүүдэд үндэслэн 2 хэмжээст болон 3 хэмжээст газрын зурагийг бид үүсгэх шарадлагатай болж байгаа юм.

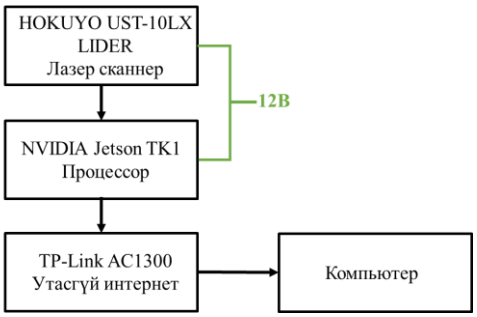
II. Системийн шийдэл

Эмбэддэд компьютер болон лазер мэдрэгчүүд ашиглан газрын зураг үүсгэх, байршил тогтоогч роботын бүтэцийг доорхи зургийн дагуу хийж гүйцэтгэлээ.



Зураг 4. Газрын зураг үүсгэ, байршил тогтоогч роботын бүтцийн диаграм

Роботын бүтцийн диаграмыг зурагт 4-т харуулав. газрын зураг үүсгэх, байршил тогтоогч робот нь лазер сканнер (HOKUYO UST-10LX LIDER), процессор (NVIDIA Jetson TK1), утасгүй интернет (TP-Link AC1300), дэлгэц, удирдлагтай машин гэсэн бүрэлдэхүүн хэсэгүүдтэй. Уг роботоос утасгүй интернет холбоогоор толгой компьютертэй холбогдоно.



Зураг. 5. Роботын ажиллагааны бүдүүвч

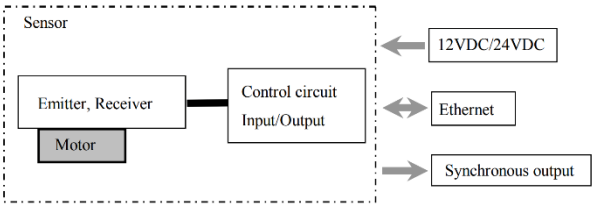
Ubuntu 14.04 дээр ROS багцыг суулгаж RVIZ ашиглаж газрын зурагийг дүрслэх, хадгалах, хадгаласан газрын зурагийг цаашид ашиглаж болно.

Зураг. 6. Роботын үүсгэх 2 хэмжээст газрын зураг

Уг газрын зураг нь 2 хэмжээст (зураг 6) бөгөөд харласан хэсгийг чөлөөт орон зай буюу роботыг жолоодох хэсэг, цагаан өнгөөр дүрслэгдсэн хэсэг бол саад тотгор харин саарал өнгөтөй бусад хэсэг бол судлагдаагүй хэсэг. Робот нь газрын зураг үүсгэхдээ лазер сканнер ашиглаж, чөлөөт хэсгээр зорчиж саад тотгорын байршлыг тогтооно.

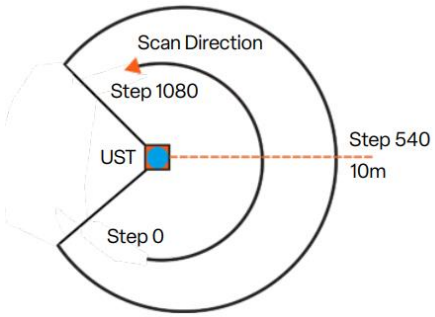
Зураг 7. Лазер сканнер (UST-10LX)

UST-10LX нь хөдөлгөөнт роботууд болон автомат удирдлагатай тээврийн хэрэгсэл дээр байрлуулахад тохиромжтой бөгөөд хэмжилт, илрүүлэлт хийдэг 2D LIDAR мэдрэгч юм.



Зураг.8. Лазер сканнерын бүдүүвч

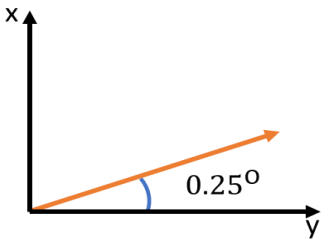
Мэдрэгч нь энгийн DC мотор дээр байрлах бөгөөд тогтмол хүчдэлийн 12В-д ажиллана. Интернет кабелиар мэдээллээ дамжуулна.



Зураг.9. Лазер сканнерын техникийн өгөгдөхүүн

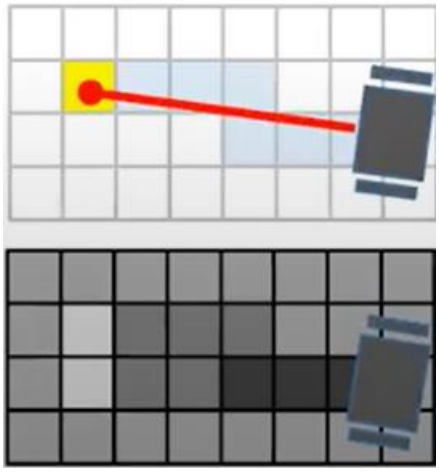
- Жин: 130 гр
- Илрүүлэх хэмжээ: 10м/20м
- Илрүүлэх өнцөг: 270
- Хариу: 25мс
- Өндөр өнцөгт тогтоц: 0.25°
- Биетийн хэмжээ, байрлал, хөдлөх чиглэлийг илрүүлэх боломжтой.
- Сканнердах хурд: 40Гц
- Ажиллах хүчдэл: 12/24В
- Интерфэйс: ETHERNET

ЛАЗЕР СКАННЕР- HOKUYO/UST-10LX LIDAR-ийг автомат робот, нисгэгчгүй нисэх хэрэгсэл, зэсгэлэн, үн амын нягтаршилыг тооцоход, хүний хөдөлгөөний загварыг судлах зэрэгээр ашигладаг.



Зураг.10. Лазер сканнерын босоо өнцөгийн өгөгдөхүүн

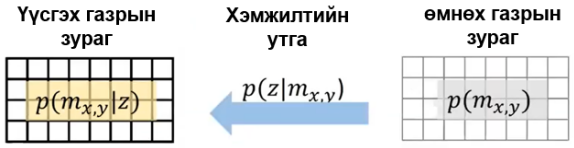
Үл мэдэгдэх орчинд байрлах робот нь LIDAR-ын тусламжтай орчны мэдээллийг цуглуулна, LIDAR-т ирсэн өгөгдөлийг интернет кабелиар процессорт дамжуулагдана, процессор газрын зурагийг үүсгэж байрлалыг тогтооно. Дараа нь мэдээллийг зам төлөвлөлт, саад бэрхшээлээс зайлсхийх гэх мэт зүйлсэд ашиглана. Мөн үүсгэсэн газрын зурагийг цаашид ашиглах боломжтой. [15]



Зураг.11. Роботын орчиноо тооцоолох арга

Робот орчиноо чөлөөтэй эсвэл саад тотгор байгаа эсэхийг ялгах хэрэгтэй. Ялгахын тулд Bayesian дүрэмийг ашиглана. [7-9] [Томъёо 1]

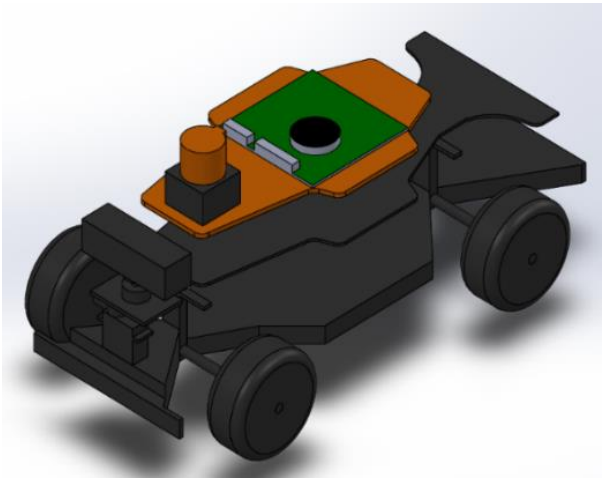
$$p(m_{x,y}|Z) = \frac{p(Z|m_{x,y})\,p(m_{x,y})}{p(Z)} \qquad \textbf{[Томъёо 1]}$$



Зураг.12. ялгах арга

Орчны төлөв байдлаас шалтгаалан 0 эсвэл 1 гэсэн утга авна. Бидний хийх ёстой зүйл бол орчин чөлөөтэй эсвэл саад тотгортой байх магадлалын хэмжилтийн утгаас шалгаатлж Bayesian дүрэмийг хэрэгжүүлэх.[10,14]

III. Туршилт, үр дүн

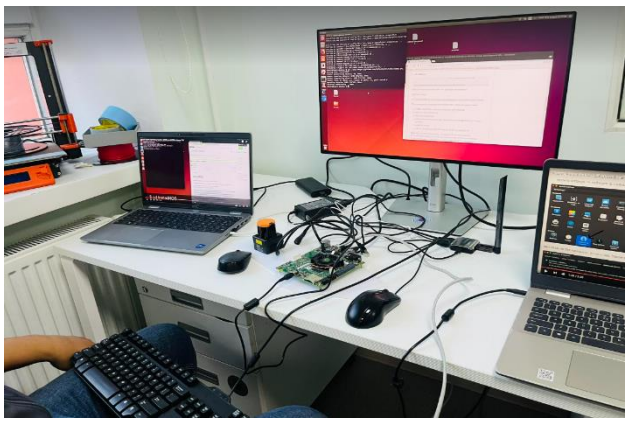


Зураг 13. Байршил тогтоох болон газрын зураг үүсгэх аргачлал

Solidworks програм дээр роботын 3 хэмжээст зургийг зурж лазер сканнер, процессор зэргийг

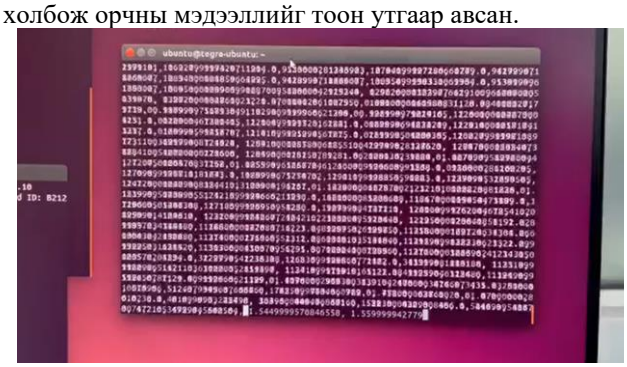
байрлуулсан. Үүний дараа роботын дээд талын 2 тавцанг 5 мм зузаантай акрилк материал лазер зүсвэр хийж хэвэнд оруулсан. Гар удирдлагтай машины явах эд анги дээр уг 2 тавцанг байрлуулж лазер сканнер, процессор зэргийг байрлуулсан. Дараа нь 12В-н липо баттерейг эхний тавцан дээр байрлуулж лазер сканнер, процессорыг тэжээлээр хангасан. [11-13]

NVIDIA Jetson TK1 процессорт ROS, RVIZ зэрэг шаардлагатай програмуудыг суулгасан. Мөн утасгүй интернетийг холбосон.

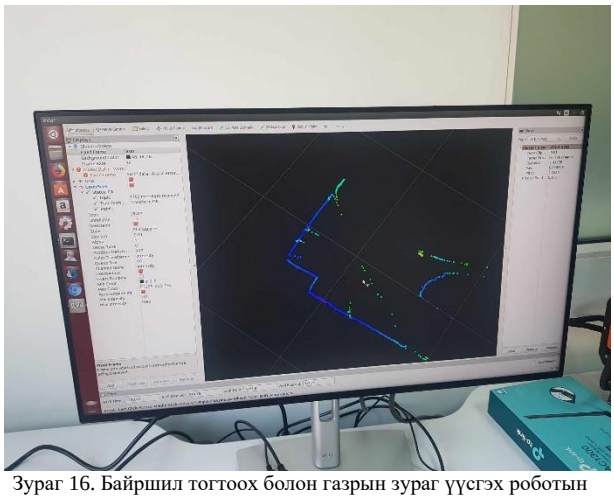


Зураг.14. процессорт RVIZ суулгах үйл явц

HOKUYO UST-10LX LIDAR-ийг процессортой холбож орчны мэдээллийг тоон утгаар авсан.



Зураг.15. UBUNTU дээр лазер сканнерын тоон утга



Зураг 16. Байршил тогтоох болон газрын зураг үүсгэх роботын лидараас утга авж байгаа зураг

Jetson Tk1 процессорт ubuntu 14.04 дээр ажиллах RVIZ нь лидараас өгсөн утгыг 2 хэмжээст хавтгайд алдалгүй дүрсэлж байна.

IV. Дүгнэлт

Туршилтаас хархад SLAM аргыг хэрэгжүүлхэд NVIDIA jetson TK1 эмбэддэд комьютерийн хүчин чадал нь гологдох зарим тохиолдолд гацаж байсан. Тийм учраас дараагийн роботоо илүү хүчин чадалтай эмбэддэд компьютер буюу NVIDIA jetson TX2 ашиглахаар зорьж байна. Мөн цаашид камер ашиглан Visual Slam ийг хэрэгжүүлэх, автомат жолоолдлого бүхий өөрийгөө жолооддог роботыг туршихаар зорьж байна. Цаашид энэхүү роботоо хөгжүүлж сургалтанд ашиглан сургалтын робот болгон хөгжүүлэнэ.

Ном зүй

[1] Durrant, H., Bailey, T.: Simultaneous localization and mapping: part I. IEEE Robot. Autom. Mag. 13(2), 99–110 (2006)

[2] Dissanayake, M.W.M.G., Newman, P., Clark, S., Durrant-Whyte, H.F., Csorba, M.: A solution to the simultaneous localization and map building (SLAM) problem. IEEE Trans. Robot. Autom. 17(3), 229–241 (2001)

[3] Yadkuri, F.F., Khosrowjerdi, M.J.: Methods for Improving the Linearization Problem of Extended Kalman Filter. J Intell Robot Syst. 78(3), 485–497 (2014)

[4] Jia, S.M., Wang, K., Li, X.Z.: Mobile Robot Simultaneous Localization and Mapping Based on a Monocular Camera, Journal of Robotics, vol.2016, Article ID 7630340, 11 pages, (2016)

[5] Thrun, S., Liu, Y., Koller, D., Ng, A.Y., Ghahramani, Z., Durrant Whyte, H.: Simultaneous localization and mapping with sparse extended information filters. Int. J. Robot. Res. 23(7–8), 693–716 (2004)

[6] Walter, M.R., Eustice, R.M., Leonard, J.J.: Exactly sparse extended information filters for feature-based SLAM. Int. J. Robot. Res. 26(4), 335–359 (2007)

[7] Burkhart, Michael C. (2019). "Chapter 1. An Overview of Bayesian Filtering". A Discriminative Approach to Bayesian Filtering with Applications to Human Neural Decoding. Providence, RI, USA: Brown University

[8] Chen, Zhe Sage (2003). "Bayesian Filtering: From Kalman Filters to Particle Filters, and Beyond". Statistics: A Journal of Theoretical and Applied Statistics

[9] M. Sanjeev Arulampalam, Simon Maskell, Neil Gordon, and Tim Clapp A Tutorial on Particle Filters for Online Nonlinear/Non-Gaussian Bayesian Tracking

[15] https://acroname.com/store/scanning-laser-rangefinder-ethernet-r359-ust-10lx#applications

КИРИЛЛ МОНГОЛ БИЧГЭЭС УЛАМЖЛАЛТ МОНГОЛ БИЧИГТ ХӨРВҮҮЛЭХ СИСТЕМ ХӨГЖҮҮЛЭЛТ

BAOYINCHAOGELA, А.Отгонбаяр, И.Цэрэн-Онолт

Компьютерийн Ухааны Салбар
Мэдээлэл, Холбооны Технологийн Сургууль
Шинжлэх Ухаан Технологийн Их Сургууль

chaogela0229@gmail.com , otgonbayar.a@must.edu.mn, tseren-onolt@must.edu.mn

Хураангуй

Кирилл монгол ба уламжлалт монгол хэл нь монгол бичгийн хоёр өөр бичгийн систем бөгөөд цагаан толгойн систем, дүрс, дуудлага, түүхэн үндэс, хэрэглээний цар хүрээ зэргээрээ ялгаатай байдаг. Энэ нь хоёр өөр монгол бичгийн систем хэрэглэгчдэд ихээхэн хүндрэл учруулдаг. Иймээс энд "Кирилл монгол бичгээс уламжлалт монгол бичигт хөрвүүлэх систем"-г судалж, хөгжүүлж, кирилл монгол бичиг болон уламжлалт монгол бичиг хэрэглэгчдэд монгол хэлийг хурдан, үр дүнтэйгээр хэрэглэх, сурах, харилцах нь туслах зорилгоор ажиллаж байна.

Түлхүүр үг: (keywords). *хөрвүүлэх систем, мэдээллийн сан, Кирилл монгол үсэг, уламжлалт монгол үсэг*

Удиртгал

XIII зуунаас эхлэн Монголчууд Монгол бичгийг төрийн үйл хэрэгт болон шинжлэх ухааны бүтээл туурвилыг бүтээхэд хэрэглэсээр ирсэн, албан ёсны сонгодог төдийгүй дэлхийн бичиг соёлын нандин өв юм. Монгол үндэстэн оршин тогтнох соёл, сэтгэлгээний баталгаа болсон Монгол бичгээ сурч эзэмших, судлан сурталчлах, түгээн дэлгэрүүлэх, хамгаалах, өвлүүлэх, хөгжүүлэх нь Монгол хүн бүрийн төдийгүй дэлхийн бичиг соёлын өв сангийн өмнө Монголчуудын хүлээж байгаа эрхэм үүрэг юм.

Монгол Улс 1946 оноос хойш төрийн албан хэргийг кирилл бичгээр хөтлөн явуулж байгаа ч төрийн байгууллагын тамга, тэмдгийг монгол бичгээр үйлдэн хэрэглэж, иргэний болон боловсролын бичиг баримтыг кирилл болон монгол бичгээр зэрэгцүүлэн бичиж байгаа нь монгол бичиг төрийн хэрэгт зохих үүргээ гүйцэтгэсээр байгаагийн нэгэн бодит жишээ болно.

2010 оноос хойш Монгол улс уламжлалт Монгол бичгийн хэрэглээг өргөжүүлж эхэлсэн. Энэхүү судалгаа нь мөн Монгол улсын "2025 оноос Уйгуржин Монгол бичгийн хэрэглээг бүрэн сэргээх" бодлогыг дэмжиж байна.

1. Өгөгдөл цуглуулах, өгөгдлийн сангийн зохиомж

Хөрвүүлэлтийн системийг бий болгох, ашиглах үед их хэмжээний өгөгдлийн дэмжлэг шаардлагатай бөгөөд мэдээллийн үнэн зөв, бүрэн бүтэн байдал, хүрэлцээтэй байдлыг хангах ёстой. Тиймээс хөрвүүлэх системийг бий болгохын тулд өгөгдөл цуглуулах, өгөгдөлд дүн шинжилгээ хийх, өгөгдөл боловсруулах нь маш чухал юм. Мэдээлэл цуглуулах явцад орчуулгын системийн гүйцэтгэл, ерөнхий ойлголтыг сайжруулахын тулд мэдээллийн чанар, олон талт байдлыг хангасан.

1.1. Мэдээлэл цуглуулах арга, мэдээллийн эх сурвалж

Өгөгдөл цуглуулах нь текст орчуулгын системийг бий болгох гол үе шатуудын нэг юм. Бид дараах байдлаар өгөгдлийг цуглуулсан.

a. Гараар цуглуулах: орчуулсан мэдээллийг мэргэжлийн орчуулагчдаас авах. Эдгээр өгөгдлүүд нь мэргэжлийн хүмүүс орчуулсан бөгөөд харьцангуй өндөр чанартай.
b. Толь бичиг, ном: илүү олон сэдвээр орчуулгын мэдээлэл авахын тулд том толь бичиг, дижитал ном ашиглав.
c. Веб хуудас хөтлөгч: интернет дахь хэлний текстийг, ялангуяа холбогдох орчуулгын веб хуудас хөтлөгчийг ашиглав. Энэ арга нь орчин цагийн болон олон төрлийн өгөгдлийг олж авах боломжтой.
d. Нээлттэй эхийн орчуулгын өгөгдлийн багц: эрэлттэй байгаа нээлттэй эхийн орчуулгын өгөгдлийн багцыг ашиглалаа.

Эдгээр өгөгдлийн багцууд нь их хэмжээний сэдвүүдийн орчуулгын хослуулдаг бөгөөд энэ нь системийн ерөнхий гүйцэтгэлийг сайжруулахад тусалдаг.

1.2. Өгөгдлийн сан үүсгэх:

Хөрвүүлэлтийн системийн мэдээллийн сан нь системийн дизайн, үйл ажиллагаанд гол үүрэг гүйцэтгэдэг. Хөрвүүлэлтийн системд мэдээллийн санг бий болгож, мэдээллийн баазыг оруулах нь дараах байдалтай байна.

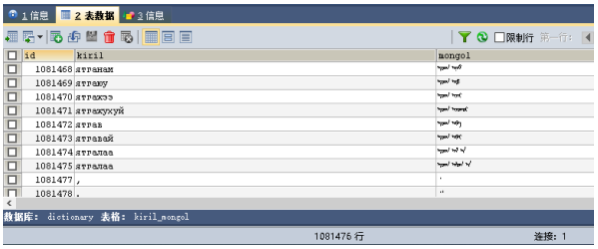
a. Өгөгдлийн сангийн бүтцийг зохиох: Мэдээллийн сангийн хүснэгтийн бүтцийг тодорхойлох, үүнд эх хэлний кирилл бичвэр, зорилтот хэлний уламжлалт монгол бичвэр, хөрвүүлэх загварын параметрүүд болон бусад мэдээллийг хадгалдаг хүснэгтүүд багтана. Хүснэгтийн нэр нь kiril_mongol.

Зураг 1. Хүснэгтийн бүтцийн дэлгэрэнгүй

Зураг 2. Хүснэгтийн бүтцийн дэлгэрэнгүй

b. Өгөгдлийн сангийн хөдөлгүүрийг сонгоно: Системийн шаардлагад үндэслэн тохирох өгөгдлийн сангийн хөдөлгүүрийг сонгодог. Энэ систем нь Relational Data Management System (RDBMS) MySQL-ийг ашигладаг.
c. Холболт ба интерфейсийг бий болгох: Систем ба мэдээллийн сангийн хоорондох холболт, интерактив интерфэйс нь хэрэгжиж, систем нь өгөгдлийн санг үр дүнтэй ашиглаж, шинэчлэх боломжийг олгодог.
d. Өгөгдлийн сангийн өгөгдлийн хэмжээ: Одоогийн байдлаар мэдээллийн санд

1’000’000 орчим мөр өгөгдөл байна. Дэлгэрэнгүйг Зураг 2-оос үзнэ үү.



Зураг 3. Өгөгдлийн сангийн өгөгдлийн хэмжээ

2. Хөрвүүлэх системийг хөгжүүлэх

Энэхүү орчуулгын систем нь компьютерийн технологиор кирилл Монгол бичгийг уламжлалт Монгол бичигт хөрвүүлэх хэрэгсэл юм. Түүний хөгжлийн технологи, үндсэн чиг үүрэг нь дараах байдалтай байна.

2.1 Хөгжүүлэх технологи

Энэхүү судалгаанд Java програмчлалын хэл болон MySQL мэдээллийн сантай хамтран хөгжүүлсэн хөрвүүлэх системийг ашигласан. Java болон MySQL-ийг хослуулан хөгжүүлснээр олон давуу талтай. Үүнд хэмжээнээс үл хамааран бүх төрлийн хэрэглээнд тохиромжтой хүчирхэг, өндөр гүйцэтгэлтэй, уян хатан хөгжүүлэлтийн орчин бүрдүүлдэг. - түвшний програмууд.

```
package com.hbl.servlet;

import java.sql.Connection;

public class Hurbelhe {
    public void Hurb(String kiril){
        Connection conn = null;
        Statement st;
        ResultSet rs;
        String url="jdbc:mysql://127.0.0.1:3306/dictionary?useUnicode=true&characterEncoding=utf-8";
        try {
            Class.forName("com.mysql.jdbc.Driver").newInstance();
            conn=DriverManager.getConnection(url,"root","root");
            st=conn.createStatement();

            String arr[] = kiril.split(" ");
            String monggol = "";
            for(int i=0;i<arr.length;i++){
                rs = st.executeQuery("select mongol from kiril_mongol where kiril = \"" + arr[i] + "\"");
                while(rs.next()){
                    monggol = rs.getString("mongol") + " ";
                    System.out.print(monggol);
                    break;
                }
                if(" ".equals(monggol) || "".equals(monggol)){
                    System.out.print(arr[i] + " ");
                }
                monggol = "";
            }

        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

Зураг 4. Код боловсруулах

2.2 Системийн хэрэглэгчийн интерфэйс

Энэхүү системийн интерфэйс нь WEB технологид суурилсан бөгөөд ойлгомжтой, хэрэглэхэд хялбар хэрэглэгчийн интерфэйсийг хангаснаар хэрэглэгчдэд хөрвөлтийн үр дүнг хялбар оруулах, авах боломжийг олгодог.

Зураг 5. Системийн хэрэглэгчийн интерфэйс

2.3. Системийн функцүүдийн танилцуулга

Хөрвүүлэх функцууд нь: *үг хөрвүүлэх, өгүүлбэр хөрвүүлэх, богино өгүүлбэр хөрвүүлэх, урт текст хөрвүүлэх* зэрэг орно. Хэрэглэгч хөрвүүлэх гэж буй кирилл Монгол бичвэрийг оруулах ба систем нь харгалзах уламжлалт монгол бичвэр хөрвүүлэх үр дүнг гаргадаг.

Үгийн функц нэмэх: Өгөгдлийн санд хөрвүүлэх шаардлагатай үг байхгүй бол та үгийн функцийг нэмж мэдээллийн санд байгаа өгөгдлөө дуусгах боломжтой бөгөөд дараагийн удаа энэ үгийг хайхад систем хэвийн хөрвүүлэх болно.

Зураг 6. Үгийн функц нэмэх

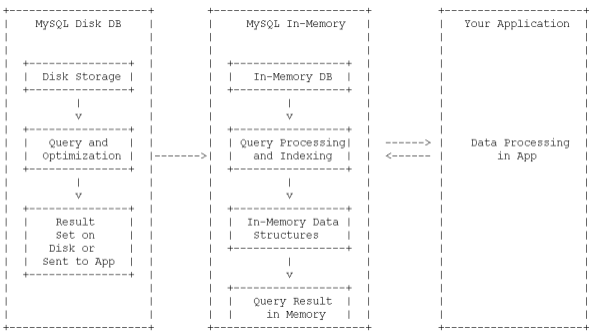
2.4. Ажиллагааны байдал

Системийн үр дүнтэй дизайн, мэдээллийн сангийн менежментээр дамжуулан хөрвүүлэх системүүд нь өгөгдлийг илүү сайн ашиглаж, орчуулгын чанар, хариу үйлдэл, хэрэглэгчийн туршлагыг сайжруулж чадна. Одоогоор систем хэвийн ажиллаж байна.

3. Хайлтын хурдатгалын шийдэл

Эхний хувилбарт текстийг хөрвүүлэхдээ өгөгдлийн сангаас хайдаг байсан. Хэрэв хөрвүүлэх шаардлагатай текстийн хэмжээ их байвал маш их цаг зарцуулдаг бөгөөд хөрвүүлэх хурд нь ялангуяа удаан байдаг. Энэ асуудлыг шийдэхийн тулд MySQL өгөгдлийн сан дахь өгөгдлийг дискнээс санах ой руу ачаалж, дараа нь програм руу шилжүүлэх байдлаар хайлтыг хурдасгах шийдлийг боловсруулсан. Энэ процесс нь олон холбоосыг

хамардаг. Энэ үйл явцын үндсэн алхмуудыг харуулсан энгийн схемийг Зураг 7-д харуулав.



Зураг 7. flow chart

Урсгал диаграм дахь үндсэн алхамууд:

a. Дискний өгөгдлийн сангийн давхарга:
MySQL мэдээллийн сан нь дискэн дээр хадгалагддаг бөгөөд хүснэгт, индекс, өгөгдлийн файлуудыг агуулдаг.
b. Query optimization layer:
Аппликешн асуулга эхлүүлэх үед MySQL нь өгөгдлийг олж авах хамгийн үр дүнтэй аргыг тодорхойлохын тулд асуулгын оновчлолыг гүйцэтгэдэг.
c. Дискний өгөгдлийг санах ойд ачаалах:
Асуулгын оновчтой төлөвлөгөөний дагуу MySQL нь хүснэгтийн өгөгдөл, индекс зэрэг холбогдох өгөгдлийг дискнээс санах ой руу ачаалдаг.
d. Санах ойн өгөгдлийн сангийн давхарга:
Дараагийн асуулгын гүйцэтгэлийг хурдасгахын тулд санах ойд асуулгын үр дүнгийн багц болон индексийг бий болгоно.
e. Хэрэглээний давхарга:
Програм нь MySQL руу асуулгын хүсэлт илгээж, санах ойн мэдээллийн сангаас асуулгын үр дүнг авдаг. Дараа нь програм нь өгөгдлийг цаашид боловсруулах, бизнесийн логик хийх гэх мэт боломжтой.

Дүгнэлт

Тус Крилл Монгол бичгээс уламжлалт Монгол бичигт хөрвүүлэх систем нь вэбд суурилсан, хэрэглэхэд хялбар байдлаар хийгдсэнээс гадна хөрвүүлэлтийн хурд буюу өгөгдөлд хайлт хийх хурдыг өндөр хэмжээнд хүргэх шийдлийг нэвтрүүлсэн. Тухайлбал, хайлтын хурдыг сайжруулаагүй, энгийн хайлтын үед 10 үгийг хөрвүүлэх хугацаа 22 секунд байсан. Сайжруулалт хийсний дараа хөрвүүлэлтийг 1 секундэд гүйцэтгэх боломжтой болж хөрвүүлэлтийн хурд 95% нэмэгдсэн; сайжруулах төлөвлөгөөний өмнө 100 үг хөрвүүлэхэд 45 секунд зарцуулсан. Сайжруулах төлөвлөгөөний дараа хөрвүүлэлтийг 1 секундэд хийж, хөрвүүлэх хурд нэмэгдсэн. 98%-иар хүлээгдэж буй зорилгодоо хүрсэн.

Дараагийн хийх зүйл: 1. Уламжлалт монгол үсгээс кирилл үсэгт шилжих функц нэмэх. 2. Системд хэрэглэгчийн бүртгэл, хэрэглэгчийн нэвтрэх функцээр хангах, хэрэглэгчийн зөвшөөрлийг ангилах зэрэг удирдлагын функцуудыг нэмэхээр төлөвлөж байна.

Ном зүй

[1] Carine Khalil,Sabine Khalil. Exploring knowledge management in agile software development organizations[J]. International Entrepreneurship and Management Journal,2020,16(4).

[2] Kevin A. Gary,Ruben Acuna,Alexandra Mehlhase,Robert Heinrichs,Sohum Sohoni. SCALING TO MEET THE ONLINE DEMAND IN SOFTWARE ENGINEERING[J]. International Journal on Innovations in Online Education,2020,4(1).

[3] Hosseini Hadi,Zirakjou Abbas,Goodarzi Vahabodin,Mousavi Seyyed Mohammad,Khonakdar Hossein Ali,Zamanlui Soheila. Lightweight aerogels based on bacterial cellulose/silver nanoparticles/polyaniline with tuning morphology of polyaniline and application in soft tissue engineering.[J]. International journal of biological macromolecules,2020,152.

[4] Dylan G. Kelly,Patrick Seeling. Introducing underrepresented high school students to software engineering: Using the micro:bit microcontroller to program connected autonomous cars[J]. Computer Applications in EngineeringEducation,2020,28(3).

[5] Soft Computing; Research Conducted at School of Computing Science and Engineering Has Updated Our Knowledge about Soft Computing (Indeterminate Likert scale: feedback based on neutrosophy, its

distance measures and clustering algorithm)[J]. News of Science,2020.

[6] "Neural Machine Translation" by Kyunghyun Cho, Minjoon Seo, and Barry Devereux

[7] "Foundations of Statistical Natural Language Processing" by Christopher D. Manning and Hinrich Schütze

[8] "Neural Network Methods in Natural Language Processing" by Yoav Goldberg

[9] "Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition" by Daniel Jurafsky and James H. Martin

[10] "Neural Machine Translation and Sequence-to-sequence Models: A Tutorial" by Graham Neubig

[11] "Attention is All You Need" by Ashish Vaswani et al.

ВЭБ СИСТЕМИЙН ХАЛДЛАГА ИЛРҮҮЛЭХ ТЕХНИКИЙН СУДАЛГАА

Батмөнх ДАШДОРЖ, Бат-эрдэнэ МӨНХБАЯР

[1]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Мэдээллийн сүлжээ, аюулгүй байдлын салбар

Холбоо барих зохиогчийн и-мэйл хаяг: munkhbayar.b@must.edu.mn, bagaeegx@gmail.com

Хураангуй: **Мэдээлэл харилцаа холбооны технологи өндөр хурдацтайгаар хөгжиж буй өнөө үед цахим үйлчилгээ, хэрэглэгчийн тоо улам өссөөр байна. Энэхүү судалгааны ажлаар Монгол улсын Мэдээлэл холбооны сүлжээ, кибер халдлагын судалгаа, олон улсад системийн халдлага илүрүүлэх орчин үеийн техникүүдийн судалгааг хийсэн.**

Түлхүүр үг: интернет, тоног төхөөрөмж, сүлжээний 7-н түвшин, протокол, ачаалал, систем

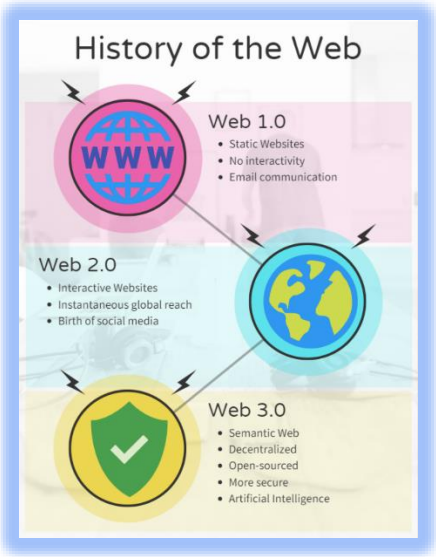
I. УДИРТГАЛ

Вэб системийн халдалга болон илрүүлэх техник нь вэб аппликейшн, вэб сайт, вэб сервисийг хөгжүүлэх, ашиглах, хэрэглэх боломжийг хангахад зориулагдсан технологийн нэг юм. Интернэтэд хандсан хэрэглэгчид вэб-д байгаа контентуудад хурдан хандах, аюулгүй байдлыг хангах, хандалттай ажиллах гэх мэт хэрэгтэй ажил гүйлгээг хангахад энэ техник хамгийн чухал юм.

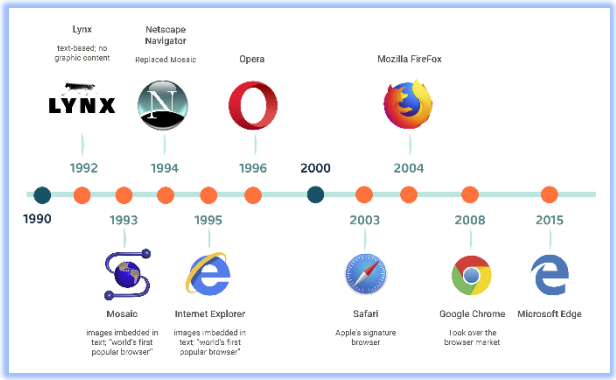
Вэб системийн халдалгыг илрүүлэх техник боломжууд нь:

1. **Хувийн үйлчилгээ хамгаалалт:** Хэрэглэгчийн мэдээллийг хамгаалалт, нууцлал, холболтоо хамгаалалтыг баталгаажуулах.
2. **Өгөгдлийн аюулгүй байдлыг хангах:** Өгөгдлийг хадгалах, хангах, заавал хамгаалалтын аргаар шифрлэх гэх мэт аюулгүй байдлыг хангах.
3. **Сүлжээний тодорхойлох:** Хэрэглэгчид вэб сайтын хамаарлыг нэмэгдүүлэх, хурдан хандахыг зориулах.
4. **Амжилттай хандалттай ажиллах:** Вэб систем амжилттай ажиллаж, хэрэглэгчид хурдан, үргэлжлүүлэн ажиллана гэх мэт амжилттай ажиллах техникүүд.
5. **Тогтвортой хэрэглэгчийн интерфэйс:** Хэрэглэгчид хялбар, тогтвортой интерфэйстэй вэб сайтыг хангах.

Эдгээр техникүүд нь вэб системийг аюулгүй байдлыг хангах, эргэн тогтоолыг мэдэлэх, амжилттай ажиллахад зориулагдсан байдаг.



Зураг 1. ВЭБ-ийн түүх



Зураг 2. ВЭБ-ийн түүх

II. КИБЕР, СИСТЕМИЙН АЮУЛГҮЙ БАЙДАЛ

Кибер аюулгүй байдлын талаархи тодорхойлолт нь компьютерийн систем, сүлжээ, сүлжээний сүлжээ, компьютерийн сүлжээний үйл ажиллагааг хамгийн бага тогтмол хэлбэлзэх ба компьютерийн хэрэглэгчид, өгөгдлийн сан, програм хангамжийг

хамгийн өндөр аюулгүй байдлыг хангахад хандах. Энэ нь компьютерийн сүлжээ, сүлжээний сүлжээ, сүлжээний түвшний үйл ажиллагаа, интернэт холболтын сүлжээ, компьютерийн програм хангамж болон өгөгдлийн сангийн хамгийн өндөр зөвлөгөө, эрсдэлтэй байдал, цаашид боловсруулах, хамгийн түргэн шаардлагатай байдлыг зааварчилдаг болно.

Кибер аюулгүй байдлын аюулгүй байдлын шалгалтыг хийхдээ байгууллагууд, бизнесүүд, хэрэглэгчид интернэт холболтын шаардлагатай аюулгүй байдлыг хангаж байхыг зөвлөж, тэр чигээрээ нууцлалын талаар сургалт, мэдээллийг хамгаалах, замыг төгсөх, өгөгдлийг халдлагатай болгох, холбогдох системүүдийг аюулгүй байдлын асуудалтай орчин үед хиймэл оюун ухаан үүсэн улам нарын төвөгтэй тулгарч байна.

Интернэтийн хурдацтай өсөлт, түүний өргөн цар хүрээтэй шинж чанараас шалтгаалан өнөө үед хэрэглэгчид өдөр тутмын үйл ажиллагаандаа компьютерийн сүлжээнд найдаж байна.

- Халдлага нь зорилтот сүлжээний эмзэг байдлыг ашиглан сүлжээний аюулгүй байдлын механизмыг тойрч гарахыг оролддог. Халдлагууд нь сүлжээний хууль ёсны үйл ажиллагааг тасалдуулж, сүлжээний төхөөрөмжүүдийн буруу ажиллагаа, сүлжээг хэт ачаалах, сүлжээний үйлчилгээг хууль ёсны хэрэглэгчдэд хүргэхээс татгалзах, сүлжээний дамжуулалтыг эрс багасгах, хорлонтойгоор сканнердах болон бусад ижил төстэй үйлдлүүд орно.
- Халдагчид мөн сүлжээний хэвийн үйл ажиллагааг тасалдуулахын тулд програм хангамжийн үйлчилгээний цоорхой, алдаа, буруу тохиргоог ашиглаж болно.
- Аюулгүй байдлын хэрэгслүүд нь сүлжээний халдагчид болон сүлжээ хамгаалагчдад сүлжээний эмзэг байдлыг тодорхойлох, сүлжээний статистик мэдээллийг цуглуулахад тусалдаг.
- Халдагчид хост дээр нээгдсэн нийтлэг үйлчилгээн дээр тулгуурлан цоорхойг илрүүлж, амжилттай халдлага эхлүүлэхийн тулд холбогдох мэдээллийг цуглуулахыг санаатайгаар оролддог.
- Хамгаалагчид сүлжээний шууд урсгалаас үүсэх хэвийн бус үйл ажиллагааг багасгахыг хичээдэг.
- Сүлжээний аюулгүй байдлын олон тооны хэрэгслийг зохион бүтээсэн олон зорилготой янз бүрийн төрлийн халдлагуудыг эхлүүлэх, барих, дүрслэх, илрүүлэх. Жишээлбэл, LOIC (Pras et al., 2010), HOIC (Mansfield-Devine, 2011), Wireshark (Orebaugh нар, 2006), Gulp (Satten, 2007), Ntop (Deri et al., 2001) гэх мэт. Эдгээр хэрэгслүүдийг сүлжээний шууд урсгалыг барьж авах, урьдчилан боловсруулах, онцлог задлах, эмзэг байдлын шинжилгээ, хөдөлгөөний дүрслэл болон халдлагыг бодитоор илрүүлэхэд ашиглаж болно.

II. СҮЛЖЭЭНИЙ ХАЛДЛАГА БА ХОЛБОГДОХ ОЙЛГОЛТУУД

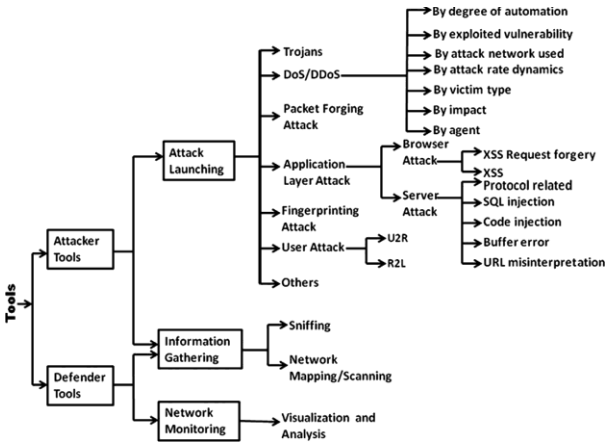
Халдлага нь трояны халдлага, DoS/DDoS халдлага, скан хийх халдлага гэх мэт олон хэлбэртэй байж болно. DDoS халдлага нь олон тооны эвдэрсэн хостуудыг ашигладаг тул аливаа мэдээллийн системд маш их гамшиг учруулдаг бөгөөд ийм халдлагын анхны эх сурвалжийг илрүүлэхэд маш хэцүү байдаг. Системийн эвдрэлээс хамгаалах нь DDoS халдлагаас хамгаалах сайн арга юм.

Довтолгоог эхлүүлэх алхамууд

Ерөнхийдөө халдлага үйлдэгчид халдлага үйлдэхийн тулд дөрвөн үндсэн алхмыг …

1. **Мэдээлэл цуглуулах:** Халдагчид зарим мэдээллийг дараагийн халдлагад туслах зорилгоор ашиглаж болно гэж найдаж эмзэг байдлын мэдээллийг цуглуулахыг оролддог.
2. **Эмзэг байдлыг үнэлэх:** Өмнөх алхамд олж мэдсэн эмзэг байдлын үндсэн дээр халдагчид халдлагыг эхлүүлэхийн урьдал болгон хортой кодыг ашиглан мэдээллийг эвдэхийг оролддог.
3. **Довтолгоо эхлүүлэх:** Халдагчид эвдэгдсэн мэдээллийг ашиглан зорилтот хохирогчийн системүүд рүү дайралт хийдэг.
4. **Цэвэрлэх:** Эцэст нь халдагч хохирогчийн системүүд рүү дахь бүх бүртгэл эсвэл бүртгэлийн файлуудыг цэвэрлэх замаар халдлагын түүхийг арилгахыг оролддог.

Хүмүүс янз бүрийн зорилгоор сүлжээг тасалдуулахын тулд өөр өөр халдлагын хэрэгслийг ашигладаг. Өмнө дурьдсанчлан халдагчид өөрсдийн сул тал дээр тулгуурлан мэдээлэл цуглуулах замаар вэб сайтууд эсвэл мэдээллийн баазууд болон байгууллагын сүлжээг онилодог. Олон тооны хамгаалалтын хэрэгслийг сүлжээний аюулгүй байдлын судалгааны янз бүрийн бүлгүүд болон хувийн хамгаалалтын мэргэжилтнүүд ашиглах боломжтой болгосон. Эдгээр хэрэгслүүд нь өөр өөр зорилго, чадвар, интерфейстэй байдаг. Одоо байгаа хэрэгслүүдийг халдагчид болон сүлжээний хамгаалагчдад зориулсан хэрэгсэл гэсэн хоёр үндсэн ангилалд хуваадаг. Сүлжээний аюулгүй байдлыг хангахад хэрэглэгдэх хэрэгслүүдийн ангилал зүйг зурагт үзүүлэв.



Зураг 3. Сүлжээний аюулгүй байдлын хэрэгслүүдийн ангилал зүй.

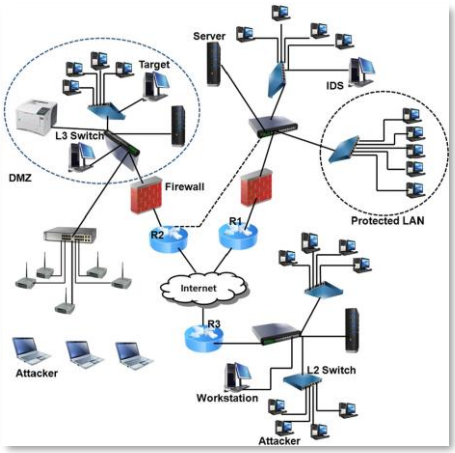
Мэдээлэл цуглуулах хэрэгсэл

Халдлага үйлдэхээсээ өмнө халдагчид халдлага хийх орчинг ойлгох хэрэгтэй. Үүний тулд халдагчид эхлээд сүлжээний тухай мэдээлэл, тухайлбал машин, үйлчилгээний портын дугаар, үйлдлийн систем гэх мэт мэдээллийг цуглуулдаг. Мэдээлэл цуглуулсны дараа халдагчид янз бүрийн хэрэгслийг ашиглан сүлжээний сул талыг олж илрүүлдэг. Мэдээлэл цуглуулах хэрэгслийг үнэрлэх хэрэгсэл, сүлжээний зураглал/сканнердах хэрэгсэл гэж ангилдаг.

Довтолгоог эхлүүлэх, илрүүлэх

Халдлага үйлдэхээсээ өмнө халдагчид эхлээд зорилтот системийн талаарх эмзэг байдлын мэдээллийг цуглуулахыг оролддог бөгөөд энэ нь халдлага үүсгэхэд тустай. Халдагчид nmap гэх мэт мэдээлэл цуглуулах хэрэгслийг ашиглан сүлжээг сканнердаж, системийн цоорхойг олдог. Цуглуулсан мэдээлэлд үндэслэн халдагчид сүлжээнд байгаа зарим хортой кодыг ашигладаг.

- Хортой кодыг эхлээд сүлжээн дэх хостуудыг эвдэх эсвэл шууд халдлага хийж сүлжээг тасалдуулахад ашиглаж болно. Довтолгоо хийх олон арга бий. Жишээлбэл, систем эсвэл сүлжээнд халдлага үүсгэхийн тулд троян эсвэл өт ашиглаж болно. Сканнердах эсвэл мэдээлэл цуглуулах ажлыг халдлагатай уялдуулж, нэгэн зэрэг хийж болно.
- Dsniff (Danielle, 2002), IRPAS (Yeung нар, 2008), Ettercap (Norton, 2004) болон Libnet (Schiffman, 2000) зэрэг халдлага эхлүүлэх хэрэгслийг MAC халдлага, ARP халдлага эсвэл VLAN халдлага үүсгэх боломжтой.
- Ихэнх тохиолдолд халдагчийн гол зорилго нь нөөцийг ашиглах эсвэл зурвасын өргөнийг ашиглах замаар сүлжээгээр үзүүлж буй үйлчилгээг тасалдуулах явдал юм. Эдгээр төрлийн халдлагыг TCP SYN үерлэх, ICMP үерлэх болон UDP үерлэх зэрэг хууль ёсны хүсэлтийг ашиглан эхлүүлж болно. Довтолгоог илрүүлэхийн тулд түүний шинж чанарыг мэдэх шаардлагатайхалдлага ба түүний сүлжээн дэх зан байдал.
- Сүлжээний администраторт хэвийн бус урсгал болон хэвийн бус урсгалын шинж чанаруудын ялгааг ажиглахын тулд дүрслэл эсвэл хяналтын систем хэрэгтэй. Пакетийн толгой хэсэг эсвэл сүлжээний урсгалын мэдээлэл дээр үндэслэн хөдөлгөөний хэмжээнээс халдлагыг илрүүлж болно. Мэдээжийн хэрэг, бүх халдлагыг тодорхойлж чадах бодит цагийн хамгаалалтын механизмыг зохион бүтээх нь хэцүү бөгөөд боломжгүй ажил юм. Ихэнх илрүүлэх аргууд нь илрүүлэх явцад ашиглахын тулд халдлагын шинж чанаруудын талаар урьдчилсан мэдээлэл шаарддаг. Эдгээр халдлагыг илрүүлэх механизм эсвэл системийн үнэлгээг буруу ангиллын түвшин эсвэл худал дохиоллын түвшинг ашиглан гүйцэтгэдэг.
- Сэтгэл ханамжтай үр дүнд хүрэхийн тулд IDS-ийн дизайнер арга барил, тохирох механизм эсвэл аливаа эвристикийг сонгох эсвэл таамаглал гаргахдаа болгоомжтой байх хэрэгтэй.
- Илрүүлэх системүүд нь сүлжээг сүйрүүлэх эсвэл хувийн болон аюулгүй мэдээллийг олж авах боломжтой янз бүрийн төрлийн эмзэг байдлаас сүлжээг хамгаалах зорилготой юм. Аномали илрүүлэх үнэн зөв, үр дүнтэй системийг ашиглах нь стандарт аюулгүй байдлын шаардлага, эрсдлийн шинжилгээнд нийцүүлэн зохих загварыг шаарддаг. Илрүүлэх систем нь хост дээр суурилсан эсвэл сүлжээнд суурилсан байж болно.



Зураг 5. Хамгаалагдсан LAN, DMZ болон IDS байршуулалт бүхий ердийн сүлжээний бүтэц.

Довтолгоо эхлүүлэх хэрэгсэл

Вэб дээр халдлага үйлдэхэд криптограф механизм ашигладаг олон тооны сүлжээний аюулгүй байдлын хэрэгслүүд байдаг. Хүмүүс эдгээр хэрэгслийг чөлөөтэй татаж авах боломжтой бөгөөд трояны тархалт, сүлжээний зураглал, шалгалтын халдлага, буферийн хэт халдлага, DoS/DDoS халдлага, хэрэглээний түвшний халдлага зэрэг хортой үйл ажиллагаанд ашиглах боломжтой. Ийм хэрэгслийг HTTP, SMTP, FTP эсвэл SNMP-тэй холбоотой халдлага гэх мэт давхарга болон протоколын тусгай халдлагуудыг эхлүүлэхэд ашиглаж болно. Сүлжээ эсвэл вэб сайтын үйлчилгээг маш хурдан тасалдуулж болох DoS/DDoS халдлагыг эхлүүлэхийн тулд бусад хэрэгслийг ашиглаж болно. Зарим хэрэгслийг утастай сүлжээнд үнэ цэнэтэй мэдээллийг олж авах, ашиглахад ашигладаг бол зарим нь утасгүй сүлжээнд ашиглагддаг.

- Трояннууд
- DoS/DDoS халдлага
- Хэрэглээний давхаргын халдлага
- Хурууны хээгээр халдлага
- Хэрэглэгчийн халдлага
- Бусад халдлага гэх мэт

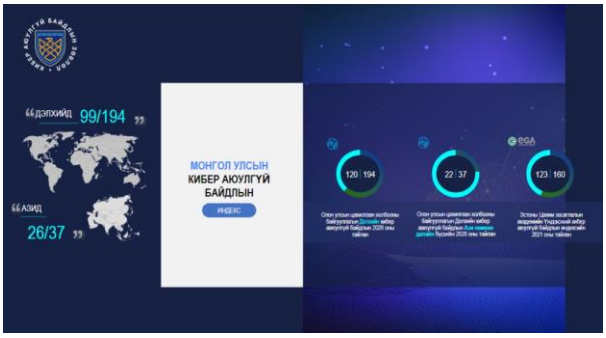
III. КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЗӨВЛӨЛ

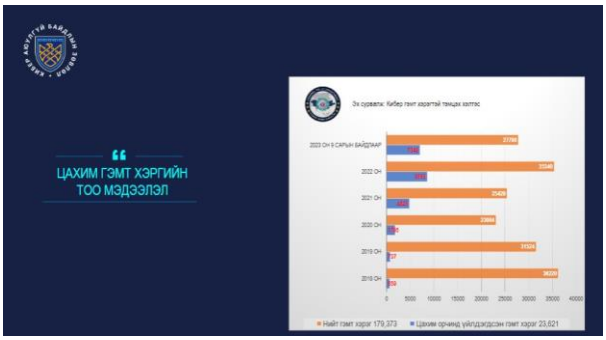
Монгол Улсын “Кибер аюулгүй байдлын үндэсний стратеги” батлагдсан: (2023 оны 01 сарын 31 өдөр)

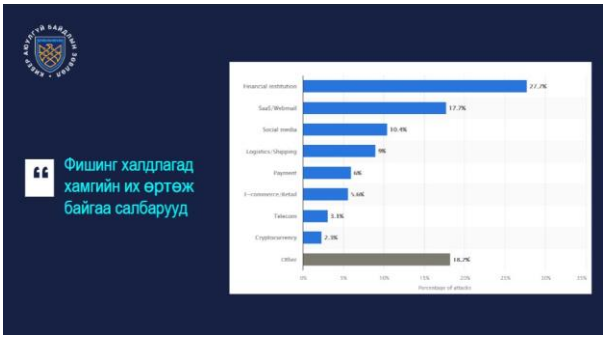
Кибер орчинд төр, иргэн, хуулийн этгээдийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг хангах энэхүү стратеги нь дараах зорилтуудыг дэвшүүлсэн. Үүнд:

- Кибер аюулгүй байдлыг хангах зохицуулалтын орчинг сайжруулан нэгдсэн удирдлагын тогтолцоог бүрдүүлэх
- Онц чухал мэдээллийн дэд бүтцийн кибер аюулгүй байдлыг хамгаалах
- Кибер аюулгүй байдлын уян хатан байдлыг сайжруулж, халдлагад хариу үйлдэл үзүүлэх чадамжийг бүрдүүлэх
- Бүх нийтийн кибер аюулгүй байдлын мэдлэгийг дээшлүүлж, хүний нөөцийн чадавхыг нэмэгдүүлэх
- Гадаад болон дотоод хамтын ажиллагааг хөгжүүлэх

Кибер аюулгүй байдлын үндэсний стратегийг хэрэгжүүлснээр Монгол Улсын кибер халдлагаас урьдчилан сэргийлэх, халдлагад хариу үйлдэл үзүүлэх, таслан зогсоох, кибер гэмт хэрэгтэй тэмцэх тогтолцоо бэхжиж, кибер аюулгүй байдлыг хангах хамтын ажиллагаа өргөжин, кибер орчинд төр, иргэн, хуулийн этгээдийн мэдээллийн аюулгүй байдлыг хангах, иргэдийн мэдлэг, ойлголтыг дээшлүүлэх, зохистой хэрэглээг төлөвшүүлэхэд чухал ач холбогдолтой юм.







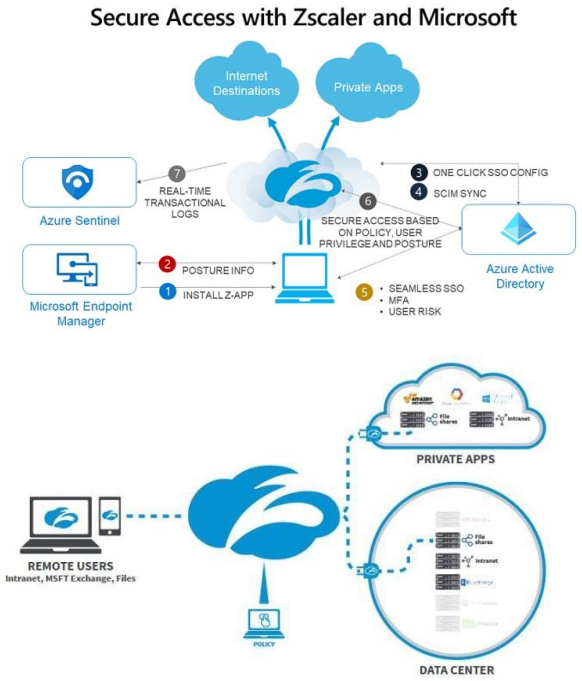
Зураг 12. Кибер аюулгүй байдлын зөвлөлийн 2023 оны судалгаа

IV. ӨНӨӨГИЙН ҮЕИЙН ВЭБ СИСТЕМ

Вэб хөгжүүлэлтийн гол чиг хандлагын нэг бол янз бүрийн дэлгэцийн хэмжээ, нягтралд дасан зохицох вэб сайтыг бий болгоход чиглэсэн хариу үйлдэл үзүүлэх дизайныг ашиглах явдал юм. Илүү олон хүмүүс мобайл төхөөрөмж дээр вэб рүү нэвтэрч байгаа тул энэ нь маш чухал бөгөөд вэбсайтуудыг эдгээр жижиг дэлгэцүүдэд оновчтой болгох шаардлагатай байна. Сүүлийн жилүүдэд мобайл төхөөрөмжүүдийн өсөлт, мэдээллийн нууцлал, аюулгүй байдлын ач холбогдлын улмаас вэбэд томоохон өөрчлөлтүүд гарсан. Энэ нь хариу үйлдэл үзүүлэх вэб дизайн, Прогрессив вэб програмууд (PWAs), WebAuthn API зэрэг шинэ вэб технологи, стандартуудыг хөгжүүлэхэд хүргэсэн бөгөөд энэ нь хэрэглэгчдэд вэб контент, үйлчилгээнд олон төрлийн төхөөрөмж дээр илүү хялбар, аюулгүй нэвтрэх боломжийг олгодог.

- ❖ Аюулгүй байдал нь өнөө үед вэб системд ихээхэн анхаарал хандуулдаг асуудал болж байгаа бөгөөд улам их хэмжээний мэдээллийн зөрчил, кибер халдлага гарч байна. Үүний үр дүнд вэб хөгжүүлэгчид өөрсдийн хэрэглээний аюулгүй байдлыг хангах, болзошгүй аюулаас хамгаалахын тулд хамгийн сүүлийн үеийн аюулгүй байдлын туршлага, технологийг сайн мэддэг байх шаардлагатай.
- ❖ Орчин үеийн вэб хөгжүүлэлтийн хамгийн чухал чиг хандлагын нэг бол үүлэнд суурилсан үйлчилгээ, сервергүй тооцоолол руу шилжих явдал юм. Үүлэнд суурилсан үйлчилгээний тусламжтайгаар хөгжүүлэгчид өөрсдийн сервер болон дэд бүтцийг удирдах шаардлагагүйгээр вэб программуудыг хурдан бөгөөд хялбар бүтээж, байршуулахын тулд үүлэн тооцооллын хүчийг ашиглах боломжтой.
- ❖ Ерөнхийдөө өнөөгийн вэб систем нь нарийн төвөгтэй бөгөөд байнга өөрчлөгдөж байдаг боловч энэ нь хөгжүүлэгчдэд дэлхийн үзэгчдэд хүрч чадах шинэлэг, сонирхолтой програмуудыг бүтээх асар их боломжийг олгож байгаа. Мөн өнөөгийн вэб систем нь дижитал контент, үйлчилгээ, харилцан үйлчлэлийн хувьд боломжтой зүйлсийн хил хязгаарыг үргэлжлүүлэн шахаж буй хүчирхэг, уян хатан платформ юм.

Өнөөдрийн байдлаар Монгол улсад MOBINET LLC “ISP” компани нэвтрүүлсэн үйл ажиллагаанд ашиглаж албан байгууллагуудад санал болгож байна. Үүний жишээ бол Zscaler систем юм. Zscaler нь вэб, аппликейшн, дата, үйлчилгээнүүдийг аюулгүй байдлын хамгаалалтын хэрэгслүүдийн нэг бөгөөд анхдагч SaaS (Software as a Service) байгууллага юм. Zscaler-ийн үйлчилгээ нь бүхэлдээ аюулгүй байдлын зорилгоор хангах бөгөөд компанийн интернэт холболтыг захиалгатай замын хэлбэр, ашиглалтын төрлөөр хамгаалдаг байдлыг бүрэн баталгаажуулна.



Зураг 13. Zscaler

Zscaler нь гол зорилгоор аюулгүй байдлын үйлчилгээнүүдийг нээлттэй, шийдвэрлэлттэй, хүчин чадалтай хэрэглэж байгаа бөгөөд компанийнхаа гарын авлагыг дээшлүүлэхэд зориулж тухайн компанид хүлээн авагчийн хэмжээгээр үйлчилгээ үзүүлнэ. Zscaler нь компаниудын байгууллага, дэргэдэх үйлчилгээндээ технологийн шийдвэрлэл, хэрэглээний санах ойн тогтолцоог хянах, аюулгүй байдлыг санхүүжилтэй ажиллагаатай хамгаалдаг зорилготой юм. Мөн хиймэл оюун ухааныг хангахад

зориулагдсан аюулгүй байдлын шинжилгээний технологийн үйлчилгээ юм. Энэ технологи нь хэрэглэгчийн ухаалаг, шилдэг, шуурхай веб хуудсуудад ханддаг, мэдээлэл суулгах болон хандуулах програмуудад зам, шалгалтыг дамжуулдаг бөгөөд аюулгүй байдлын үйл ажиллагааны төвөөс олон улсын байгууллага, банк, онлайн дэлгүүр гэх мэт санхүүгийн аюулгүй байдлын хамгийн дээд түвшинд ашиглагддаг. Zscaler үүлэн үйлчилгээ нь үүнээс сэргийлдэж, онлайн дамжуулалтын аюулгүй байдлыг сулруулах, хадгалах зэрэг төхөөрөмжүүдийг ашиглан мэдээллийг аюулгүй байдлын түвшинд дээшлүүлэхэд тусалж байна.

ДҮГНЭЛТ

Дэлхийн хэмжээнд кибер аюулгүй байдал, системийн, мэдээллийн аюулгүй байдал нь өнөөдрийн цахим шилжилтийн хүрээнд номер нэгт анхаарах зүйл болсон. Иймд системүүдийг сүлжээний түвшинд ямар нэгэн халдлагаас урьдчилан сэргийлэх арга зам илүү нарийн төвөгтэй байна. Мөн хиймэл оюун ухаан хөгжсөнөөр сүлжээний аюулгүй байдлын төхөөрөмжүүд ч даган хув,саж улам илүү боловсронгуй болж байна. Иймд сүлжээний, мэдээллийн, кибер аюулгүй байдлыг олон нийтэд илүү энгийнээр илүү хүртээмжтэй, илүү мэргэжлийн байдлаар хүргэх шаардлага гарч байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Кибер аюулгүй байдлын зөвлөлийн тайлан

[2] “Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр 2010-2015” дүгнэлт

[3] тайлан

[4] “ДЦХБ, Олон Улсын кибер аюулгүй байдлын индекс - 2020”

[5] Үндэсний дата төв УТҮГ-ын 2017 оны үйл ажиллагааны жилийн эцсийн

[6] https://legalinfo.mn/mn

[7] https://mddc.gov.mn/mn/

[8] Journal of Network and Computer Applications 40 (2014) 307–324

[9] https://crc.gov.mn/

ХӨГЖҮҮЛЖ БУЙ ПРОГРАММЫН НИЙЛҮҮЛЭЛТИЙН ГИНЖИН ХЭЛХЭЭНИЙ АЮУЛГҮЙ БАЙДЛЫН СУДАЛГАА

[1]Т.Отгонбаяр, [2]Г.Ганчимэг

[1,2]Компьютерын ухаан салбар, Мэдээлэл, Холбооны Технологийн Сургууль, ШУТИС, Монгол улс

[1]senarius.s@gmail.com, [2]ganaa@must.edu.mn

***Хураангуй*—Бараг бүх программ хангамжийн төсөлд гуравдагч талын сан, веб сервис эсвэл хэсэгчлэн авч ашигласан кодын хэсэг багтдаг. Программ хангамжийг хөгжүүлэх ийм арга нь функцийг хурдан хөгжүүлэх, одоо байгаа кодыг дахин ашиглах боломжийг олгодог боловч нийлүүлэлтийн гинжин хэлхээний довтолгооны хаалгыг нээж өгдөг. Иймээс дэлхий даяар программ хангамжийн нийлүүлэлтийн гинжин хэлхээний *(supply chain)* халдлагын талаарх санаа зовоосон асуудал улам бүр нэмэгдээд зогсохгүй, advanced persistent threat (APT) аргатай холбоотой халдлагын аргууд улам боловсронгуй болж байна. Ийм учраас программ хангамжийн аюулгүй байдлын стратегийг хөгжүүлэлтийн эхний үе шатнаас нь дахин үнэлэх шаардлагатай. Энэхүү судалгааны зорилго нь зөвхөн программ хангамж хөгжүүлэгчдэд орчин үеийн программ хангамжийн нийлүүлэлтийн гинжин хэлхээний аюулаас хамгаалах, эрсдлийн хүрээг багасгах зорилготой юм.**

Түлхүүр үг— Software Supply Chain, Security, Threat, Threat Mitigation

I. Удиртгал

Хакерууд программ хангамжийн нийлүүлэлтийн гинжин хэлхээг ашиглан системийн админ болон системийн орчны хувьсагчдын мэдээллийг хулгайлан нууцаар бүхэл систем болон сүлжээ рүү нэвтрэх нь жил ирэх бүр нэмэгдэж байна. Халдлагын хүрээ нь зөвхөн нэг системийг сонгохоос эхлэн бүхэл бүтэн сүлжээний дэд бүтэц хүртэл байна [1-6]. Уламжлалт аргаар системийг халдлагаас хамгаалахад ихэвчлэн хост, сүлжээний аюулгүй байдал, firewall, anti-mailware зэрэг арга техникуудэд түлхүү анхаардаг [7]. Дээрх аргууд нь яг систем хөгжүүлэлтийн үеийн аюулгүй байдлын баталгаа бүрэн болж чаддаггүй [6-7]. Орчин үед систем болон сүлжээний аюулгүй байдлын стандарт ерөнхийдөө сайжирсан нь хакерууд программ хангамжийн нийлүүлэлтийн гинжин хэлхээг онилон системд халдах эрсдлийг ихэсгэж байгаа.

Түүнчлэн программ хангамжийн нийлүүлэлтийн гинжин хэлхээ нь өөрөө аюулгүй байдлын арга техникээр төдийлөн сайн хангагдаагүй байдаг нь нөлөөлж байна. Энэ сэдвийн хүрээнд хамгийн том жишээ бол “SolarWinds” гэж нэрлэгдсэн халдлага бөгөөд хакерууд тухайн системийн шинэ хувилбарт аюултай код нэмсэн бөгөөд тухайн шинэ хувилбарыг татан ашигласан халдлагад өртсөн системийн хүрээ нь дэлхий даяар бөгөөд дэлхий дамнасан корпорациуд төрийн байгууллагууд хүртэл багтаж, нийт халдварласан хэрэглэгчдийн тоо 18000 гэсэн тооцоо гарсан байдаг [5].

II. Нийлүүлэлтийн гинжин хэлхээний тухай

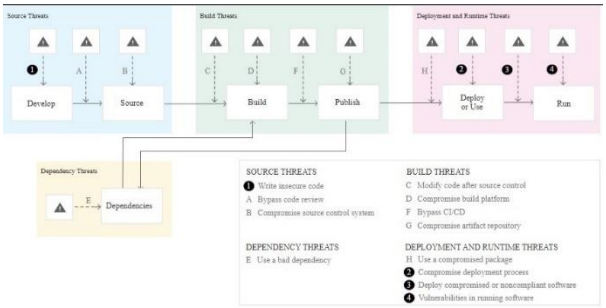
Программ хангамжийн нийлүүлэлтийн гинжин хэлхээ нь эх код, хоёртын файлууд болон бусад бүрэлдэхүүн хэсгүүдээс бүрдэнэ. Үүнд программыг бий болгох, савлах, ашиглахад зориулсан хөгжүүлэлтийн баг, багаж хэрэгсэл, үйл явц, үүнийг танай байгууллагын дотор болон гадна талд ажиллуулахад ашигладаг дэд бүтцийг багтаасан болно. Энгийнээр хэлбэл, программ хангамжийн нийлүүлэлтийн гинжин хэлхээ нь хөгжүүлэлтээс эхлээд үйлдвэрлэл, шинэчлэлт, сайжруулалт хүртэл тухайн кодыг хөндөж байгаа бүх зүйл юм [4]. Ерөнхийдөө программ хангамжийн нийлүүлэлтийн гинжин хэлхээ нь программ хангамжийг хөгжүүлэх бүх амьдралын мөчлөгийн туршид программ хангамжийг бүтээх, үйлдвэрлэх, түгээхэд шаардагдах бүх үйл ажиллагааг нэгтгэдэг гэж болно. *Үүнд [1-6]:*

- Программ хангамжийн хөгжүүлэлтийн амьдралын мөчлөгийн (SDLC) үйл явцын элементүүд, үүнд таны үүсгэсэн код, түүний хамаарал, программ хангамжийг хөгжүүлэх, багц суулгах, туршилтын орчин болон программ хангамжийг ажиллуулахад ашигладаг дотоод болон гадаад программ хангамжууд орно.
- Системд нэвтрэх процесс болон бодлого, тест, *"review"*, хяналт.
- Хөгжүүлэлтэнд ашиглаж байгаа бусад системүүд болон сангууд тэдгээрийг ажиллуулах, *"build*" хийх.

- Нээлттэй эхийн эсвэл гуравдагч этгээдийн программ хангамжийг энтерпрайс системийн нэг хэсэг болгон ашигласан.
- Нээлттэй эхийн платпормыг энтерпрайс системд ашигласан.
- Вэндоруудын мэргэжлийн үйлчилгээнүүд, зөвлөгөө өгөх эсвэл хөгжүүлэлтийн үйлчилгээнүүд бүтэн болон хэсэгчилсэн.
- Энтерпрайс-ууд партнер ашиглан дата хадгалах болон боловсруулах.
- Үүлэн технологийн үйлчилгээнүүд. Үүнд: IaaS, PaaS эсвэл SaaS
- Өдийг хүртэл дата болон системийн эрх нь хүчинтэй байгаа хуучин хамтран ажиллагчид, партнерууд.

III. Аюулын бүдүүвч

Аюулын бүдүүвчийн загварчлалын тухайд мэдлэг, сургалт, эрсдлийн үнэлгээ гэсэн уламжлалт гэсэн 3 үндсэн ашиглах арга байдаг [1]. Хэрэв бид зорилго, оролцогч, довтолгоо, TTP (тактик, арга техник, процедур), нийлүүлэлтийн гинжин хэлхээнд хамаарах аюулын үүрэг гүйцэтгэгч гэх мэт өргөн хэрэглэгддэг ойлголтуудыг авч үзвэл, өргөн хэрэглэгддэг STIX [35] аюулын бүдүүвч илүү тохиромжтой болно. Гэсэн хэдий ч энэ сэдвийн хүрээнд бид илүү нийлүүлэлтийн гинжин хэлхээг чиглэсэн *“Supply chain Levels for Software Artifacts”* (SLSA) загварт илүү анхаарлаа хандуулах ба, (SLSA) нь мэдээлэл технологийн салбарын том тоглогчдын зөвшилцлийн дагуу [2] зөвлөмж тогтоон, баталж нийлүүлэлтийн гинжин хэлхээний аюулгүй байдлын удирдамжуудын багц үүсгэдэг фремворк юм. SLSA нь нийлүүлэлтийн гинжин хэлхээг нийтлэг халдлагаас хамгаалахад тусалдаг [3].



Зураг 1. SLSA-д суурилсан аюулын бүдүүвч загвар. Энэ нь ердийн программ хангамжийн нийлүүлэлтийн гинжин хэлхээ болон хөгжүүлэлтийн амьдралын мөчлөгийг харуулсан бөгөөд бүх холбоос дээр тохиолдож болох халдлагын жишээг агуулдаг [3]

IV. Нийтлэг халдлагын төрлүүд

Хорлонтой нээлттэй эхийн код: Нээлттэй эхийн кодын эрсдэл нь аюул заналхийлэгчид олон нийтэд нээлттэй кодын модульд хорлонтой код оруулах үед үүсдэг бөгөөд үүнийг үл тоомсорлон хөгжүүлэгчид тодорхой функцуудыг гүйцэтгэхийн тулд кодын үнэгүй блокуудыг хайж, улмаар өөрсдийн дотроо нэмэн ашигладаг [14]. *“Typo squatting”* нь модулиудыг суулгах явцад үсгийн алдааны давуу талыг ашигладаг бол *“combo squatting”* нь модулиудын нэр олон үгнээс бүтсэн үед тухайн үгний дарааллын алдааг ашигладаг жишээ нь "nmap-python" гэж бичсэн "python-nmap" [23] *(зураг 4)*. Хорлонтой модулиуд нь дууриасан модулиудын үндсэн функцуулыг агуулах ба нэмээд ихэвчлэн системийн функц, “shell script”, “boot” зэргийг ажиллуулан системд хохирол учруулах эсвэл эмзэг дата цуглуулах зориулалтай байдаг [10]. Нээлттэй эхийн энэ асуудал нь нээлттэй биш программ хангамжид ч нөлөөлж болзошгүй, учир нь тухайн программыг хөгжүүлэгчид бүтээгдэхүүндээ нээлттэй эх кодыг ашиглахгүй байх нь орчин үеийн нөхцөлд бараг боломжгүй юм [9].

Hijack the Updates: Халдагчид эцсийн хэрэглэгчдэд зориулсан программ хангамжийг тогтмол шинэчлэх явцад хорлонтой кодыг ашиглан систем рүү нэвтэрч, чухал мэдээлэлд хандах боломжтой [24]. Аюул заналхийлэгчид хохирогчийн сүлжээнд давуу эрх, байнгын хандалтыг олж авахын тулд программ хангамжийн вендор-уудыг хакердах замаар төлөвлөгөөгөө гүйцэтгэнэ. Үндсэн арга нь тухайн вендоруудын шинэчлэлтүүдийг ашиглан эцсийн хэрэглэгчдийн бүх үндсэн системийн хамгаалтууд болох “firewall”, “router” гэх мэт тойрох замаар халдлагаа үйлдэнэ [25]. Ийм төрлийн халдлагын жишээ нь “NotPetya”, тухайн программ нь Украины нутаг дэвсгэрээс цааш тархаж, олон улсын тээвэрлэлт, санхүүгийн үйлчилгээ, эрүүл мэндийн үйлчилгээ зэрэг дэлхийн томоохон чухал салбаруудад аюул үүсгэсэн [13].

Undermine the Codesigning *(Код зохиогчийн таних тэмдгээр дамжих)*: Код зохиогчийн таних тэмдэг болон кодын бүрэн бүтэн байдлыг баталгаажуулахын тулд кодын тэмдэглэгээг (*Code-signing)* ашигладаг. Халдагчид өөрөө өөртөө гарын үсэг зурах гэрчилгээ *(sefl-sign certificate)*, гарын үсэг зурах, шалгах системийг эвдэх болон цоорхойг ашиглах, эсвэл холбоотой аккоунтын буруу тохиргоог ашиглах замаар зорилгодоо хүрдэг. Дээрх аргыг хослуулан аюул заналхийлэгчид итгэмжлэгдсэн үйлдвэрлэгчийн дүрд хувирч, шинэ хувилбарт хортой код оруулах замаар эсвэл программ хангамжийн шинэчлэлтийг дуурайн эцсийн хэрэглэгчийн системд нэвтэрнэ [11-12]. Мөн аль хэдийн олон нийтэд ил болсон алдаагаар дамжин уг аргыг ашиглаж болно. *Жишээ нь*: Microsoft Windows CryptoAPI модуль нь Elliptic Curve Cryptography (ECC) функцын алдаагаар дамжин сертификетний баталгаатай эсэхийг хуурах арга [15-16].

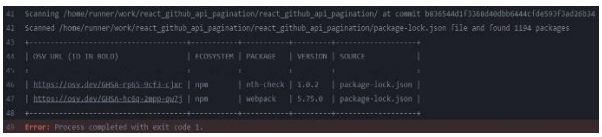
V. Халдлагын эрсдэл бууруулах стратеги

Автоматжуулалт/Automation & linter: Ерөнхийдөө аль хэдийн мэдэгдэж байгаа секюрити

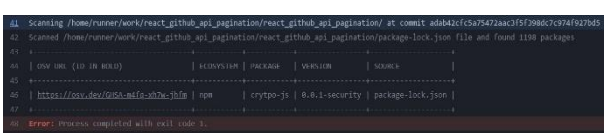
цоорхойнуудыг ашиглахаас зайлсхийхийн тулд программд ашиглаж байгаа бүх модиулуудаа сканнердах *(аюулгүй байдлын сканнер)*, ба давхар тасралтгүй интеграцийн (CI) хэрэгслийг ашиглах хэрэгтэй.

- Модулиудын түгжээний файлууд нь автоматаар үүсгэгддэг бөгөөд хүний нүдээр унших, засвар үйлчилгээ хийх зориулалттай биш тул *(зураг 1-5)*. “Lock file injection” [27-28]-ээс сэргийлэхийн тулд заавал “linter” ашиглан шалгах хэрэгтэй.
- “Arbitery command execution” [29] ашигласан модулиудыг аль болох ашиглахаас зайлсхийх хэрэгтэй эсвэл нэмэлт команд ашиглан [30] алгасах, бүр дараагийн алхам нь прожектийн “root” дотор ".npmrc" төслийн файл *(зураг 5)* үүсгэн "ignore-scripts" мөр нэмэх арга хэмжээ авч болно эсвэл глобал npm тохиргоонд энэ өөрчлөлтийг нэмсэнч болно.
- "Dependency confusion attack" [32] энэ төрлийн халдлагаас сэргийлэхийн тулд программд ашиглагдаж буй модулиудыг сохроор шинэчлэн суулгахаас зайлсхийх хэрэгтэй. Дотоод хувийн багцын нэрийг ашиглах тохиолдолд илүү өндөр хувилбартай нийтийн багцын нэртэй давхцаж байгаа нь багц менежерийг нийтийн багц руу шилжүүлэхэд хүргэж болзошгүй бөгөөд аюулгүй байдлын болзошгүй эрсдэлд хүргэнэ [31].
- Trojans source [32] халдлагаас зайлсхийж, хоёр чиглэлтэй (BIDI) юникод хувьсагчдыг шалгах эсвэл идэвхгүй болгох *(зураг 2, 4)*, GitHub нь (BIDI) ашигласан байна гэж анхааруулга харуулах боловч зөвхөн файл тус бүрийн хувьд харуулдаг.

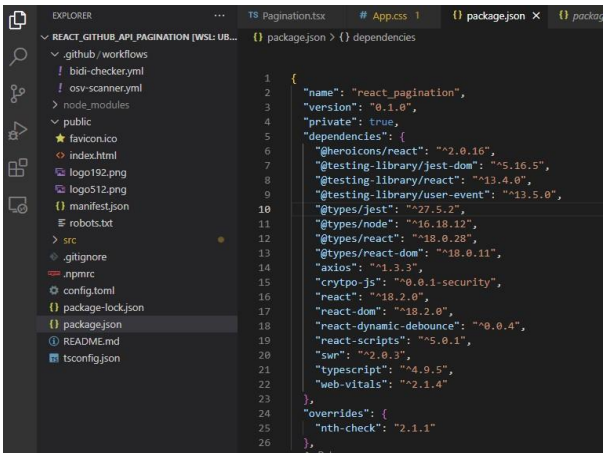
Зураг 2. BIDI checker github action ажилласны үр дүнд Trojans source илрүүлсэн байдал, ашигласан жишээ код [34]



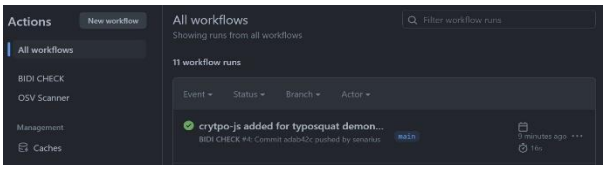
Зураг 3. osv-scanner хуучны модулиудын цоорхойг илрүүлсэн байдал, ашигласан жишээ код [34]



Зураг 4. osv-scanner typosquat ашигласан модуль илрүүлсэн байдал, ашигласан жишээ код [34]



Зураг 5. github дээр action автоматжуулалт нэмсэн байдал, nth-checker хуучин хувилбарыг хүчээр package.json файл дотор "override" дээшлүүлэн аюулгүйн байдлын эрсдлийг зассан байдал, “./.npmrc” тохиргоо нэмэн arbitrary command execution эрсдлээс сэргийлсэн, “./config.toml” osv-scanner дээрх зарим нууцлалын алдааг энэ тохиргоонд бичиж алгасах боломжтой, ашигласан жишээ код [34]



Зураг 6. After remediation all action works without error, demonstration source code included in

Defense in Depth: Defense in Depth (DiD) нь аюулгүй байдлын ерөнхий байдлыг нэмэгдүүлэхийн тулд давхар хамгаалалтыг нэмэх зарчим юм. Өөрөөр хэлбэл, хэрэв халдлага нь хамгаалалтын нэг механизмыг доголдуулахад хүргэсэн бол бусад арга хэмжээ нь халдлагыг цаашид таслан зогсоох, бүр урьдчилан сэргийлэх арга хэмжээ авах болно [22].

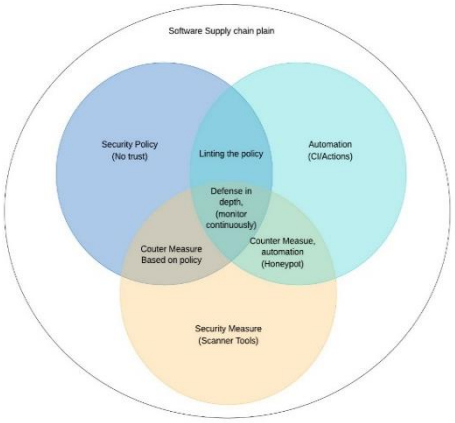
Zero Trust: Zero Trust (ZT) нь хэзээ ч аль нэг системийн "resource" итгэл үзүүлэхгүй, харин "resource"-т хандах хүсэлт тус бүрийн параметрүүдийг тасралтгүй хянах зарчим дээр тулгуурлан ажилладаг бөгөөд "resource" болгонд хандалт хийх хатуу протоколууд бий болгох зорилготой юм. ZT-ийн хүрээнд "resource" гэдэг нь *(программ, сүлжээний хандалт, дата хадгалалт, гэх.мэт)* хамаарна [8]. Энэ зарчмын хүрээнд дотоод сүлжээ болон дотоод хандалт, гадаад сүлжээ, гадаад сүлжээгээр дамжсан хандалтаас илүү аюулгүй гэж ялгаж авч үзэхгүй. Бид дотоод сүлжээ хэзээ нэгэн цагт заавал кибер халдалгад өртөнө гэж бодон үргэлж "authenticate" хийнэ гэж ойлгох хэрэгтэй. Энэ зарчмын хувьд multi factor authentication (MFA) [19-20], чиг үүргийн тусгаарлалтыг *(micro service, user access, service account)* эдгээр дээр заавал хэрэгжүүлэх болон хэрэглээний хяналтыг *(monitoring)* нэмэх шаардлагатай.

Honeypot: "Honeypot" нь кибер халдагчдыг системд нэвтэрсэн үед эрт илрүүлэх болон мэдэгдэх түүнчлэн эрт хариу арга хэмжээ авч халдлагын цар хүрээг

хянахад зориулсан жижиг систем. "Honeypot" гол үүрэг нь ихэвчлэн үндсэн системээс тусдаа байршин халдлагад өртсөн тохиолдолд халдлагын бай болох зорилготой ба давхар мэдээлэл цуглуулах болон шууд хөгжүүлэгчдэд мэдэгдэх үүрэгтэй [21]. Хөгжүүлэгчдэд мэдэгдэхийн тулд урхи болгон микро вэб үйлчилгээг бэлтгэж, уг системийн орчны хувьсагчийг зорилтод эх код руу байршуулах замаар ажилладаг. Кибер халдагад өртсөн тохиолдолд халдагчдын анхаарлыг өөртөө татан, үндсэн системд цохилт өгөхөөс, аюул учруулахаас өмнө тухайн довтолгооны талаар эрт сэрэмжлүүлж, халдагч болон тэдний аргын тухай мэдээллийг хамгаалалтын нэг хэсэг болгон цуглуулах болно. 7 дугаар зурагт үзүүлснээр AWS-н "access-key-id" болон "access-key-secret"-ийг үндсэн системийн эх код дотор өгөөш болгож, "Honeytoken"-ийн хувьд AWS дээр вэб сервисээ "lambda" хэлбэрээр байршуулан "slack" руу "webhook" хэлбэрээр мэдээллэх байдлаар тус тус тохируулсан болно [36].

Зураг 7. Халдлагад өртсөн мэдэгдэх лог Slack webhook ашиглан realtime-р мэдэж болно, ашигласан жишээ код ".env.aws" [34]

Зураг 8. Бодит байдлын туршилт AWS-ийн credentials зориудаар ил тавин шалгасан байдал. Зориудаар aws-ийн credentials-уудыг ил тавихад 4мин хугацаанд 100+ өөр халдлагын лог бүртгэгдсэн.



Зураг 9. Халдлагын эрсдэл бууруулах стратегийг Venn диаграмм дээр буулган уялдаа холбоог харуулсан байдал

Дүгнэлт

Аюулгүй байдлын сканнер, хамгаалалтын хэрэгслүүд, автоматжуулалт, аюулгүй байдлын бодлогыг хэрэгжүүлэн системийг байнга хянаж ашигласнаар нийлүүлэлтийн гинжин хэлхээний аюулгүй байдлын хүрээнд болзошгүй халдлагын нөлөөллийг үр дүнтэй бууруулж чадна. Аюулгүй байдлын бодлого нь 9 дүгээр зурагт үзүүлснээр "Zero Trust" ба "Defense in Depth" (DiD) арга барилыг баримтлах хэрэгтэй. Мөн программ хангамжийн шаардлага, төсөв, хөгжүүлэлтийн багийн туршлага зэрэг хүчин зүйлс дээр үндэслэн аюулгүй байдлын арга хэмжээ, аюулгүй байдлын сканнер хэрэгсэл зэргийг сонгох хэрэгтэй. Автоматжуулалт нь хөгжүүлэлтийн багийн тодорхойлсан аюулгүй байдлын арга хэмжээний аудитор, аюулгүй байдлын хэрэгжүүлэлтийн стандартын үүргийг гүйцэтгэнэ. Хэдийгээр эдгээр аргууд нь нийлүүлэлтийн гинжин хэлхээний халдлагын магадлалыг мэдэгдэхүйц бууруулж чаддаг ч аюулгүй байдлын бүх систем нь хамгийн сул холбоос шиг хүчтэй байдаг тул бүрэн урьдчилан сэргийлэх баталгаа байхгүй гэдгийг анхаарах нь чухал юм. Гэсэн хэдий ч бидний санал болгож буй арга нь халдлагад өртсөн тохиолдолд хөгжүүлэгчид халдлагыг багасгах үр дүнтэй сөрөг арга хэмжээ болж чадна.

Ном зүй

[1] P. Ladisa, H. Plate, M. Martinez, and O. Barais. Taxonomy of Attacks on OpenSource Software Supply Chains, 2022

[2] "Threat Model" SLSA. https://slsa.dev/spec/v0.1/threats (Accessed: 2023-03-07).

[3] "Requirements." SLSA. https://slsa.dev/spec/v0.1/requirements (Accessed: 2023-03-07).

[4] "2.1 Digital Supply Chain Security" Securing the Nation's Critical Infrastructures: A Guide for the 2021-2025 Administration. (n.d.). United States: CRC Press.

[5] R. Alkhadra, J. Abuzaid, M. AlShammari, and N. Mohammad, "Solar winds hack: In-depth analysis and countermeasures," in Proc. 2021 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), pp. 1–7, doi: 10.1109/ICCCNT51525.2021.9579611.

[6] U.S. Department of Homeland Security, "Security in the softwarelifecycle: Making software development processes—and software produced by them—more secure. DRAFT Version 1.2. ," 2006, (Accessed: 2023-01-28). [Online]. Available: http://www.cert.org/books/secureswe/SecuritySL.pdf.

[7] R. A. Khan, S. U. Khan, H. U. Khan, and M. Ilyas, "Systematic mapping study on security approaches in secure software engineering," IEEE Access, vol. 9, pp. 19139–19160, 2021, doi: 10.1109 (Accessed. 2023-02-26).

[8] Scott Rose, et al., "Zero Trust Architecture," NIST SP 800-207 (August 2020), https://doi.org/10.6028/NIST.SP.800-207.

[9] T. Herr, J. Lee, W. Loomis, and S. Scott, "Breaking trust: Shades of crisis across an insecure software supply chain," https://www.atlanticcouncil.org/in-depth-research-reports/report/breakingtrust-shades-of-crisis-across-an-insecure-software-supply-chain/, 2020, (Accessed: 2023-03-13).

[10] "Malicious packages found to be typo-squatting in Python Package Index." https://snyk.io/blog/malicious-packages-found-to-be-typo-squatting-in-pypi/. (Accessed: 2023-03-10).

[11] ENISA, "Valid Digital Certificates Code Signing Malware," European Union Agency for Cybersecurity, June 30, 2018, https://www.enisa.europa.eu/ publications/info-notes/valid-digital-certificates-code-signing-malware.

[12] CISA, “Alert (AA20-014A): Critical Vulnerabilities in Microsoft Windows Operating Systems,” Cyber and Infrastructure Security Agency, January 14, 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-014a.

[13] Fayi, Sharifah. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. 10.1007/978-3-319-77028-4_15.

[14] Wei, Zhaohui. (2011). Research on the Application of Open Source Software in Digital Library. Procedia Engineering. 15. 1662-1667. 10.1016/j.proeng.2011.08.310.

[15] CERT/CC Vulnerability Note VU#849224, https://kb.cert.org/vuls/id/849224/

[16] CERT/CC Vulnerability Note VU#491944, https://kb.cert.org/vuls/id/491944/

[17] A distributed vulnerability database for Open Source, https://osv.dev/

[18] OpenSSF, https://securityscorecards.dev/

[19] Williamson, Joseph & Curran, Kevin. (2021). Best Practice in Multi-factor Authentication. Semiconductor Science and Information Devices. 3. 10.30564/ssid.v3i1.3152.

[20] “Mfa is a necessary chore! exploring user mental models of multi-factor authentication technologies,” https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1649&context=hicss-53, 2020, (Accessed: 2023-02-10).

[21] Titarmare, Neha & Hargule, Nayankumar & Gupta, Anand. (2019). An Overview of Honeypot Systems. International Journal of Computer Sciences and Engineering. 7. 394-397. 10.26438/ijcse/v7i2.394397.

[22] Stytz, Martin. (2004). Considering Defense in Depth for Software Applications. Security & Privacy, IEEE. 2. 72 - 75. 10.1109/MSECP.2004.1264860.

[23] Vu, D.L., Pashchenko, I., Massacci, F., Plate, H., Sabetta, A.: Typosquatting and combosquatting attacks on the python ecosystem. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 509–514. IEEE (2020)

[24] Yang, Jeong & Lee, Young & McDonald, Arlen. (2022). SolarWinds Software Supply Chain Security: Better Protection with Enforced Policies and Technologies. 10.1007/978-3-030-92317-4_4.

[25] Cybersecurity and Infrastructure Security Agency (CISA), Defending Against Software Supply Chain Attacks https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf, 2021, (Accessed: 2023-03-14).

[26] George Karantzas, Constantinos Patsakis, 2021, An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. https://doi.org/10.3390/jcp1030021.

[27] Bos, A. M. (2023). A Review of Attacks Against Language-Based Package Managers. ArXiv. /abs/2302.08959

[28] Arbitrary command execution, vulnerability, https://nvd.nist.gov/vuln/detail/cve-2022-23812, (Accessed: 2023-03-21).

[29] Npm docs, ignore script option, https://docs.npmjs.com/cli/v7/commands/npm-find-dupes#ignore-scripts, (Accessed: 2023-03-18).

[30] 3 Ways to Mitigate Risk Using Private Package Feeds, Secure your hybrid supply chain, (2021) https://azure.microsoft.com/mediahandler/files/resourcefiles/3-ways-to-mitigate-risk-using-private-package-feeds/3%20Ways%20to%20Mitigate%20Risk%20When%20Using%20Private%20Package%20Feeds%20-%20v1.0.pdf, (Accessed: 2023-03-19).

[31] A Confusing Dependency, vulnerability, https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-29427, (Accessed: 2023-02-21).

[32] Boucher, N., & Anderson, R. (2021). Trojan Source: Invisible Vulnerabilities. ArXiv. /abs/2111.00169

[33] Demonstration, Otgonbayar Tuukhbaatar, https://github.com/senarius/react_github_api_pagination

[34] STIX: Assets Affected in an Incident. Available online: http://stixproject.github.io/documentation/idioms/affected-assets/, (Accessed: 2023-03-21).

[35] Honeytoken notifier system, GGCanary, GitGuardian, Available online: https://github.com/GitGuardian/ggcanary, (Accessed: 2023-03-22).

5G СПЕКТРИЙН ХУВААРИЛАЛТ, ТӨЛБӨРИЙН АСУУДЛЫН СУДАЛГАА

Алтангэрэлийн Болортуяа[1], Батаагийн Отгонбаяр[2]

[1]Магистрант, Монгол улс, Улаанбаатар, Шинжлэх Ухаан Технологийн Их Сургууль, Холбооны салбар

[2]Доктор, профессор, Монгол улс, Улаанбаатар, Шинжлэх Ухаан Технологийн Их Сургууль, Холбооны салбар

J.RC22E002@must.edu.mn [1], otgonbayar_b@must.edu.mn [2],

***Хураангуй*: Хөдөлгөөнт холбооны 5 дугаар үеийн сүлжээ нь өндөр хурд, найдваржилт, багтаамж, бага хоцролт, давтамжийн үр ашгийг шинэ түвшинд гаргаж буй технологи болж байгаа ба Монгол улсад энэхүү технологийг нэвтрүүлэхэд судлагдах шаардлагатай байгаа асуудлын нэг нь 5G спектрийн хуваарилалт, төлбөрийн асуудал юм.**

Түлхүүр үг: 5G технологи, радио давтамжийн хуваарилалт, радио давтамжийн төлбөр

I. УДИРТГАЛ

Дэлхийн улс орнууд үүрэн холбооны 5 дахь үеийн шилжилтийг нэвтрүүлээд эхэлсэн бөгөөд манай улс 2023 онд уг шилжилтийг хийхээр төлөвлөсөн.

Энэхүү төлөвлөлттэй холбоотойгоор 5G радио спектрийн хуваарилалт, Монгол Улсын эрх зүйн орчин орчин Олон Улсын IMT-2020 стандартын дагуу 5G радио давтамжийн төлбөрийг тооцох аргачлалуудыг судлан алгоритмыг боловсруулах зорилтыг дэвшүүлсэн.

II. СПЕКТРИЙН ХУВААРИЛАЛТ

Радио долгионы тухай хуулийн 3.1 дэх хэсэгт “радио долгион” гэж агаарын орон зайд тархаж байгаа цахилгаан соронзон орны 3000 Гега Герц хүртэлх давтамжтай хэсгийг хэлнэ гэж зааж өгсөн [1]. Радио долгион нь шинж чанар, онцлог, долгионы уртаас хамааран хил хязгааргүй тархдаг хязгаарлагдмал нөөц юм. Энэхүү нөөц нь улс орноор хязгаарлагддаггүй хил дамнадаг учраас Олон Улсын Цахилгаан Холбооны байгууллага (ITU) 1865 оноос эхлэн дэлхийн улс орнуудыг байршлаас хамааруулан радио долгионыг 3 бүсэд хуваан цахилгаан холбоо, радио холбоо, өргөн нэвтрүүлэг, сансрын холбоо, интернэт, программ хангамж, хиймэл оюун ухаан зэрэг мэдээлэл, харилцаа холбооны салбарын судалгаа шинжилгээний байгууллага, сургуулиуд, зохицуулагч байгууллагуудтай хамтран ажиллаж, тухайн салбарт үүсэж буй хүндрэл асуудлыг шийдвэрлэн холбогдох дүрмийг боловсруулан батлан гаргадаг [2]. Үүнийг нь тухайн байгууллагад гишүүнчлэлтэй улс орнууд даган мөрдөн, өөрийн улс орондоо хэрэгжүүлдэг. Манай Монгол Улс Олон Улсын Цахилгаан холбооны байгууллага (цаашид ОУЦХБ гэх)-ын Дэлхийн радио холбооны дүрэм гэж нэрлэгддэг Олон Улсын гэрээнд 1964 онд нэгдэн орсон [3]. Энэхүү гэрээгээр Монгол Улсын нутаг дэвсгэрт үйл ажиллагаа явуулж байгаа Радио холбооны үйлчилгээ нь бусад орны Радио холбооны үйлчилгээнд нөлөөлөл үзүүлэхгүй байх мөн бусад орны Радио холбооны үйлчилгээнээс үзүүлэх нөлөөллөөс хамгаалагдаж байдаг. Ийм учраас Монгол Улсын радио давтамжийн спектр төлөвлөлт, хуваарилалт нь ОУЦХБ-ын төлөвлөлттэй нягт уялдсан байх шаардлага тавигддаг. ОУЦХБ нь үйл ажиллагааны чиглэлээс хамааран хэд хэд хуваагддаг бөгөөд Радио холбооны товчоо (ITU-R)-нд бүх төрлийн радио холбооны үйлчилгээний радио давтамжийн спектрийг ижил тэнцүү нөхцөлөөр, эдийн засгийн хувьд үр ашигтай ашиглах боломжийг бүрдүүлэхээр байнгын ажиллагаатай зургаан судалгааны бүлэг, хэд хэдэн ажлын хэсэг ажилладаг.

Энэхүү судалгааны үндэс нь 5G технологид ашиглахаар тодорхойлогдож буй зурваст судалгаа хийж, судалгааны үр дүнг Дэлхийн Радиогийн Их Хуралд танилцуулан батлуулдаг. Дэлхийн Радиогийн Их Хурал нь сүүлийн жилүүдэд 4 жил тутамд хуралдаж хэлэлцсэн асуудлаа шийдвэрлэж байна. Хамгийн сүүлд 2019 оны уг хурлаар 5G технологид ашиглах радио спектрийн зурвасуудыг тодорхойлсон [4].

Монгол Улсын хувьд дээрх радио спектрийн хуваарилалтыг хийхдээ Радио долгионы тухай хуулиар Цахим хөгжил, харилцаа холбооны яам бодлогын чиглэлээ тодорхойлж, Харилцаа холбооны зохицуулах хороо хэрэгжилтийг нь хангуулахаар заасан [1]. 5G радио спектрийн хувьд бодлогын чиглэлийн хүрээнд Харилцаа холбоо, Мэдээллийн технологийн газрын даргын 2020 оны А/45 тушаалаар батлагдсан “Монгол Улсад дараа үеийн хөдөлгөөнт холбооны системийг нэвтрүүлэхэд баримтлах бодлогын чиглэл” [5], Цахим хөгжил, харилцаа холбооны сайдын 2023 оны А/42 дугаар тушаалаар батлагдсан “Үндэсний радио давтамжийн хуваарилалтын хүснэгт” [6], Харилцаа холбооны зохицуулах хорооны 2023 оны 106 дугаар тогтоолоор батлагдсан “Дараа үеийн хөдөлгөөнт холбооны системд ашиглах радио давтамжийн зурвасын хуваарилалт, техникийн нөхцөл, шаардлага” [7] гэсэн

баримт бичгүүдээр нийт 16 радио спектрийн давтамжийн цараг тодорхойлсон байна.

МОНГОЛ УЛСАД 5G ТЕХНОЛОГИД АШИГЛАХААР ТОДОРХОЙЛОГДСОН СПЕКТРИЙН МЭДЭЭЛЭЛ

1-Р ХҮСНЭГТ

№	Зурвасын дугаар	Хэрэглэгч –Бааз станц (МГц)	Бааз станц –Хэрэглэгч (МГц)	Технологи
1	31	452,5-457,5	462,5-467,5	FDD
2	28	703-748	758-803	FDD
3	5	824-834	869-879	FDD
4	20	847-862	806-821	FDD
5	8	880-915	925-960	FDD
6	3	1710-1785	1805-1880	FDD
7	1	1920-1980	2110-2170	FDD
8	7	2500-2570	2620-2690	FDD
9	40	2300-2400		TDD
10	38	2570-2620		TDD
11	n74	1427-1470	1475-1518	FDD
12	n78	3300-3400		TDD
13	n77	3400-4200		TDD
14	n79	4500-4800		TDD
15	n258	24250-27500		TDD
16	n259/n260	37000-43500		TDD

Үүнээс үзэхэд Олон улсад 5G радио спектрийн хуваарилалтыг 68 зурваст хийсэн байхад Монгол улсад 16 радио давтамжийн зурваст буюу нийт хуваарилсан зурвасын 24%-ийн зурвасыг 5G технологид ашиглахаар заасан байна.

III. МОНГОЛ УЛС 5G ТЕХНОЛОГИЙГ ТУРШСАН БАЙДАЛ

“Монгол Улсад дараа үеийн хөдөлгөөнт холбооны системийг нэвтрүүлэхэд баримтлах бодлогын чиглэл”-ийн 3.4.4-д “Дараа үеийн хөдөлгөөнт холбооны 5 дахь үеийн технологийн үйлчилгээ эрхлэх болон радио давтамжийн ашиглах тусгай зөвшөөрлийг 2023 оноос эхлэн олгоно.” заасны дагуу Харилцаа холбооны зохицуулах хороо нь 2023 ондоо багтаан 5G технологид ашиглах радио давтамжийг сонгон шалгаруулалтын аргаар олгохоор төлөвлөн ажиллаж байгаа юм байна.

Монгол Улсад 5G технологийг нэвтрүүлэхээр үүрэн холбооны оператор компаниуд Радио долгионы тухай хуулийн 13.6-д “Эрдэм шинжилгээ, туршилт болон сонирхогчийн радио станцын зориулалтаар ашиглах эрхийн бичгийг гурван сарын хугацаагаар олгох бөгөөд хугацааг анх олгосон хугацаагаар нэг удаа сунгаж болно.” заасны дагуу 2021 он эхлэн зөвшөөрлийг Харилцаа холбооны зохицуулах хорооноос авч, туршилтуудыг хийсэн байна.

Үүрэн холбооны оператор компаниудаас 5G технологийн нэвтрүүлэхээр үйл ажиллагаагаа төлөвлөн туршилт хийсэн үр дүнг судалж үзвэл туршилтыг радио давтамжийн 3,300 МГц – 3,800 МГц-ийн зурваст, сүлжээ зохион байгуулалтын хувьд Non-stand-Alone технологийг сонгон туршсан байна. Туршилтаар гарсан хурдны хувьд татах хурд нь хамгийн ихдээ 1,710 Мбит/сек (Юнител), илгээх хурд нь хамгийн ихдээ 191,36 Мбит/сек (Ондо) хэмжигдсэн байна.

IV. 5G ТЕХНОЛОГИЙГ НЭВТРҮҮЛЭХЭД ШААРДАГДАХ ТӨЛБӨРИЙН АСУУДЛЫН СУДАЛГАА

5G технологийг Монгол Улсад нэвтрүүлэхдээ Мэдээлэл, харилцаа холбооны салбарт тусгай зөвшөөрөл авч үйл ажиллагааг явуулах эрхтэй болдог. Эдгээр зөвшөөрөл нь Харилцаа холбооны тухай хууль [8] болон Радио долгионы тухай хуулиар Радио давтамж ашиглах болон үйлчилгээ эрхлэх тусгай зөвшөөрөл авч ашигладаг. Одоогийн байдлаар дээрх зөвшөөрлүүдийн төлбөр нь 2 янз байдаг бөгөөд үйлчилгээ эрхлэх төлбөрийг Харилцаа холбоо, мэдээллийн технологийн газрын даргын 2017 оны А/42 дугаар тушаалаар батлагдсан “Тусгай зөвшөөрөл эзэмшигчдэд үзүүлэх зохицуулалтын үйлчилгээний хөлсний хэмжээг тогтоох журам” [9]-д үндэслэн Харилцаа холбооны зохицуулах хорооны 2022 оны 61 дүгээр тогтоолоор батлагдсан “Зохицуулалтын үйлчилгээний хөлсний хэмжээ” [10]-ний дагуу тооцдог бол радио давтамж ашиглах тусгай зөвшөөрлийн төлбөрийг Цахим хөгжил, харилцаа холбооны сайдын 2022 оны А/37 дугаар тушаалаар батлагдсан “Радио давтамжийн ашиглалт, үйлчилгээний төлбөр тогтоох журам” [11]-д үндэслэн Харилцаа холбооны зохицуулах хорооны 2023 оны 94 дүгээр тогтоолоор батлагдсан “Радио давтамж ашиглалт, үйлчилгээний төлбөрийн хэмжээ” [12] гэсэн баримт бичгүүдэд үндэслэн тус тус төлбөр хураамжийг тооцон авдаг байна.

Зохицуулалтын үйлчилгээний хөлс болон радио давтамж ашиглалтын төлбөрийг тооцдог хураамжуудыг тусгай зөвшөөрлийн хүчинтэй хугацаанд жил бүр тооцон авдаг ба үйлчилгээний хөлсний хэмжээ нь тогтмол дүн байдаг бол радио давтамж ашиглалтын төлбөр нь үндсэн 3 параметр үзүүлэлтээс хамааран тооцож төлбөрийг тогтоодог.

Энэхүү судалгааны хүрээнд бид 5G радио спектртэй холбоотой үүсэж буй төлбөрийн асуудлыг судалж байгаа тул үйлчилгээ эрхлэхтэй холбоотой төлбөрийн асуудлыг үлдээж, радио давтамжийн ашиглалттай холбоотой төлбөрийг нарийвчлан судаллаа.

Радио давтамжийн ашиглалт, үйлчилгээний төлбөр тогтоох журам [11]-ын дагуу радио давтамжийн ашиглалт, үйлчилгээний төлбөр тогтоох журмаар радио давтамжийн ашиглалтын төлбөрийг дараах томьёогоор тооцоолохоор томьёолсон.

$$P_L = (F + P + T) * 1.2 \quad (1)$$

F – Радио давтамжийн зурвас ашиглалтын төлбөр

P – Радио нэвтрүүлэгчийн гаралтын чадлын төлбөр

T – Төрөл ангилал / хамрах хүрээний төлбөр

1.2 – Радио давтамжийн зурвасын коэффициент

Радио давтамжийн зурвас ашиглалтын төлбөр нь ашиглах зурвасын цараа болон зурвасын өргөнөөс хамаарна, радио нэвтрүүлэгчийн гаралтын чадал нь ашиглах зурвасын цараа болон нэвтрүүлэх чадлын хэмжээнээс хамаарсан үзүүлэлтүүдтэй байна.

Мөн тусгай зөвшөөрлийн жил бүр авдаг төлбөрөөс гадна анх тухайн зөвшөөрлийг авахтай холбоотой нэг удаагийн төлбөрийг авдаг байна. Энэхүү нэг удаагийн төлбөр нь тухайн радио давтамжийн үнэ цэнийг илтгэх төлбөр байна.

ОУЦХБ-аас гаргасан SM.2012-3 “Радио давтамжийн зурвасын үнэлэмж тогтоох Олон улсын туршлага” [13] зөвлөмжид зааснаар радио давтамжийн төлбөрийг тооцохдоо улсын хэмжээнд нэг жилд спектр менежментийн үйл ажиллагаанд зайлшгүй шаардлагатай зардлын нийлбэр байх ба үүнд нь үндэсний болон гадаад үйл ажиллагааны бүх зардлууд багтсан байдаг байна. Мөн зурвасуудаа үнэлж, хугацаа, газар зүйн хүчин зүйлс, нийгэм эдийн засаг, бизнесийн үнэ цэнийг шингээх, зурвасын нөөцийг тодорхойлох гэх мэт олон хүчин зүйлс буюу параметрээс хамааран төлбөрийг тооцоолдог томьёололтой байна.

Монгол улсын хэмжээнд үүрэн холбооны үйлчилгээнд ашигладаг радио давтамжийн ашиглалтын төлбөр нь анх 2003 онд батлагдсан ба энэхүү төлбөрийн хэмжээнд 2023 онд анх удаа өөрчлөлт орсон байна.

РАДИО ДАВТАМЖИЙН ЗУРВАСЫН ТӨЛБӨРТ ӨӨРЧЛӨЛТ ОРСОН БАЙДАЛ

2-Р ХҮСНЭГТ

Радио давтамжийн зурвас [МГц]	**1 МГц-д оногдох төлбөр [төгрөг]**	
	2003 он	**2023 он**
300 – 3,000	4,250,000	4,000,000
3,000-8,000	820,000	2,000,000
8,000-24,000	820,000	800,000
24,000-30,000	820,000	500,000
30,000 дээш	520,000	500,000

Олон Улсад радио давтамж ашиглалттай холбоотой төлбөрийг тооцох нэгдсэн аргачлалыг мөрддөггүй улс орон бүр өөрийн улсын онцлог, газар зүйн байршил, эдийн засаг гэх мэт хүчин зүйлүүдэд үндэслэн төлбөрөө тооцоолдог.

V. 5G ТЕХНОЛОГИД АШИГЛАХ РАДИО ДАВТАМЖИЙН АШИГЛАЛТЫН ТӨЛБӨР ТООЦОХ АРГАЧЛАЛЫГ ШИНЭЧЛЭХ БОЛОМЖИЙН ХАРЬЦУУЛСАН СУДАЛГАА

Үүрэн холбооны 5G технологийг нэвтрүүлэхийн тулд олон улсын туршлага, судалгааны байгууллагаас гаргасан үнэлгээ зөвлөмжид [14] үндэслэн зарим шинэчлэлтийг хийх шаардлагатай байна. Үүний тулд төлбөрийн хэмжээг ирээдүйг харсан, технологийн хувьд төвийг сахисан байхаар, өнөөгийн чиг хандлага, шилдэг туршлагыг харгалзан зөвхөн тодорхой хүчин зүйлсийг өөрчлөх замаар тодорхойлж болно.

Радио спектрийг үр ашигтай ашиглах, өсөлт, хөгжилтийг дэмжих зорилгоор спектрийн эдийн засгийн үнэ цэнийг тусгасан үнийн томъёолол гаргах шаардлагатай болох нь харагдаж байна. Шинэчилсэн төлбөрийн томъёололд дараах зүйлсийг харгалзан үзнэ [15].

a) тогтоосон спектрийн хэмжээ;

b) давтамжийн зурвас ба зурвас доторх ачааллын түвшин;

c) зах зээлийн эрэлт хэрэгцээ;

d) гаралтын чадал, тоо ширхэг;

e) бүс нутгийн хэрэглээний нөхцөл байдал, ашиглалт;

f) бусад хүчин зүйлс орно.

Санал болгож буй загвар нь спектрийг үр ашигтай ашиглах, үндэсний хөгжлийг дэмжих хөшүүрэг бүхий төлбөрийн загварыг хэвээр хадгалсаар байх бөгөөд зардал бууруулах хүчин зүйлээр урамшуулах замаар илүү өндөр давтамжийн зурвасыг ашиглахыг дэмжинэ. Шинэ загвар нь тусгай зөвшөөрөл эзэмшигчдээс ашигласан спектрийн төлбөрийг авч, зөвхөн шаардлагатай спектрийг үр ашигтай ашиглахыг урамшуулдаг ба бүх хэрэглэгчдэд ойлгомжтой, ялангуяа нэг нэгжийн үнийг нэгдмэл үнээр тооцно. Мөн технологи, үйлчилгээний төвийг сахих боломжийг олгодог бүтэцтэй бөгөөд спектрийн хэрэглэгчдэд үйл ажиллагааны зардлаа удирдахын тулд ялгаатай параметрүүд дээр ажиллах боломжийг олгосноор технологи хөгжүүлэхэд зайлшгүй шаардлагатай нэмэлт зардалгүйгээр, спектрийг дахин ашиглах зэрэг санаачилгуудыг хэрэгжүүлэх боломжийг олгоно.

Энэхүү загвар нь хэд хэдэн хүчин зүйлээс дараах байдлаар хамаарна [15].

$$\boldsymbol{Fee} = (\boldsymbol{UNIT} * \boldsymbol{FREQ\_M} * \boldsymbol{BW} * \boldsymbol{HD} * \boldsymbol{SHR} * \boldsymbol{AF}) \quad (2)$$

Энд:

$\boldsymbol{UNIT}$ – Тодорхойлогдсон спектрийн МГц тутамд ноогдох нэгж үнэ

$\boldsymbol{FREQ\_M}$ – Давтамжийн хүчин зүйл нь газар зүйн болон давтамжийн тархалтын онцлогоос хамаарах бөгөөд хуурай газрын хөдөлгөөнт үйлчилгээнд, өндөр давтамжийн үнэлгээ нь нам давтамжаас хямд байдаг.

$\boldsymbol{BW}$ – Зурвасын өргөн (МГц)

$\boldsymbol{HD}$ – Эрэлтээс хамаарсан хүчин зүйл

$\boldsymbol{SHR}$ – Спектрийг хуваалцахад бэлэн байгаа зөвшөөрөл эзэмшигчдэд 50% хүртэл хувийн хөнгөлөлт үзүүлдэг, спектр хуваалцах хүчин зүйл

$\boldsymbol{AF}$ – Хамрах хүрээний коэффициент, км^2-аар тухайн цэгээс хамрагдсан гадаргууг тусгасан талбайн коэффициент.

5.1. НЭГЖИЙН ҮНЭ (UNIT): Нэгжийн үнэ нь харилцаа холбооны үйлчилгээ үзүүлэгчдэд олгож буй 1 МГц-ийн спектртэй дүйцэхүйц утгатай тэнцүү байна. Энэ төлбөрийн хэмжээг Харилцаа холбооны зохицуулах хорооны 2023 оны 94 дүгээр тогтоолын хавсралтаар баталсан.

Олон улсын туршлагаас харахад зарим тохиолдолд 1 МГц спектрийн төлбөрийн шинэ утгыг гурван жилийн хугацаанд жил бүр инфляцийн түвшинг харгалзан өсгөж тооцсон байна. Энэхүү тооцооллоор гурван (3) жилийн мөчлөгийн нэгжийн үнэ дараах байдалтай болохоор байна. Радио давтамжийн 300-3,000 МГц-ийн царааnd:

a. 2023-2024 онд 4,000,000₮

b. 2024-2025 онд 4,040,000₮

c. 2025-2026 онд 4,080,400₮

болох бөгөөд инфляцийг 1%-ийн өсөлттэй гэж үзээд жишээ болгосон онолын тооцоолол болно.

5.2. РАДИО ДАВТАМЖИЙН ХҮЧИН ЗҮЙЛ (FREQ_M): IMT-2020 спектрийн үнэ нь шинэ технологийг хөгжүүлэхэд саад болох биш илүү идэвхжүүлэгч байх ёстой. IMT 2020 нь үр дүнтэй байхын тулд илүү өргөн радио давтамжийн зурвасын өргөнийг шаарддаг бөгөөд одоогийн үнийн тогтолцоонд тулгуурлан 5G технологид ашигласан спектрийн зардлын тооцооллын томьёонд зурвасын өргөний шаардлагыг тусгасан үнийн тохируулга хийнэ. Шинэ хүчин зүйлсийг доорх хүснэгтэд харуулав.

РАДИО ДАВТАМЖИЙН ХҮЧИН ЗҮЙЛИЙН КОЭФФИЦИЕНТ

3-Р ХҮСНЭГТ

Давтамжийн зурвас	Төвийг давтамж	FREQ_M
VLF	3-30 кГц	1.2
LF	30-300 кГц	1
MF	0.3-3 МГц	0.87
HF	3-30 МГц	0.7
VHF	30-300 МГц	0.54
UHF	0.3-1 ГГц	0.38
UHF	1-3 ГГц	0.29
SHF	3-5 ГГц	0.084
SHF	5-30 ГГц	0.042
EHF	30-60 ГГц	0.032
EHF	60 ГГц-ээс дээш	0.01

5.3. ЗУРВАСЫН ӨРГӨН (BW - BANDWIDTH): Тусгай зөвшөөрлөөр олгосон радио давтамжийн зурвасын өргөн (МГц)-өөр илэрхийлэгдэх нийт зурвасын өргөний хэмжээгээр тооцогдоно.

5.4. ЭРЭЛТИЙГ ТОДОРХОЙЛОХ (HD – HIGH DEMAND): Эрэлтээс хамаарсан хүчин зүйлийг дараах байдлаар тодорхойлох боломжтой.

ЭРЭЛТИЙГ ТОДОРХОЙЛОХ КОЭФФИЦИЕНТ

4-Р ХҮСНЭГТ

Эрэлтийн хэмжээ	HD
Өндөр эрэлттэй бол	2
Бага эрэлттэй бол	1

Эрэлтийн хэмжээг Харилцаа холбооны зохицуулах хороо тодорхойлно.

5.5. ХУВААЛЦАХ ХҮЧИН ЗҮЙЛС (SHR - SHARING FACTOR): Спектрийг хуваалцахад бэлэн байгаа зөвшөөрөл эзэмшигчдэд 50% хүртэл хувийн хөнгөлөлт үзүүлдэг, спектр хуваалцах хүчин зүйл. Энэ хүчин зүйлийг хуваалцах зэрэглэлээс хамааруулан дараах байдлаар утга оноох боломжтой.

ХУВААЛЦАХ ХҮЧИН ЗҮЙЛСИЙН КОЭФФИЦИЕНТ

5-Р ХҮСНЭГТ

Хуваалцах зэрэглэл	SHR
Дангаараа эзэмших бол	1
Хуваалцах тохиолдолд	0.5

[15]-д үзүүлснээр спектр хуваалцах гэдэг ойлголт нь хоёр ба түүнээс дээш тусгай зөвшөөрөл эзэмшигчид нэг газарзүйн бүсэд нэг (ерөнхий) давтамжийн хуваарилалтыг хуваалцаж байгаа тохиолдлыг хэлнэ.

5.6. ХАМРАХ ХҮРЭЭНИЙ ХҮЧИН ЗҮЙЛС (AF – AREA FACTOR): Хамрах хүрээний коэффициент, км^2-аар тухайн цэгээс хамрагдсан гадаргууг тусгасан талбайн коэффициент. Дараах хүснэгтэд AF-ийн янз бүрийн утгыг харуулав.

ХАМРАХ ХҮРЭЭНИЙ КОЭФФИЦИЕНТ

6-Р ХҮСНЭГТ

Талбай (м^2)	AF
0-1	0.6
1-10	1.8
10-100	5.6
100-1,000	17.8
1,000-5,000	39.9
5,000-10,000	56.4
10,000-аас дээш	73.6

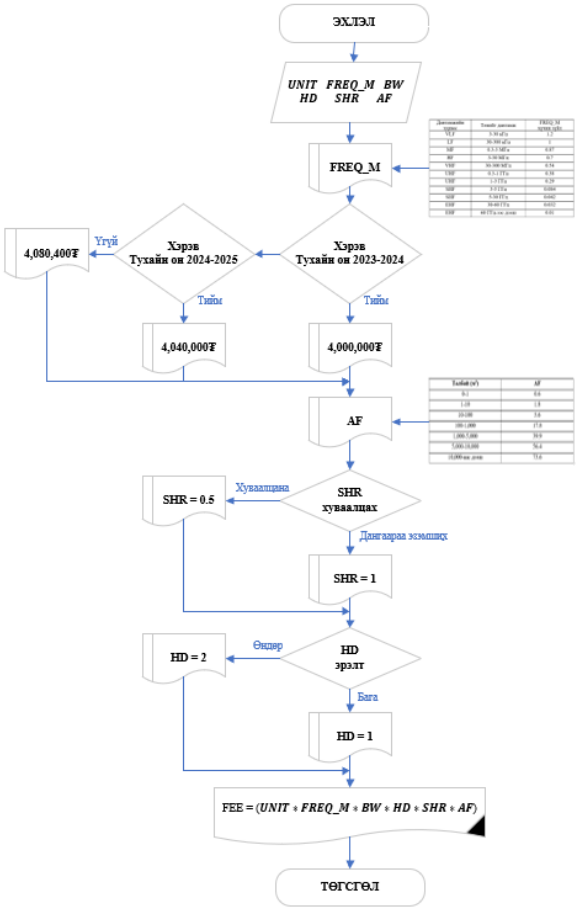
Дээрх хүчин зүйлүүдэд үндэслэн 5G радио давтамжийн төлбөр тогтоох аргачлалын алгоритмыг үзүүлэв.

1-р зураг. 5G радио давтамжийн төлбөр тогтоох алгоритм

VI. ДҮГНЭЛТ

Энэхүү судалгааны үр дүнд спектрийн МГц тутамд ноогдох нэгж үнэ, эзэмшиж буй зурвасын өргөн, эрэлт хэрэгцээ, спектрийг хуваалцах боломж, газар зүйн байрлал буюу хамрах хүрээний онцлог

зэрэг хүчин зүйлүүдийг тооцон 5G радио давтамжийн төлбөр тогтоох алгоритмыг боловсруулж, тооцоолол хийсэн болно.



АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Монгол Улсын “Радио долгионы тухай” хууль, 2023 онд нэмэлт, өөрчлөлт орсон

[2] https://www.itu.int/en/about/Pages/default.aspx .

[3] Монгол Улсын Радио давтамжийн хуваарилалтын дунд хугацааны төлөвлөлт (2018-2023 он).

[4] Module 2 - 5G Technologies5G-Advanced Mobile Broadband Internet and New Services - ITU Centres of Excellence for Europe зохион байгуулсан 2022 оны сургалтын материал.

[5] Харилцаа холбоо, Мэдээллийн технологийн газрын даргын 2020 оны А/45 тушаалаар батлагдсан “Монгол Улсад дараа үеийн хөдөлгөөнт холбооны системийг нэвтрүүлэхэд баримтлах бодлогын чиглэл”, 2022 он.

[6] Цахим хөгжил, харилцаа холбооны сайдын 2023 оны А/42 дугаар тушаалаар батлагдсан “Үндэсний радио давтамжийн хуваарилалтын хүснэгт”, 2022 он.

[7] Харилцаа холбооны зохицуулах хорооны 2023 оны 106 дугаар тогтоолоор батлагдсан “Дараа үеийн хөдөлгөөнт холбооны системд ашиглах радио давтамжийн зурвасын хуваарилалт, техникийн нөхцөл, шаардлага”, 2023 он.

[8] Монгол Улсын “Харилцаа холбооны тухай” хууль, 2023 онд нэмэлт, өөрчлөлт орсон.

[9] Харилцаа холбоо, мэдээллийн технологийн газрын даргын 2017 оны А/42 дугаар тушаалаар батлагдсан “Тусгай зөвшөөрөл эзэмшигчдэд үзүүлэх зохицуулалтын үйлчилгээний хөлсний хэмжээг тогтоох журам”, 2017 он.

[10] Харилцаа холбооны зохицуулах хорооны 2022 оны 61 дугаар тогтоолоор батлагдсан “Зохицуулалтын үйлчилгээний хөлсний хэмжээ”, 2022 он.

[11] Цахим хөгжил, харилцаа холбооны сайдын 2022 оны А/37 дугаар тушаалаар батлагдсан “Радио давтамжийн ашиглалт, үйлчилгээний төлбөр тогтоох журам”, 2022 он.

[12] Харилцаа холбооны зохицуулах хорооны 2023 оны 94 дүгээр тогтоолоор батлагдсан “Радио давтамж ашиглалт, үйлчилгээний төлбөрийн хэмжээ”, 2023 он.

[13] ОУЦХБ-аас гаргасан SM.2012-3 “Радио давтамжийн зурвасын үнэлэмж тогтоох Олон улсын туршлага” 2018 он.

[14] GTTO судалгааны байгууллагаас гаргасан “5G үйлчилгээний радио давтамжийн эрхийн төлбөр, ашиглалт үйлчилгээний төлбөр тооцох аргачлал боловсруулах” 2021 он.

[15] Eswatini Communications Commission, “Spectrum Pricing Model 2021: Explanatory Memorandum,” Spectrum Fee Schedule 2021 Consultation Document, 2021 он.

ТЕСТИЙН АВТОМАТЖУУЛАЛТ БА ХЭРЭГСЛИЙН СОНГОЛТ

[1]Б.Хулан, [2]Г.Ганчимэг

[1,2]Компьютерын ухаан салбар, Мэдээлэл, Холбооны Технологийн Сургууль, ШУТИС, Монгол улс

[1]khulanka.ba@gmail.com, [2]ganaa@must.edu.mn

***Хураангуй*— Технологи асар их хурдаар хөгжихийн хэрээр программ хангамж хөгжүүлэгчид өрсөлдөх чадвартай байхын тулд салбарын чиг хандлага, сорилтуудыг дагаж мөрдөж байх шаардлагатай байна. Программын бүтээмж, үр ашгийг нэмэгдүүлэхийн тулд байгууллагууд программ хангамжийн хөгжлийн чиг хандлагыг дагахаас гадна энэ тал дээрээ илүү төвлөрдөг болсон. Үүний нэг тод жишээ бол тестийн автоматжуулалт юм. Энэхүү өгүүлэлд тестийн автоматжуулалт болон тестийн автоматжуулалтын хэрэгслийг хэрхэн сонгох талаар өгүүлнэ.**

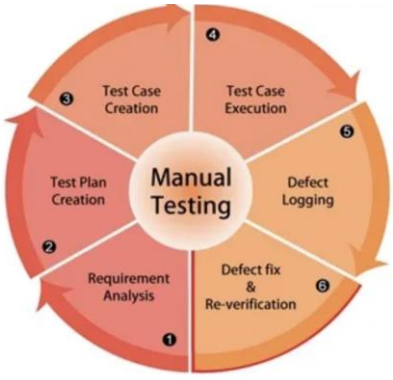
Түлхүүр үг— Тест, автоматжуулалт, туршилт, тестер

I. Удиртгал

Программыг тестлэхдээ гар аргаар эсвэл автомат гэсэн хоёр аргаар тестлэдэг. Гар аргаар тестлэх гэдэг нь программын ажиллагааг хүн шалгах үйл явцыг хэлнэ. Үүнийг хийхийн тулд тестерүүд программ руу орж, хэрэглэгчийн хийдэг үйлдлүүдийг хийнэ. Тестерүүд мөн өөрсдийн үр дүнг бүртгэх шаардлагатай. Үүнд лог файлууд, гадаад үйлчилгээнүүд, мэдээллийн сангуудад алдаа байгаа эсэхийг шалгах шаардлагатай. Программ хангамжийг гар аргаар тестлэхэд ихээхэн цаг хугацаа, хүчин чармайлт шаарддаг [1-2]. *Үүнд:*

- Шаардлага, шинжилгээ
- Туршилтын төлөвлөгөө
- Турших кейс үүсгэх
- Туршилтын гүйцэтгэл
- Алдаа бүртгэх
- Алдаа засах, дахин баталгаажуулах

Гараар тестлэх журмын дарааллыг 1 дүгээр зурагт үзүүлэв.

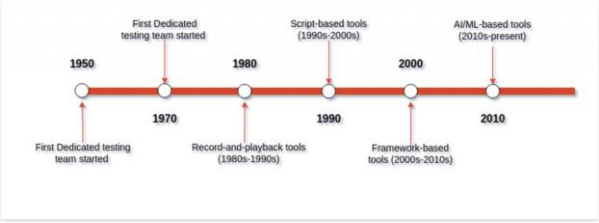


Зураг 1. Гараар тестлэх журам [7]

Автоматжуулсан тест гэдэг нь урьдчилан тодорхойлсон үйлдлүүдийг давтах замаар тестийн тохиолдлуудыг гүйцэтгэхийн тулд багаж хэрэгсэл, скрипт, программ хангамжийг ашиглах үйл явцыг хэлнэ. Энэ нь том хэмжээтэй эсвэл туршилтыг олон удаа давтах шаардлагатай төслүүдэд тохиромжтой. Автоматжуулалтыг ашигласнаар тестерүүд өндөр үнэ цэнтэй ажлуудад илүү их цаг зарцуулж чадна. Хэдийгээр энэ нь тестерүүдээс тестийн скриптүүдийг хадгалахыг шаарддаг ч программын чанар, тестийн хамрах хүрээ, өргөтгөх чадварыг нэмэгдүүлэхэд тусална [1-2]. Байгууллага автоматжуулсан тестийн тусламжтайгаар программын туршилтыг илүү хурдан хийх боломжтой [3].

II. Тестийн автоматжуулалтын үе шат

Тестийн автоматжуулалт шинэ зүйл биш тооцооллын эхэн үеэс энэ ойлголт эхэлж байсан хэдий ч 1970 оны үед анхны практик хэрэгжиж эхэлсэн түүхтэй [4]. Анхны автоматжуулсан тестийн жишээнүүдийн нэг бол IBM боловсруулсан Automated Test Engineer (ATE) систем юм. Үндсэн фреймийн программ хангамжийн хэрэглээний туршилтыг автоматжуулах зорилготой ATE систем нь томоохон нээлт болж, ирээдүйн тестийн автоматжуулалтын системд жишиг болсон юм [4-5].



Зураг 2. Тестийн автоматжуулалтын түүх [4]

Тестийн автоматжуулалтыг дараах дөрвөн үед хувааж болно [5]. Үүнд:

- **Бичлэг болон тоглуулах хэрэгслүүд (1980-1990)**: Эдгээр хэрэгслүүд нь тестерүүдэд программ хангамжийн хэрэглүүртэй харилцан үйлчлэлийг бүртгэж, дараа нь тэдгээр харилцан үйлдлийг скрипт болгон дахин тоглуулах боломжийг олгосон. Скриптүүдийг дахин дахин

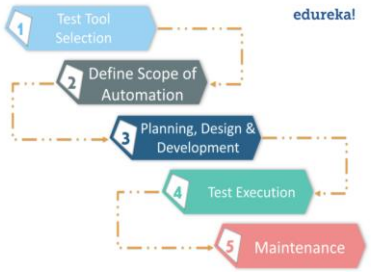
ажиллуулж болох бөгөөд энэ нь давтагдах тестийн даалгаврууд ыг автоматжуулах боломжтой болсон.

- **Скрипт дээр суурилсан хэрэгслүүд (1990-2000)**: Эдгээр хэрэгслүүд нь тестийн даалгаврууд ыг автоматжуулахын тулд программчлалын хэлээр скрипт бичих боломжийг тестерүүдэд олгож, илүү уян хатан байдал, хяналтыг бий болгосон.
- **Framework дээр суурилсан хэрэгслүүд (2000-2010)**: Эдгээр хэрэгслүүд нь тестийн автоматжуулалтын скриптүүдийг бүтээх, удирдахад зориулсан номын сан, функц, арга зүйг багтаасан тестийн цогц тогтолцоог бүрдүүлж өгсөн.
- **AI/ML дээр суурилсан хэрэгслүүд (2010 оноос өнөөг хүртэл)**: Хиймэл оюун ухаанд суурилсан тестийн хэрэгслүүд нь машин сургалтын алгоритмуудыг ашигладаг. AI дээр суурилсан тестийн хэрэгслүүд нь программ эсвэл орчны өөрчлөлтийг тодорхойлж, дасан зохицож, илүү тогтвортой, найдвартай болгодог. Нэмж дурдахад эдгээр хэрэгслүүд нь техникийн туршлага бага эсвэл огт шаарддаггүй ба энэ нь техникийн бус оролцогч талуудын туршилтын хүчин чармайлтад хувь нэмрээ оруулах боломжийг олгож, туршилтын үйл явцыг бүхэлд нь илүү үр дүнтэй болгодог.

Тестийн автоматжуулалт яагаад чухал вэ? гэдэг асуултын хувьд тестийн *автомжуулалт нь яагаад чухал болохыг дараах зүйлсүүдээр тайлбарлаж болно [8]. Үүнд:*

- **Сайжруулсан үр ашиг**: Тестийн автоматжуулалт нь нэгэн хэвийн даалгаврууд ыг автоматжуулж, QA шалгагчдыг ээдрээтэй, чухал сорилтод анхаарлаа төвлөрүүлэх замаар асар их цаг хугацаа, хүчин чармайлтыг хэмнэдэг.
- **Чанарын баталгаа**: Программ хангамжийн инженерчлэл дэх туршилтын автоматжуулалт нь асуудал, согогийн талаар үнэн зөв, хурдан санал хүсэлт өгөх замаар программ хангамжийн бүтээгдэхүүн нь чанарын чухал стандартад нийцэж байгаа эсэхийг баталгаажуулахад тусалж, тестийн автоматжуулалтын хөгжүүлэлтийн багуудад тэдгээрийг үр дүнтэй, хурдан шийдвэрлэх боломжийг олгодог.
- **Сайжруулсан өргөтгөх чадвар**: Тестүүдээ автоматжуулах нь таны тестийн QA багийн ажиллах цар хүрээг өөрчилдөг тул компьютерууд өдөрт 24 цагийн турш тест хийх боломжтой. Энэ нь танд ижил төстэй нөөцтэй олон тест хийх боломжийг олгоно.
- **Тестийн хамрах хүрээг нэмэгдүүлсэн**: Автоматжуулсан туршилтууд нь олон туршилтын тохиолдлыг хурдан бөгөөд үнэн зөв гүйцэтгэх боломжтой бөгөөд QA шалгагчдад гараар шалгахад хэцүү байж болох өргөн хүрээний хувилбарууд болон захын тохиолдлуудыг хамрах боломжийг олгодог.
- **Зах зээлд хүргэх хугацааг багасгасан**: Тестийг автоматжуулснаар хөгжүүлэлтийн багууд зах зээлд гаргах/хувилбарын мөчлөгөө хурдасгаж, дээд зэргийн чанартай бүтээгдэхүүнийг зах зээлд хурдан хүргэх боломжтой.
- **Тогтвортой байдал ба өртөг хэмнэлттэй**: Автоматжуулсан туршилтыг нэг удаад ижил аргаар хийж, тууштай байдлыг баталгаажуулдаг. Энэ нь программ хангамжийн бүтээгдэхүүнийг турших ашигтай арга байж болох бөгөөд энэ нь туршилтын том багийг ажиллуулахтай холбоотой зардлыг бууруулдаг.

Автоматжуулсан тест яаж ажилладаг вэ? гэдэг асуултын хувьд автоматжуулсан тестийг амжилтанд хүргэхийн тулд нарийн төлөвлөлт, дизайны ажлыг шаарддаг [1].



Зураг 3. Автоматжуулсан тестийн ажиллах алхамууд[1]

Автоматжуулалтын үйл явц нь ерөнхийдөө дараах алхмуудыг дагаж мөрддөг [1-3]. Үүнд:

- **Туршилтын хэрэгслийн сонгох**: Энэ нь хийгдэж буй тестийн төрлөөс болон тухайн хэрэгсэл нь программ хангамжийг боловсруулж байгаа платформыг дэмжиж байгаа эсэхээс хамаарна.
- **Автоматжуулалтын хамрах хүрээг тодорхойлох**: Энэ нь программ хангамжийн тестийн хэр ихийг автоматжуулсан гэсэн үг юм.
- **Төлөвлөж, зохиож, хөгжүүл**: Энэ алхамд автоматжуулалтын стратегийг төлөвлөх, туршилтын скрипт боловсруулах зэрэг орно.
- **Тестийг гүйлцэтгэх**: Программ хангамжийг автоматжуулалтын скрипт ашиглан шалгадаг. Тестийн хэрэгсэл нь өгөгдөл цуглуулж, нарийвчилсан туршилтын тайланг өгнө.
- **Засвар үйлчилгээ**: Автомат тестийн скриптүүдийг шаардлагатай бол программ хангамжийн шинэ хувилбараар өөрчилж шинэчилдэг.

III. Автоматжуулсан тестийн хэрэгслүүд

Тестийн төрөл болон хэрэгжүүлэх гэж буй хүрээний төрлөөс хамааран автоматжуулалтын хэрэгслийг сонгох хэрэгтэй. Зах зээл дээр та өөрийн шаардлагад нийцүүлэн сонгох боломжтой маш олон хэрэгсэл байдаг [13]. Тестийн автоматжуулалтын хэрэгсэл нь үнэтэй байж болох бөгөөд ихэвчлэн гар аргаар турших туршилттай хослуулан ашиглагддаг [12]. Программ хангамжийн тестийн автоматжуулалтын хэрэгслийг сонгохдоо дараах гол хүчин зүйлүүдийг анхаардаг. *Үүнд:*

Программ хангамжийг шалгах зөв хэрэгслийг сонгох нь янз бүрийн хүчин зүйлээс хамаарна. Туршилтын үе шат бүр эхний шатанд өвөрмөц бөгөөд төсөл хэрэгжих тусам цоо шинэ болж хувирах боломжтой. Түүнчлэн танд төслийн хэрэгцээ шаардлагад нийцсэн найдвартай туршилтын хэрэгсэл хэрэгтэй. Боломжтой янз бүрийн хэрэгслийг үнэлэхэд цаг хугацаа шаардагдах боловч туршилтын үе шат болон төслийн нийт амжилт нь зохих туршилтын хэрэгслээс хамаардаг [14].

Сонгосон хэрэгсэл нь таны төслийн хэрэгцээг хангасан байх ёстой бөгөөд туршилт хийхэд цаг хугацаа, мөнгөө хэмнэх болно [1-3].

Төсөлд тавигдах шаардлагын эхний алхам бол туршилтын хэрэглүүрийг ашиглан шийдвэрлэхээр төлөвлөж буй төслийн шаардлага, асуудлуудыг жагсаах явдал юм. Тухайн төслийн хэрэгцээний талаар ойлголт авахын тулд та дараах ерөнхий асуултуудыг асууж болно. *Үүнд:*

- *Программын хэл:* Хэрэв та туршилтын автоматжуулалтад тусгай программчлалын хэл ашиглахаар төлөвлөж байгаа бол энэ тал нь маш чухал юм.
- *Туршилт хийх шаардлагатай программын төрөл*: Та ширээний компьютер, API, гар утас эсвэл вэб программ дээр ажиллаж байгаа эсэх.
- *Танд төхөөрөмж хоорондын тест эсвэл хөтөч хоорондын туршилт хэрэгтэй юу?* Хэрэв та гар утас эсвэл вэб программ дээр ажиллаж байгаа бол танд энэ шалгалт хэрэгтэй болно.
- *Туршилт хийх шаардлагатай платформууд*: Хэрэв та вэб программтай ажиллаж байгаа бол дэмжигдсэн хөтчүүдийг тэмдэглэж авна. Мөн энэ нь гар утасны программ бол тохирох гар утасны үйлдлийн системийг жагсааж, ширээний программын хувьд ижил зүйлийг хийнэ.

Багийн ур чадвар, түвшинг тодорхойлох: Туршилтын автоматжуулалтын хэрэгслийг хоёр төрлөөр авах боломжтой ба зарим нь кодлохыг шаарддаг боловч зарим нь кодгүй байдаг. Тиймээс программ хангамжийн туршилтын автоматжуулалтын хэрэгслийг сонгохдоо багийнхаа ур чадвар, туршлагын түвшинг харгалзан үзэх нь чухал юм. Зарим хэрэгсэл нь нэмэлт сургалт эсвэл туршлага шаарддаг бол бусад нь танай баг энэ чиглэлээр анхан шатны мэдлэгтэй бол сурахад хялбар байж болно. Нэмж дурдахад, ямар нэгэн шийдвэр гаргахын өмнө сонгосон хэрэгсэл нь танай багт байгаа зүйлээс гадна нэмэлт техникийн туршлага шаарддаггүй эсэхийг шалгана.

Төсөв: Аль хэрэгсэл нь танд хамгийн сайн тохирохыг шийдэхээсээ өмнө хэр их мөнгө зарцуулах хүсэлтэй байгаагаа ойлгох нь чухал юм. Төсвөө тодорхойлохын өмнө дараах зүйлийг анхаарах хэрэгтэй. *Үүнд:*

- Танай баг уг хэрэгслийг сурахад зарцуулах цаг
- Автоматжуулалтад зарцуулсан цаг
- Автоматжуулалтад шаардагдах хүний нөөцийн зардал

Засвар үйлчилгээ болон тестийн кейс үүсгэхэд хялбар байх: Туршилтын тохиолдол үүсгэх нь цаг хугацаа их шаарддаг. Тиймээс сонгосон программ хангамж нь скрипт бичихэд хялбар, хурдан болгодог хэрэглэгчдэд ээлтэй интерфэйс эсвэл бага кодын шаардлага зэрэг хэрэглэхэд хялбар функцуудыг санал болгодог. Энэ нь танд зардлыг багасгах замаар үнэ цэнтэй хөгжүүлэлтийн цагийг хэмнэх болно.

Дахин ашиглах боломжтой байх: Дахин ашиглах чадвар нь таны төслийн хамгийн сайн сонголтыг сонгоход анхаарах чухал хүчин зүйл юм. Энэ нь танай багт нэг орчинд үүсгэсэн скрипт болон тестийг өөр орчинд дахин ашиглах боломжийг олгож, ямар нэг шинэ зүйл туршиж үзэх бүрд гараар тохируулах шаардлагагүй болно.

Өгөгдөлд тулгуурласан тест хийх чадвар: Өгөгдөлд суурилсан тест нь таны туршилтын багт нэг өгөгдлийн багц дээр олон тест хийх боломжийг олгодог. Тэд хамгийн бага хүчин чармайлтаар программ эсвэл системийн үнэн зөв, найдвартай байдлыг хялбархан шалгаж чадна. Өгөгдөлд тулгуурласан тестийн тусламжтайгаар скриптүүд нь туршилтын тохиолдол бүрийг өөр өөр өгөгдлийн багцаар автоматаар гүйцэтгэдэг. Туршилтын алхам бүрдээ тодорхой зорилт тавьж, хэмжигдэхүйц чухал үр дүнтэй байх тул та алхам бүрд ахиц дэвшлийг хянах боломжтой.

Хамтын ажиллагааны дэмжлэг: Сонгосон хэрэгсэл нь туршилтыг амжилттай байлгахын тулд өөр өөр байршлаас хэлтсийн багууд хамтран ажиллаж, хурдан бөгөөд үр дүнтэй харилцах боломжийг олгодог функцуудыг агуулсан байх ёстой.

Интеграцийн дэмжлэг: Интеграцийн дэмжлэг нь туршилтын мөчлөгт оролцдог олон хэрэгсэл бүхий томоохон төслүүдэд чухал үүрэг гүйцэтгэдэг.

24/7 дэмжлэг, сургалт: Сонгосон хэрэгсэл нь сургалтын иж бүрэн нөөцөөр хангагдсан байх ёстой бөгөөд ингэснээр танай баг ашиглалтын заавартай хурдан танилцах боломжтой болно.

Дүгнэлт

Энэхүү өгүүлэлд программыг тестлэх аргууд, автоматжуулалтын хөгжлийн үе шатуудыг болон хэрэгслүүдийн талаар танилцуулсан. Хэрэгслийг сонгох арга зүй болон үндсэн шаардлага нь тухайн тестлэх төслийн төрлөөс хамаарна. Түүнчлэн программ хангамжийн туршилтыг автоматжуулах нь таны төслийн үр ашгийг дээшлүүлэх маш сайн арга юм. Бидний шаардлагыг хангахын тулд зөв хэрэгслийг сонгох нь хамгийн чухал байдаг. Техникийн онцлогоос гадна туршилтын баг тань ямар нэгэн бэрхшээл тулгарвал 24/7 дэмжлэг авах боломжтой эсэх нь хамгийн чухал юм. Таны сонгосон тестийн хэрэгсэл таны туршилтын үр ашгийг дээшлүүлж, хамгийн өндөр чанартай бүтээгдэхүүнийг түргэн шуурхай хүргэх багийг тань хүчирхэгжүүлж байдаг. Иймд тестийн автоматжуулалтыг зөв найдвартай хэрэгжүүлэх нь чухал юм.

Ном зүй

[1] https://www.edureka.co/blog/what-is-automation-testing/#differences

[2] https://smartbear.com/learn/automated-testing/what-is-automated-testing/

[3] https://www.techtarget.com/searchsoftwarequality/definition/automated-software-testing#:~:text=Automated%20testing%20is%20a%20software,faster%20pace%20without%20human%20testers.

[4] https://www.globalapptesting.com/blog/what-is-automation-testing

[5] https://www.linkedin.com/pulse/20141007123253-16089094-a-very-brief-history-of-test-automation

[6] https://testrigor.com/blog/the-history-of-test-automation/

[7] https://medium.com/oceanize-geeks/manual-testing-process-340173d40141

[8] https://www.browserstack.com/guide/what-is-test-automation#:~:text=Test%20automation%20can%20be%20used,cost%20and%20time%20of%20testing.

[9] Ingibjorg Birna Kjartansdottir, etc, Building Information Modelling Bim, 2017, Iceland Great Britain

[10] Little book OF BIM, 2020, https://www.bsigroup.com/globalassets/localfiles/en-us/brochures/bim/little-book-bim.pdf

[11] Yusuf Arayici, Building Information Modeling, 2015

[12] https://en.wikipedia.org/wiki/Test_automation

[13] https://intellipaat.com/blog/what-is-automation-testing/

[14] https://www.freepdfbook.com/building-information-modeling/

[15] https://www.stress-free.co.nz/bimserver_and_the_potential_of_serverside_bim

МАШИН СУРГАЛТЫН DNN+ResNET ХОСОЛСОН АЛГОРИТМ АШИГЛАН ӨВЧНИЙГ АНГИЛАХ НЬ

Тэгшээгийн Түвшинсайхан[1], Хишигбаярын Ариунзаяа[2], Нямаагийн Дуламсүрэн[3], Батжаргалын Долгорсүрэн[4]
[1]ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Компьютерийн ухааны салбар
[2,3,4]ШУТИС, Мэдээлэл холбооны технологийн сургууль, Мэдээллийн технологийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг: b.dolgorsuren@must.edu.mn[4]

Хураангуй: **Бэтэг өвчин нь удаан явцтай эмнэлзүй шинж тэмдэг тод илэрдэггүй учраас өвчтөнгүүд цаг хугацаа алддаг бөгөөд тэднийг үнэн зөв оношлох эмчилэхэд бэрхшээлтэй байдаг. Энэ асуудлыг шийдвэрлэхэд туслах зорилготойгоор шинэ үеийн технологи хиймэл оюун, машин сургалт ашигласан систем бий болгох, хэрэглээнд нэвтрүүлэх зайлшгүй шаардлагатай гэж үзэж байна. Дэлхийн эрүүл мэндийн байгуулгаас бэтгийн үе шатуудыг ерөнхийд нь таван ангилалд хамааруулдаг бөгөөд бэтэг өвчний төрлийг зөв таних, өвчний үе шатыг тодорхойлох нь өвчтөнд хамгийн тохиромжтой эмчилгээг үзүүлэх анхны бөгөөд чухал үе шат юм. Энэхүү судалгааны ажлаар машин сургалтын ML.NET технологийг ашиглан уйланхайт эхинококкозын төрлийг ангилан ялгах алгоритм боловсруулах, хэрэгжүүлэх, программын үр дүнг танилцуулахыг зорилоо. Мөн цаашлаад уйланхайн буруу ангилалын танилтын хувийг ихэсгэхийн тулд өгөгдөл болон машин сургалтын арга алгоритмуудаа хэрхэн өргөтгөх боломжийг судалсан.**

Түлхүүр үг: ***зураг боловсруулалт, машин сургалт, бэтэг, бэтгийн ангилал***

I. УДИРТГАЛ

Бэтэг өвчин нь амьтнаас хүнд халдварладаг цестодозын бүлэгт хамааран туузан хорхойгоор үүсгэгдэж элэг, уушиг гэх мэт бусад эрхтэнд шимэгчлэн уйланхай үүсгэдэг зоонозын төрлийн халдварт өвчин юм. Энэ үүсгэгчийн 5 төрөл байдгаас Echinococcus granulosus ба Echinococcus multilocularis гэсэн хоёр зүйлийн шимэгч нь түгээмэл байдаг. Энэ хоёр нь хоорондоо ялгаатай бэтгийн төрөл үүсгэдэг. Үүнд cystic echinococcus (CE) буюу уйланхайт эхинококкоз, alveolar echinococcus (AE) буюу цулцангийн эхинококкозууд багтана. Эхинококкоз нь шинэ болон дахин сэргэж буй "Анзаарагддаггүй" зоонозын өвчин юм. Судалгаагаар [1] Төв Азийн 270 сая хүн cystic echinococcosis (CE)-ийн эрсдэлтэй бүсэд амьдардаг.

Гидатид уйланхай үүсэхэд хүргэдэг шимэгчийн халдвар болох эхинококк гранулосус нь дэлхий дахин даяар нийгмийн эрүүл мэндийн асуудалд ихээхэн анхаарал хандуулж байна. Энэ хор хөнөөлтэй өвчин нь янз бүрийн хөхтөн амьтдад нөлөөлж болох ба мөн нохой болон бусад махчин амьтдын ялгадсаар бохирдсон хоол хүнс, усыг хүн хэрэглэх залгих замаар голчлон халдварладаг. Нэг эст шимэгчээр үүсгэгдсэн гидатид уулинхай нь ихэвчлэн удаан хугацааны туршид илрэх шинж тэмдэггүй байдаг бөгөөд хүний дотор чимээгүйхэн ургадаг. Гэсэн хэдий ч эдгээр уулинхай нь томрох тусам хүрээлэн буй эд эс, эрхтэн тогтолцоондоо дарамт учруулж өвчтөний амьдралын чанарт ихээхэн нөлөөлдөг. Бүр илүү аймшигтай нь эдгээр уулинхай хагарвал эрүүл мэндийн ноцтой хүндрэлүүд гарч болзошгүй.

Гидатидын уулинхайг оношлох үйл явц нь ихэвчлэн рентген туяа, хэт авиан гэх мэт эмнэлгийн дүрслэлийн аргуудыг ашигладаг. Харин ангилалын хувьд манай Монгол улс нь гараар ангилдаг. Эдгээр уйланхайг үнэн зөв хурдан шуурхай ангилах нь өвчтөндөө тохирох эмчилгээг цаг тухайд нь баталгаажуулж хүндрэлийн эрсдэлийг бууруулахад чухал ач холбогдолтой юм. Энэхүү судалгааны гол зорилго нь хэт авиан дүрсийг ашиглан уйланхайт эхинококкозыг (active, inactive, transition) гэсэн гурван ангилалд ангилахын тулд машин сургалтын арга алгоритм ашиглах явдал юм. Зорилгодоо хүрэхийн тулд бид ML.Net Model builder-ийг ашиглаж байгаа бөгөөд зураг дээр суурилсан ангилалын ажилд гүн сургалтын нейрон сүлжээний (DNN) алгоритм ашиглаж системийн кодыг C# хэл дээр бичлээ. Энэхүү алгоритм нь зургуудаас нарийн төвөгтэй хэв маягийг өөрөө сурах чадвартай учир дүн шинжилгээ хийх ангилахад нэн тохиромжтой загвар юм. Гидатидын уйланхай оношилгоог сайжруулах, нарийвчлал ангилах, ангилалын танилтын үр дүнгийн хувийг нэмэгдүүлэх зэрэг ажилууд цааш цаашид алгоритм, загвараа сайжруулах боломжтой бөгөөд энэхүү ажил Монголд хийгдэж буй нь уг төрлийн судалгааны анхдагч оролдлого юм.

II. ОНОЛЫН ХЭСЭГАШИГЛАХАД ХЯЛБАР

A. Бэтгийн ангилал

CE-ийн анхдагч оношийг ийлдэс судлалын шинжилгээ (serology)-гээр, эсвэл хэт авиан шинжилгээ ашиглан илрүүлэх боломжтой байдаг. Хэт авиан шинжилгээгээр (ЭХО) жижиг хэмжээст уйланхайн илрэхгүй байж болно. Харин дараагийн үе шат буюу нарийвчлан бэтгийн үе шатыг нь илрүүлэхдээ дүрс оношилгооны зургийг мэргэжлийн эмч нар уншиж Gharbi болон ДЭМБ ангилалын дагуу тодорхойлно. Анх 1981 онд эрдэмтэн Gharbi [2] хэт авиан шинжилгээн дээр үндэслэн элэгний уйланхайг ангилах шалгуурыг (Хүснэгт 1-ээс харна уу.) боловсруулсан ба 2001 онд Дэлхийн эрүүл мэндийн байгуулгаас (WHO-IWGE) үүнийг илүү сайжруулж Хүснэгт 2-т үзүүлсэнчлэн WHO-IWGE [3]

стандарчлагдсан ангилалыг үүсгэсэн. ДЭМБ гарал үүсэл нь тодорхойгүй уйланхайг хэв шинжээр нь үндсэн 3 хэлбэрийн уйланхай болгоод тэдгээрийг мөн үе шатаар таван дэд төрөлд оруулсан.

Хүснэгт 1. Гидатидын уйланхайн Gharbi ангилал

Type	Characteristics
I	Unilocular cyst, wall and internal echogonicities
II	Cyst with detached membrane (water-lily sign)
III	Multivesicular, multiseptated cyst, daughter cyst (honeycomb pattern)
IV	Hererogeneous cyst, no daughter vesicules
V	Cyst with partially or completely calcified wall

Уйланхай нь “идэвхтэй, идэвхгүй, шилжилтийн” гэсэн гурван төрлийн ангилал байна. CE1 ба CE2-р хэлбэрийн уйланхайг “идэвхтэй” хэлбэрийн уйланхай гэж үздэг бол CE3 хэлбэрийн уйланхайг “шилжилтийн” гэж үздэг. Харин CE4-CE5-р хэлбэрийн уйланхайг “идэвхгүй” хэлбэрийн уйланхай гэж тус тус ангилдаг.

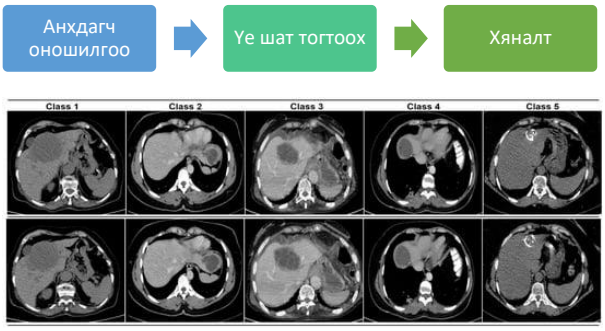
Хүснэгт 2. ДЭЛХИЙН ЭРҮҮЛ МЭНДИЙН БАЙГУУЛГЫН ГИДАТИК УЙЛАНХАЙН АНГИЛАЛ

WHO stage	Characteristics	Activity
CE1	Uniloculer, anechoic cyst with double line sign	Active
CE2	Multiseptated “rosette-like” “honeycomb patern” cyst	Active
CE3a	Cyst with detached membrane (water-lily sign)	Transitional
CE3b	Daughter cysts in solid matrix	Transitional
CE4	Hererogeneous cyst, no daughter vesicules	Inactive
CE5	Solid matrix with calcified wall	Inactive

Шилжилтийн гэж тооцогдож байсан 3-р хэлбэрийн уйланхайг цаашид хоёр дэд бүлэгт хуваадаг болсон. CE3a (тусгаарлагдсан эндокистууд) харин CE3b (цэвэр цэврүү агуулсан) гэж ангилах болсон. Харин зарим судалгаагаар [4] CE3a цист идэвхгүй бол CE3b цист идэвхтэй байна гэж гаргажээ. Мөн хэт авиан шинжилгээг гэмтэлийг хянах зорилгоор ашиглаж болно. Эмчилгээ хийсэн өвчитнүүдийн хувьд 3-6 сар тутамд хяналтын үзэлгээ хийлгэж дараа нь жил бүр үзлэг хийлгэх хэргтэй гэж үзэж байна. Тэгвэл бид энэхүү хоёр ангилалын аргаас сүүлд гаргасан ДЭМБ-аас гаргасан ангилалын дагуу бэтгийг хэт авиан зурган мэдээллээс ангилахыг зорьсон юм.

B. Зургаас ангилах арга

Зарим нэг тохиолдолд хэт авиан шинжилгээгээр тодорхой тогтсон онош тавих боломжгүй байдаг тул соронзон резонансын дүрслэл (MRI) болон компьютерийн томографи (CT) шаардлагатай байж болно. Үүнд таргалалттай өвчтөнүүд, диафрагмын доорх уйланхай эсвэл уйланхайн хоёрдогч халдвартай өвчтөнүүд, цөсний фистул зэрэг хүндрэлтэй тохиолдлууд болон хэвлийн хөндийн гадуур тархсан тохиолдлууд гэх мэт нийтлэг өвчнөөр өвчилсөн өвчтөнүүд орно. Дүрс оношлогооны CT ба MRI нь мэс заслын өмнөх болон дараагийн үзлэгт онцгой ач холбогдолтой юм. Оношлогоо, хяналтын шинжилгээнд MRI ашиглах нь CT-ээс илүү үр дүн сайн.



Зураг 1. Дүрс оношилгооны зураг

Энэ хоёр арга нь хоёулаа биеийн эмгэгийг дүрслэн харуулдаг боловч MRI нь зөөлөн эдүүдийн төлөв байдлын талаар, CT нь яс болон бусад хатуу эдүүдийн эрүүл мэндийг үнэлэхэд илүү их ашиглагддаг. Компьютерийн томографид рентген туяа нь зөөлөн эдийг нэвтэрч, нягт бүтэцэд ойдог. Тиймээс өндөр мэдээлэл сайтай, нарийвчлал сайтай 3D давхаргат зургийг бүтээдэг. Гэхдээ уг зургуудыг мэргэжлийн эмч нар л тайлж тайлбарлаж бэтгийг үе шат явц хэр байгааг хэлж өгдөг. Гэтэл уг өвчин маань ховор тохиолдох үл анзаарагдам өвчин тул нарийн мэргэшсэн эмч цөөн байдаг. Тэгэхээр дараагийн бүлэгт яригдах шинэ технологиудыг ашиглан MRI болон CT зурагнаас өндөр нарийвчлалтай бэтгийн уйланхай үе шат тогтоох, өвчний хяналтыг хийх чадамжтай оюун ухаант систем бий болгох хэрэгтэй байна.

C. ML.NET ба DNN+RESNET50

Microsoft-ын боловсруулсан ML.NET нь нээлттэй эх сурвалжтай, платформ хоорондын машин сургалтын систем юм. Энэ нь хөгжүүлэгчдэд машин сургалтын өмнөх туршлага шаардахгүйгээр C# эсвэл F# ашиглан машин сургалтын загвар бүтээх боломжийг олгодог. Мөн ML.NET нь .NET хөгжүүлэгчдэд зориулсан машин сурахад туслах зорилготой бөгөөд вэб, ширээний компьютер, гар утас, клоуд, IoT программ зэрэг төрөл бүрийн домайнуудад хэрэглэгдэх боломжтой. ML.NET-ийн гол онцлог, шинж чанаруудыг доор харуулав.

ML.NET нь .NET экосистемтэй саадгүй нэгдэж, C# хөгжүүлэгчдэд машин сургалтыг программдаа оруулахад хялбар болгодог. Үүнийг ASP.NET, Xamarin, Azure, Visual Studio гэх мэт сангууд болон хэрэгслүүдтэй хамт ашиглаж болно. ML.NET нь нээлттэй эх сурвалж бөгөөд энэ нь түүний эх кодыг хөгжүүлэгчид үзэх, өөрчлөх, хувь нэмэр оруулах боломжтой гэсэн үг юм. Энэхүү нээлттэй хандлага нь олон нийтийн оролцоог дэмжиж, шинэ онцлог,

сайжруулалтыг хөгжүүлэхэд түлхэц өгдөг. ML.NET нь хөндлөн платформ бөгөөд үүнийг Windows, macOS болон Linux дээр ажиллуулах боломжийг олгодог. Энэхүү олон талт байдал нь өөр өөр үйлдлийн системүүд дээр машин сургалтын програмуудыг хөгжүүлэхэд тохиромжтой болгодог.
ML.NET нь өгөгдлийг хувиргаж, машин сурахад бэлтгэх боломжийг олгодог. Та өгөгдлийн сан, CSV файл эсвэл API зэрэг янз бүрийн эх сурвалжаас өгөгдлийг импортлох боломжтой бөгөөд үүнийг ангилал, регресс, кластер, зөвлөмж зэрэг ажлуудад зориулж машин сургалтын загвар бүтээхэд ашиглаж болно. ML.NET нь өгөгдсөн даалгаварт хамгийн сайн машин сургалтын алгоритм болон гиперпараметрийг сонгох үйл явцыг автоматжуулдаг AutoML функцуудыг агуулдаг. Энэ нь машин сурах гүнзгий мэдлэггүй хөгжүүлэгчдийн хувьд ч үр дүнтэй загвар бүтээх үйл явцыг хялбаршуулдаг.
ML.NET нь TensorFlow болон ONNX зэрэг бусад алдартай машин сургалтын системүүдтэй харилцан ажиллах боломжийг олгодог. Та эдгээр фрэймворкуудаас урьдчилан бүтээгдсэн загваруудыг импортлож, ML.NET програмдаа ашиглах боломжтой. ML.NET нь C# эсвэл F# ашиглан машин сургалтын загвар, дамжуулах шугам үүсгэх боломжийг олгодог. Энэ нь машин сургалтын үйл явцыг тодорхой хэрэгцээ, шаардлагад нийцүүлэн өөрчлөх боломжийг олгодог.

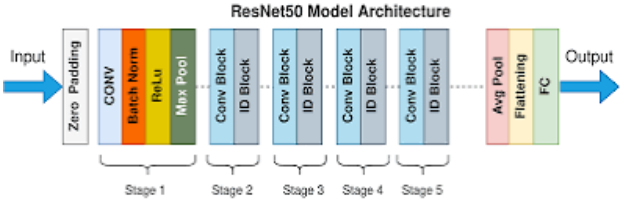
ML.NET нь том өгөгдлийн багц боловсруулахад оновчтой бөгөөд хурдасгасан сургалт, дүгнэлт хийхэд олон цөмт процессоруудыг ашиглах боломжтой. Энэ нь өндөр гүйцэтгэлтэй хувилбаруудад зориулагдсан. ML.NET нь бэлтгэгдсэн загваруудыг янз бүрийн орчинд байрлуулах механизмыг санал болгодог бөгөөд үүнд дотоод серверүүд, үүлэн платформууд (жишээ нь, Azure), хөдөлгөөнт төхөөрөмжүүд болон захын төхөөрөмжүүд орно. Энэ нь бодит цагийн таамаглалыг хөнгөвчлөх, машин сургалтыг программд нэгтгэх боломжийг олгодог. ML.NET нийгэмлэг нь заавар, баримт бичиг, форум болон GitHub-ээр дамжуулан хөгжүүлэгчдийг идэвхтэй дэмждэг. Энэ нь ML.NET-ийг үр дүнтэй сурах, ашиглах өргөн хүрээний нөөцөд хандах боломжийг олгодог. ML.NET-тэй ажиллахын тулд ердийн ажлын урсгалд өгөгдөл бэлтгэх, загвар сонгох, сургах, үнэлэх, байршуулах, байршуулсан загваруудыг ашиглан бодит цагийн таамаглал орно. ML.NET нь .NET программд машин сургалтын интеграцчиллыг хялбаршуулж, үүнийг илүү өргөн хөгжүүлэгчдийн үзэгчдэд хүртээмжтэй болгож, төрөл бүрийн домэйн дээр ухаалаг програмуудыг бий болгох боломжийг олгодог.

Deep neural network

Deep neural network (DNN) нь Feed Forward Neural Network (FFNN) гэгддэг бөгөөд өгөгдлийн шаталсан дүрслэлийг сурах замаар нарийн төвөгтэй ажлуудыг загварчлах, шийдвэрлэхэд зориулагдсан хиймэл мэдрэлийн сүлжээний нэг төрөл юм. DNN нь хүний тархины бүтэц, үйл ажиллагаанаас сэдэвлэсэн хиймэл мэдрэлийн сүлжээ, тооцооллын системүүдийн нэг хэсэг юм. Эдгээр нь хоорондоо холбогдсон зангилаа (нейрон) бүхий давхаргуудаас бүрдэнэ. DNN-д "гүн" гэсэн нэр томъёо нь оролтын болон гаралтын давхаргын хооронд олон далд давхаргууд байдгийг илэрхийлдэг бөгөөд энэ нь сүлжээнд өгөгдлийн улам хийсвэр, төвөгтэй шинж чанаруудыг сурах боломжийг олгодог. Жишээлбэл, дүрсийг танихад эхний давхарга нь ирмэгийг, дараагийн давхарга нь дүрсийг, дараагийн давхарга нь объектыг эсвэл бүр бүх дүр зургийг илрүүлдэг.
DNN-ийг том өгөгдлийн багц ашиглан сургаж, нейрон хоорондын холболтын хүчийг (жин) тохируулдаг. Сургалт нь оролтын өгөгдлийг сүлжээгээр дамжуулах, сүлжээний гаралтыг хүссэн гаралттай харьцуулах, жинг шинэчлэх, алдааг багасгахын тулд буцаан тархалт гэх мэт оновчлолын алгоритмуудыг ашиглах явдал юм. Идэвхжүүлэх функцийг нейрон бүрийн оролтын жигнэсэн нийлбэрт ашигладаг бөгөөд сигмоид, ReLU (Шулуулагдсан шугаман нэгж) болон tanh функц зэрэг нийтлэг функцуудтай. DNN нь дүрс, яриа таних, байгалийн хэл боловсруулах, зөвлөмж өгөх систем, бие даасан тээврийн хэрэгсэл зэрэг янз бүрийн салбарт ихээхэн амжилтанд хүрсэн. Тэд эрүүл мэнд, санхүү болон бусад олон салбарт амлалтаа харуулсан. Гэсэн хэдий ч DNN нь ихээхэн хэмжээний өгөгдөл, тооцоолох нөөцийн хэрэгцээ гэх мэт бэрхшээлтэй тулгардаг. Загвар нь сургалтын өгөгдөлд хэт нягт нийцэх, хэт тохируулга хийх, хэт тохируулга хийх зэрэг нь нийтлэг асуудал юм. Эдгээр сорилтуудыг үл харгалзан DNN нь хиймэл оюун ухааны салбарт хувьсгал хийж, янз бүрийн хэрэглээнд гайхалтай үр дүнд хүрсэн. Тэд судалгаа, хөгжүүлэлтийн идэвхтэй талбар хэвээр байгаа бөгөөд машин сургалт, хиймэл оюун ухааны дэвшлийг хөдөлгөсөөр байна. ResNet бол гүнзгий сүлжээний сургалтанд градиент алга болох зэрэг асуудлыг шийдвэрлэх шийдлүүдийн нэг юм.

ResNet-50

ResNet архитектур нь Convolutional Neural Network-ийн хамгийн алдартай архитектуруудын нэг юм. Ялангуяа Зураг 2-т үзүүлсэнчлэн ResNet-50 нь илүү өргөн хүрээтэй ResNet архитектурын томоохон шинэчлэлийг төлөөлдөг. Энэхүү шинэлэг зүйл нь маш гүн сүлжээг сургахад чухал үүрэг гүйцэтгэдэг үлдэгдэл эсвэл алгасах холболтыг нэвтрүүлэх явдал юм. Эдгээр холболтууд нь мэдэгдэхүйц доройтолгүйгээр сүлжээгээр дамжуулан өгөгдлийн шууд урсгалыг хөнгөвчлөх замаар градиент алга болох асуудлыг шийддэг.



Зураг 2. ResNet50 загварын архитектур

Энэ чадвар нь ResNet-д олон зуун давхарга бүхий гүн гүнзгий сүлжээг үр дүнтэй сургах боломжийг олгодог. ResNet-ийн гол шинэлэг зүйл бол алгасах холболт эсвэл үлдэгдэл холболтыг ашиглан нэг буюу хэд хэдэн давхаргыг тойрч гарах чадвар юм. Хүссэн үндсэн зураглалыг сурахын оронд ResNet загварууд үлдэгдэл зураглалд суралцдаг бөгөөд энэ нь хүссэн гаралт болон одоогийн гаралтын хоорондох ялгааг ойлгож, сүлжээний оновчлолыг илүү удирдах боломжтой болгодог. Эдгээр үлдэгдэл блокууд нь мэдээллийг олон давхаргаар дамжуулж, дараагийн давхаргууд руу шууд холбох боломжийг олгодог.

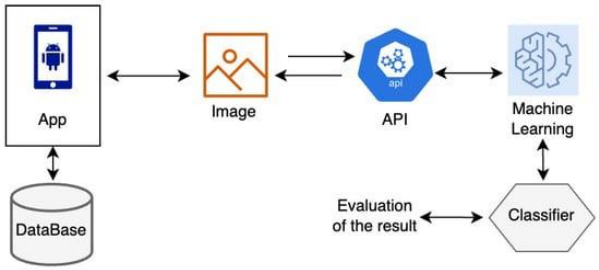
ResNet-50 нь ихэвчлэн зураг таних, ангилах ажилд ашиглагддаг бөгөөд ImageNet зэрэг өргөн хүрээний мэдээллийн багц дээр урьдчилан бэлтгэгдсэн байдаг. Энэхүү урьдчилсан сургалт нь компьютерын харааны тодорхой ажлуудад зориулж нарийн тохируулсан сургалтыг шилжүүлэх боломжийг олгодог. Үүний үр дүнд ResNet-50 нь компьютерийн харааны янз бүрийн программуудад тохиромжтой сонголт болж гарч ирсэн бөгөөд TensorFlow, PyTorch болон бусад гүнзгий сургалтын системүүдтэй нийцдэг.

DNN + ResNet-50 хослуулж ашиглах боломж

ResNet-50 нь өвөрмөц конволюцийн мэдрэлийн сүлжээ (CNN) архитектуртай. Гэсэн хэдий ч "Deep neural network" (DNN) нь сүлжээний архитектурын өргөн хүрээг хамарсан илүү ерөнхий нэр томъёо гэдгийг анхаарах нь чухал юм. Тогтмол тооны давхаргатай ResNet-50-аас ялгаатай нь DNN нь давхаргын тохиргооны хувьд ихээхэн өөрчлөлтийг харуулж чаддаг. Нэг гол ялгаа нь урьдчилан бэлтгэгдсэн загваруудын олдоц, түгээмэл байдалд оршдог. Урьдчилан бэлтгэгдсэн ResNet-50 загварууд нь хялбархан хүртээмжтэй бөгөөд янз бүрийн даалгаваруудад суралцахад өргөн хэрэглэгддэг. Үүний эсрэгээр урьдчилан бэлтгэгдсэн DNN загварууд нь тодорхой даалгаварт тохирсон байх хандлагатай байдаг тул бага түгээмэл байдаг. Цаашилбал, ResNet-50 нь ихэвчлэн компьютерийн харааны салбарт хэрэглээгээ олдог бол DNN нь илүү өргөн хүрээний хэрэглээтэй байдаг. Тэдгээрийг текст боловсруулах, яриа таних зэрэг олон салбарт ашигладаг бөгөөд тэдгээрийн олон талт байдал, өргөн хүрээний хэрэглээнд дасан зохицох чадварыг онцлон тэмдэглэдэг.

III. СУДАЛГААНЫ ХЭСЭГ

Эхинококкозын зургийг ML.NET ашиглан шинжлэх нь MRI, CT, хэт авиан зураг гэх мэт эмнэлгийн зураг дээрх эхинококкозтой холбоотой хэв шинж, гэмтлийг автоматаар илрүүлж ангилахын тулд машин сургалтыг ашиглах явдал юм. Эхинококкозын шинжилгээний хувьд уламжлалт компьютерийн хараа техник ашиглахаас илүү урьдчилан бэлтгэсэн гүн суралцах загвар болох ResNet-50 болон урьдчилан бэлтгэгдсэн Deep neural nerwork (DNN) ашиглан зургийн ангилалыг гаргаж авах болно. ДЭМБ ангиллын 2518 CT зураг байгаагаас CE1-CE2 буюу идэвхтэй үеийн 830 зураг, CE3 буюу 472 зураг, CE4-CE5 буюу 1216 зураг бүхий томоохон мэдээлэлийн багцыг Kaggle [6] системээс болон интернэтээс цуглуулсан.



Зураг 3. Системийн ажиллах зарчим

Эдгээр зургийг бид сургалтандаа ашигласан бөгөөд тестийн үе шатанд манай улсад тохиолдсон бэтэгтэй өвчтөнгүүдийн 50 зургийг ашигласан.

ХҮСНЭГТ 3. СУРГАЛТЫН БАГЦЫН ХЭМЖЭЭ

	Active	Transitional	Inactive
CT	830	472	1216
MRI	55	45	61

IV. ҮР ДҮН

Уг судалгааны ажлаар Дэлхийн эрүүл мэндийн байгуулгын гидатик уйланхай ангилалыг хэрэгжүүлсэн болно. Мөн MRI болон CT зургаар тус тус ангилал хийх боломжтой ухаалаг системийг хэрэгжүүллээ. Манай машин сургалтын загвар, туршилтаа Local CPU envorment Intel(R) Core(TM) i5-1035G1 CPU @ 1.00GHz үзүүлэлт бүхий компьютер дээр хэрэгжүүлсэн. DNN+ResNet50 нь ихэнх зургуудыг зөв ангилсан. Гэсэн хэдий ч үр дүнд нь буруу ангилсан зурагууд байсаар байна. Сонирхолтой нь (CT, MRI) нь адилхан эмнэлзүйн зураг мөртлөө ижил загварын модел дээр сургасан боловч энэ хоёрын танилтын хувь нь өөр байна. Энэ хоёрын үр дүнг харвал MRI зургийн танилт өндөр байсан бол харин эсэргээрээ CT зургийн өгөгдөл дээр сургасан загварын танилтын хувь бага байна. Бидний үзэж байгаагаар CT зургийн ангилалын танилтын хувь шалгаан нь өгөгдлийн багцыг бүрдүүлхийн тулд CT зургийг хийсэн тул зургийн өнгө чанар хэмжээ өөрчилөгдснөөс болж ерөнхий шинж байдал тодорхой хэмжээгээр нөлөөлсөн бөгөөд энэ нь субъектив байж болно.

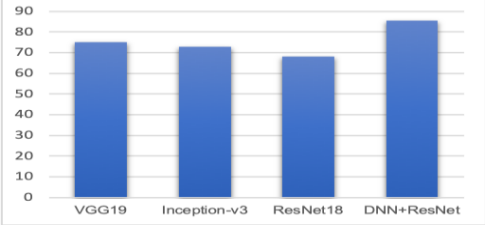
Гитадийн уйланхайн туршилтын 50 эмнэлзүйн зургаас Active ангилалд багтах 22 зургаас 17 зургийг зөв ангилсан бол үлдсэн 6 зургийг нь буруу ангилав.

ХҮСНЭГТ 4. ЗАРИМ ТЕСТИЙН ЗУРГИЙН ҮР ДҮН

Тестийн зураг	DNN+RESNET50 танилтын хувь	Эмчийн ангилсан байдал
	**Active 71%** Inactive 13% Transitional 3%	**Active**
	**Active 66%** Transitional 2% Inactive 33%	**Transitional**
	**Inactive 100%** Active 1%< Transitional 1%<	**Inactive**
	**Active 100%** Transitional 1%< Inactive 1%<	**Transitional**
	**Active 84%** Transitional 3% Inactive 13%	**Active**

Inactive ангилад орох 12 туршилтын зургийг илхад 11 зургийг зөв ангилж үлдсэн 1 зургийг буруу ангилсан. Харин Transitional ангилалд орох 16 туршилтын зургийг ангилагчаар оруулахад 14 зургийг зөв ангилсан бол үлдсэн 2 зургийг буруу тус тус ангилав. Эндээс үзэхэд манай машин сургалтын загвар нь дундажаар 85.4% хувьтайгаар (Active – 77.3%; Inactive – 91.7%, Transitional – 87.5%) өгсөн тестийн зургийг үнэн зөв ангилж чадаж байна гэж дүгнэлээ. Зарим зургийг ангилсан байдлыг Хүснэгт 4 -д харууллаа.

Мөн бусад судалгааны ажилд [7] танилцуулагдсан ангилалын аргуудтай харьцуулахад манай загварын дундаж танилтын хувь нь харьцангуй өндөр буюу 10 орчим хувиар их байгааг Зураг 4-д харуулав. Манай системийн танилтын хувь яагаад өндөр байгаа шалтгаан нь DNN алгоритмыг ResNet50 хослуулан хэрэглэсэнтэй холбоотой гэж үзэж байна.



Зураг 4.Бусад ML загваруудтай харьцуулсан туршилтын үр дүн

V. ДҮГНЭЛТ

Уйланхайт бэтэг нь биеийн олон эрхтэнд хүндрэлтэй байдаг өвчлөл юм. Рентген шинжилгээ нь энэ өвчинийг оношлох, эмчилэх, хянахад чухал үүрэг гүйцэтгэдэг. CT, MRI ULTRASOUND -гэх мэт төхөөрөмжөөс авсан, боловсруулсан хэдэн арван зургийг эмч нэг бүрчлэн өөрийн нүдээр харж ямар нэгэн асуудлыг илрүүлдэг, өвчнийг оношилдог учраас хүнээс үүдэлтэй алдаа гарах тохиолдол цөөнгүй байгаа юм. Тэгвэл манай системийн хувьд энэ асуудлыг хөндөн бэтэг өвчний тохиолдолд олон арван эмнэлзүйн зургийг машин сургалтын дэвшилтэт аргын тусламжтайгаар бэтгийн уйланхайг идэвхтэй, идэвхгүй болон шилжилтийн эсэхийг нь тодорхойлж эмчилгээний үе шатыг гаргаж авахад хялбар болгохыг зорьсон юм. Өнөөдөр эмнэлгийн ачаалал ихтэй, байгаа тул зардалыг бууруулж, цаг хугацааг хэмнэж үр ашгийг дээшлүүлэх шаардлагатай байгаа нь ойлгомжтой. Эдгээр бүх хүчин зүйлийн улмаас эмнэлгийн эмнэлзүйн зургийг үнэлэх машин сургалтын арга техникийг ашиглах нь ихээхэн ашиг тустай байна. Энэхүү санал болгож буй загвар маань одоогоор гитад уйланхайн эмнэлзүйн зургийг 85-аас дээш хувийн магадлалтайгаар үнэн зөв ангилж байна.

Цаашид зурган өгөгдлөө ихэсгэх, төхөөрөмж тус бүрээр нь ангилах, зургийн чанарыг сайжруулах, загвараа өргөтгөх гэх мэт арга замаар танилтын хувийг улам ихэсгэх боломжтой гэж үзэж байна.

ТАЛАРХАЛ

Эрдэм шинжилгээний ажлыг хийхэд шаардлагатай тестийн зургууд өгсөн АШУИС-ийн профессор Д.Тэмүүлэн багшдаа талархал илэрхийлье.

НОМ ЗҮЙ

[1] Zhang, W., Zhang, Z., Wu, W., Shi, B., Li, J., Zhou, X., Wen, H., & McManus, D. P. (2015). Epidemiology and control of echinococcosis in central Asia, with particular reference to the People's Republic of China. Acta tropica, 141(Pt B), 235–243. https://doi.org/10.1016/j.actatropica.2014.03.014

[2] Brunetti, E., Kern, P., & Vuitton, D. A. (2010). Expert consensus for the diagnosis and treatment of cystic and alveolar echinococcosis in humans. Acta tropica, 114(1), 1-16.

[3] WHO-IWGE classification Available: https://www.who.int/groups/informal-working-groups-on-echinococcosis Last Access: 2023-10-30

[4] Junghanss, T., da Silva, A. M., Horton, J., Chiodini, P. L., & Brunetti, E. (2008). Clinical management of cystic echinococcosis: state of the art, problems, and perspectives. The American journal of tropical medicine and hygiene, 79(3), 301-311.

[5] ML.NET machine learning framework Available: https://dotnet.microsoft.com/en-us/apps/machinelearning-ai/ml-dotnet Last access: 2023-11-01

[6] Kaggle - Hydatid Cyst Dataset, Available: https://www.kaggle.com/datasets/tahamu/hydatid-cyst?select=2 Last access: 2023-11-01

[7] Yildirim, M. (2023). Image Visualization and Classification Using Hydatid Cyst Images with an Explainable Hybrid Model. Applied Sciences, 13(17)

220В-ЫН ТӨХӨӨРӨМЖИД ЗОРИУЛСАН IOT АЛСЫН УДИРДЛАГАТАЙ УНТРААЛГА

Базаррагчаагийн ЭНХБАЯР[1] , Цагаанчулууны СУГИР[2]

Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, холбооны технологийн сургууль, Электроникийн салбар
[1]enhbayrb488@gmail.com , [2]sugir@must.edu.mn

Хураангуй — **Энэхүү өгүүлэлд 220В тэжээлтэй ахуйн цахилгаан хэрэгслийг алсаас буюу интернетэд холбогдсон гар утаснаас удирдан залгах/салгах, асаалттай эсэх төлөвийг нь хянах IoT системд суурилсан төхөөрөмж бүтээсэн үр дүнг өгүүлнэ. 220В цахилгаан хэрэгслийг залгах/салгах үйлдлийг Solid State Relay ашиглан микроконтроллёроор гүйцэтгэж байгаа бөгөөд хэрэглээнээс нь хамааруулан энгийн асаах/унтраах, PWM дохиогоор уян хатан байдлаар удирдах гэсэн хоёр төрлийн аргыг санал болгож байна. Төхөөрөмжийн төлөвийг гүйдлийн хэрэглээ болон өрөөний температурыг хянах хоёр аргаар тодорхойлно. Хэлхээний аюулгүй байдал, угсралт, суурилуулалтыг энгийн байлгахийг харгалзан цахилгааны щит дотор суурилуулж, хэрэглэгчтэй соронзон таслуур, автомат таслууpаар дамжуулан холбохоор төлөвлөж, овор хэмжээ, гадаад хайрцагыг зохион бүтээнэ.**

Түлхүүр үг— Solid State Relay (SSR), IoT сүлжээ, температурын хяналт ба удирдлага

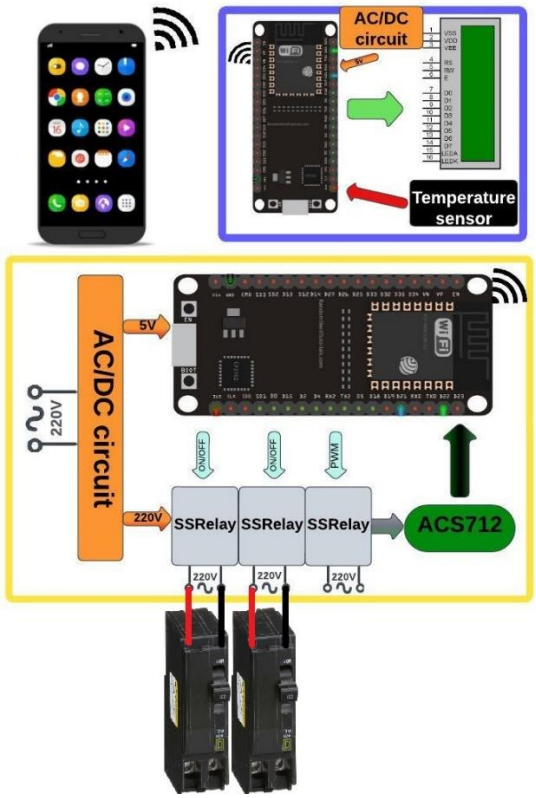
I. УДИРТГАЛ

Манай улсад хэрэглэгдэж буй алсын удирдлагатай системүүд нь ихэвчлэн нэг дотоод сүлжээнд холбоотой эсвэл IR, Bluetooth гэх мэт ойрын зайн холболттой эсвэл мэдээлэл солилцох болон хяналт тогтоох тухайн процессд төлбөр төлөх (гар утаснаас SMS зурвас илгээх) шаардлагатай системүүд байдаг. Энэ нь удирдлах хянах хүрээнээс нь хамаарч алсын удирдлагатай систем, эдийн засагт хэмнэлттэй систем гэж нэрлэхэд хүндрэлтэй нөхцөлд оруулдаг. Мөн эдгээр төхөөрөмжийн ихэнх нь асаах/унтраах гэсэн л сонголттой бөгөөд ажиллагааг нарийн хянахгүй, зөвхөн удирдлагын дохионоос хамаарсан төлөвийг илгээдэг [1][2]. Харин бидний санал болгож байгаа IoT системийн хувьд интернэтэд WiFi сүлжээгээр холбогдож ажиллах ба хэрэглэгч та гар утасны аппликешн ашиглан төхөөрөмжийг удирдах боломжтой юм.

Монголын өвөл хүйтэн байдаг нь зуслангийн эсвэл удаан хугацаагаар эзэнгүй үлдээх орон байрны цахилгаан халаалтын системийн цахилгаан зарцуулалт, аюулгүй байдлыг алсаас хянах, өрөөний температурыг тодорхой хэмд тогтвортой байлгах хэрэгцээ шаардлага их байдаг бөгөөд энэ хэрэгцээг хангаж чадах нь манай төхөөрөмжийн давуу тал юм.

II. ТӨХӨӨРӨМЖИЙН БҮТЭЦ, АЖИЛЛАГАА

А. Ерөнхий бүтэц: IoT систем нь гар утасны аппликешн программ, веб сервер, үндсэн төхөөрөмж, температур хэмжих нэмэлт төхөөрөмж гэсэн дөрвөн хэсгээс тогтоно. Үндсэн төхөөрөмж нь веб серверийн хувьд клиент, нэмэлт төхөөрөмжийн хувьд мастер болж ажиллана. Температур хэмжих нэмэлт төхөөрөмж нь тасалгааны температурыг хэмжиж дэлгэцэнд харуулах ба үндсэн төхөөрөмжтэй WiFi сүлжээгээр холбогдож, үндсэн төхөөрөмжөөс хүсэлт ирэх үед температурын утгыг хариу илгээх үүрэгтэй. Үндсэн төхөөрөмж тохируулга хийгдсэн веб серверээс удирдлагын мэдээллийг хүлээн авч, харгалзах SSR релейг удирдах ба сонголтоос хамаарч гүйдлийн мэдрэгч эсвэл өрөөний температурын утгыг боловсруулан хэрэглэгчийн төлөвийг буцааж серверт мэдээлдэг. 1-р зурагт IoT төхөөрөмжийн ерөнхий бүтцийг үзүүлэв.

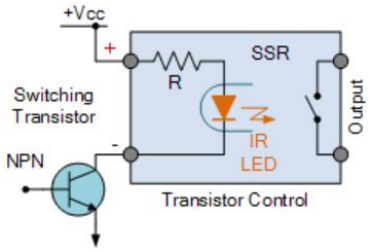


1-р зураг. Төхөөрөмжийн ерөнхий бүтэц

IoT төхөөрөмжийн PWM гаралт нь цахилгаан халаагуур удирдах зориулалттай бөгөөд тухайн хэрэглэгчийн хүссэн температур хүртэл халаах болон тухайн температурт нь дулааныг хадгалах, өрөөний температурыг хэмжиж мэдээллэх

боломжууд нь халаалтын төхөөрөмжийн хэт ачааллыг багасгах бөгөөд хэрэглээний насжалтыг уртасгах боломжтой. Бусад ахуйн цахилгаан хэрэгслийн хувьд энгийнээр асааж/унтраах үйлдэл гүйцэтгэх бөгөөд төлөвийг нь гүйдлийн мэдрэгчээр хянана.

B. Solid State Relay: 2 порттой, хагас дамжуулагч удирдлагатай диод хэлбэрээр ерөнхийлсөн бүтэцтэй, триак болон тиристорд суурилсан релейг SSR гэдэг. Удирдах порт нь ихэнхдээ тогтмол 3 – 32В хүчдэл, 10мА – 30мА гүйдэлтэй байдаг бол хувьсах гүйдлийн хэлхээ холбох портын чадлаар нь 10А, 20А, 40А, ... 150А гэж ангилдаг.[3] SSR релейн дотоод бүтцийг 2-р зурагт харуулсан хялбар хэлхээгээр төсөөлөн биполяр транзистораар дамжуулан микроконтроллёрын портоос шууд удирдаж болно.[4]

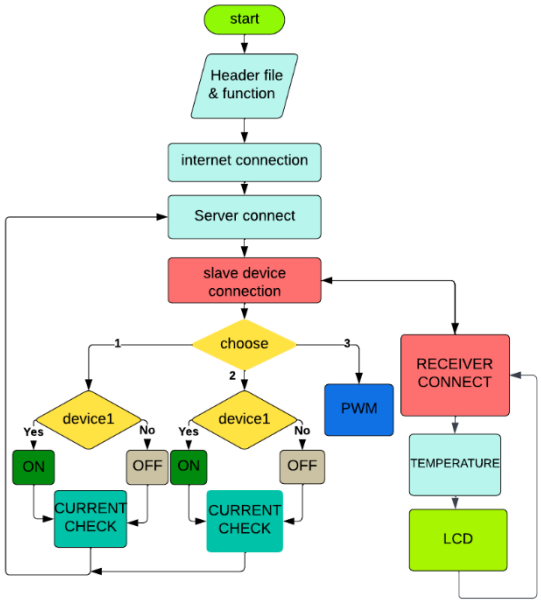


2-р зураг. SSR-ны дотоод бүтэц [4]

C. ESP32 микроконтроллёр: ESP32 өөртөө WiFi болон Bluetooth модуль агуулсан, хоёр цөмт (dual core) 32 битийн микроконтроллёр бөгөөд тухайн орчиндоо бие даасан утасгүй сүлжээг бий болгох боломжтой (Soft Access Point – AP) горим, өөрт ойрхон утасгүй сүлжээнд клиент (Station mode - STA) горимд ажиллах гэсэн үндсэн 2 горимоор ажиллаж чаддаг. Үүнээс гадна 240MHz хүртэлх хурд, 4 – 16MB шуурхай санах ойтой, ADC, DAC, SPI, UART, I^2C , I^2S зэрэг IoT системд зориулсан интерфейсүүдийг агуулсан. Arduino IDE, Espressif IDF, Javascript, Phyton зэрэг програмчлалын программуудыг дэмжин ажилладаг. Espressif System компанийн 40нм технологи ашиглан хөгжүүлсэн хөгжүүлэлтийн боард юм.[5]

3-р зураг. ESP32 микроконтроллёр

D. Программ: ESP32 микроконтроллёрыг Arduino IDE ашиглан, 4-р зурагт харуулсан алгоритмын дагуу програмчилсан.



4-р зураг. Программын алгоритм

E. BLYNK io: Энэ бол виртуал порт үүсгэн түүний бүтцийг тодорхойлж action хэлбэрт дүрслэх дэлгэц, мэдээллийг боловсруулах, хадгалах өгөгдлийн сан зэргийг цогц шийдсэн, IoT системийн веб серверийг хялбар зохион байгуулахад зориулсан сайт юм.[6]

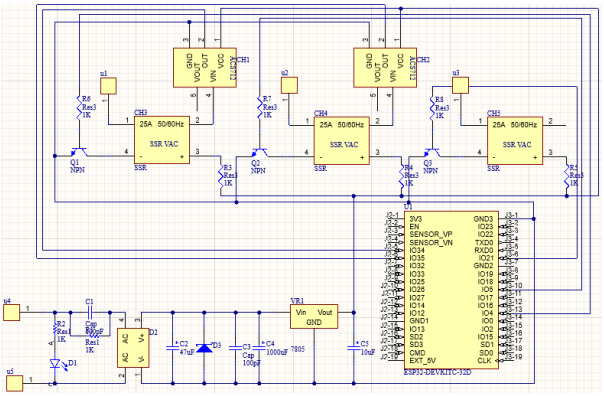
Түүнчлэн сервер дашбоард дээр угсарсан загварын дагуу бэлэн блокуудыг угсрах замаар аппликешн программаа зохион бүтээх боломжтой. Энэ сайтын тусламжтайгаар гар утасны аппликешн программыг зохиосон бөгөөд хэрэглэгчийн интерфейсийг нь 5-р зурагт харуулж байна.

5-р зураг. Гар утасны аппликешн

III. Хэрэгжүүлэлт

IoT системд суурилсан төхөөрөмжийн зарчмын схемийг боловсруулан түүний PCB загварыг гарган төхөөрөмжийн үндсэн бүтцийг бий болгохоор ажиллаж байна. Үүний үр дүнд хэрэглээнд гаргахад бэлэн төхөөрөмжийг бий болгохоор зорьж байна.

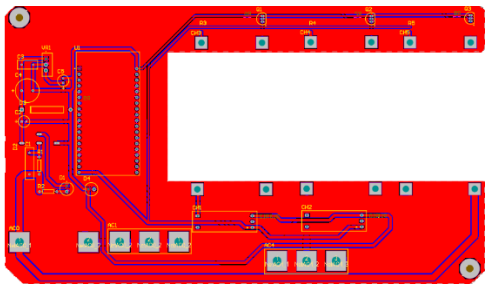
Үндсэн төхөөрөмжийн зарчмын схемийг 6-р зураг харууллаа.



6-р зураг. Үндсэн төхөөрөмжийн зарчмын схем

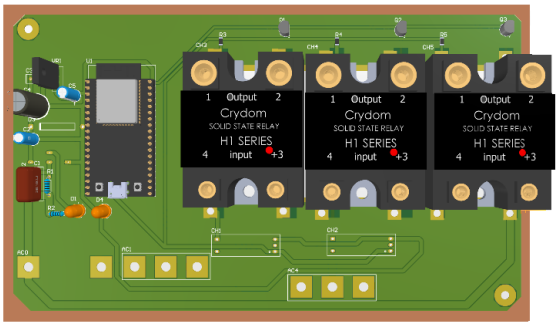
Төхөөрөмжийн үндсэн хэлхээний бүтэц буюу тэжээлийн хэсэг, микроконтроллёр , SSR релей, гүйдлийн сенсор зэрэг элементийн холболтыг харах боломжтой.

Зарчмын схемийн дагуу боловсруулсан PCB хавтан нь дээд давхрага (top layer), доод давхрага (bottom layer) гэсэн үндсэн хоёр талтай бөгөөд дээд давхраг (top layer) – ийг 7-р зурагт харуулж байна.



7-р зураг. PCB зураг

7-р зурагт харуулсан PCB хавтанг харагдах байдлын хувьд бодит байлгах үүднээс 3D зураг болгон харуулахыг зорьсон (зураг 8). SSR релей нь хэмжээ том учраас төхөөрөмжийн хэмжээг хэт том болгохгүй, холболт хийхэд энгийн байлгахын тулд боловсруулсан загвар юм.



8-р зураг. 3D PCB зураг

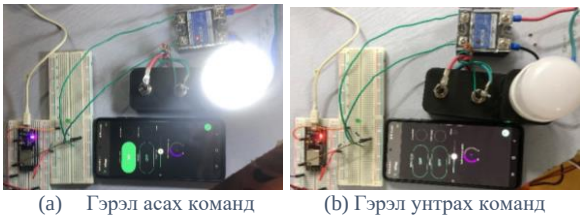
PCB – д зориулж хийхээр төлөвлөсөн кейс болон төхөөрөмжийн харагдах байдлыг бодит хэмжээг төсөөлөх боломжийг бий болгохыг зорилоо.

IV. Туршилт, үр дүн

Төхөөрөмжийн ажиллагааг үнэлэхийн тулд

1. Гар утаснаас хэрэглэгчийг залгаж/салгаж, төлөвийг нь унших туршилт
2. Температурын утгыг гар утсанд хүлээж авч дүрслэх туршилт
3. PWM гаралтын дохио болон хэрэглэгчийн чадлыг харьцуулах хэмжилт тус тус хийлээ.

А. Энгийн залгах/салгах туршилт: Хэрэглэгчийг гэрлээр төлөөлүүлэн асааж/унтраахыг зайнаас удирдах туршилт хийсэн бөгөөд үүндээ SSR релейн гүйдлийг 10мА гэж тооцоо хийн npn транзисторан түлхүүрийн хэлхээг угсарсан ба түлхүүрийн баазыг микроконтроллёрын портоос удирдсан.



(a) Гэрэл асах команд (b) Гэрэл унтрах команд

9-зураг. Гэрэл асаах/унтраах туршилт

9(a)-р зурагт хэрэглэгчийг залгах команд илгээсэн бөгөөд гар утасны дэлгэц дээр хэрэглэгч залгагдсан гэдгийг гүйдлийн мэдрэгчээр хэмжиж тодорхойлсон үр дүнг буцааж илгээснийг тод ногоон өнгөөр гэрэлтүүлж харуулж байна. 9(b)-р зурагт хэрэглэгчийн салгах команд илгээсэн бөгөөд микроконтроллёроос хэрэглэгчийн гүйдлийг хэмжиж, салгагдсан байгааг бататган шалгасан үр дүнг илгээснийг унтарсан төлөвөөр харуулж байна.

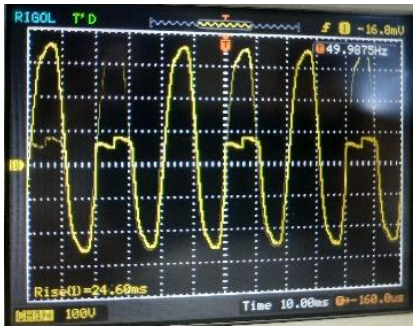
В.Температурын мэдээлэл солилцох туршилт: Туслах төхөөрөмж температурын мэдрэгчийн тусламжтайгаар тасалгааны хэмийг хэмжиж, LCD дэлгэц дээр дүрслэхээс гадна, үндсэн төхөөрөмжөөр дамжуулан серверт илгээснийг гар утасны дэлгэц дээр хэрхэн дүрсэлж байгааг 10-р зурагт харууллаа.

10-р зураг. Температурын мэдээлэл хүлээж авах туршилт

I^2C интерфейсээр мэдээлэл дамжуулдаг тоон температурын мэдрэгч сонгож хэрэглэж байгаа бөгөөд $0.5^{\circ}C$ алхамтай өөрчлөлтийг харуулна.

C. PWM дохиогоор хэрэглэгчийн чадлыг удирдах туршилт: Цахилгаан халаагуурын цахилгаан зарцуулалтыг PWM дохиогоор удирдаж хянах туршилтыг хийхдээ SSR релейн гаралтанд осцилскоп (oscillscope) ба амперметр холбон ажиллуулсан. PWM дохионы DC-ийг 10%-аас 100% хүртэл ихэсгэн хэмжилтийг хийсэн бөгөөд зарим хэмжилтийн осциллографыг 11-13-р зурагт түүвэрлэн харууллаа.

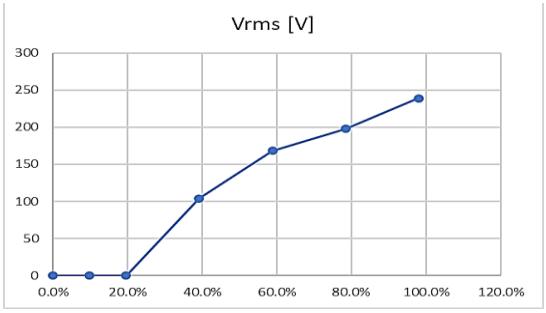
11-зураг. Дохионы 100%-ийн гаралт



12-зураг. Дохионы 70%-ийн гаралт

13-зураг. Дохионы 50%-ийн гаралт

Хэрэглэгчид очих цахилгаан хүчдэлийн үйлчлэх утга PWM дохионы DC-ээс хамаарч өөрчлөгдөж чадах эсэхийг туршилтаар тодорхойлохыг зорьсон бөгөөд 14-р зурагт хэмжилтийн үр дүнг харуулж байна.



14-зураг. PWM дохионы гаралт, хүчдэлийн хамаарал

14-р зургийн графикаас PWM дохионы DC 20% хүртэл багасахад цахилгаан хүчдэлийн үйлчлэх утга харгалзан буурсан байгааг харж болно. Энэ нь PWM дохиогоор хэрэглэгчийн чадлыг удирдах боломжтойг баталж байна.

V. Дүгнэлт

220В ахуйн цахилгаан хэрэгслийг алсаас асааж/унтраах, IoT системд суурилсан унтраалгын загварыг зохион бүтээлээ. Энэ төхөөрөмж нь ахуйн цахилгаан хэрэгслийг энгийнээр асааж/унтраах ба PWM дохиогоор чадлыг нь хязгаарлаж удирдах хэмээх хоёр горимтой. Хэрэглэгч залгагдсан эсэхийг гүйдэл мэдрэгч, температур мэдрэгч ашиглан тодорхойлдог тул тус төхөөрөмжийг цаашид цахилгааны хэрэглээг мэдээллэх, аюулгүй байдлыг хянах зэргээр өргөжүүлэх бүрэн боломжтой. Үндсэн болон нэмэлт модулиуд бүгд интернет сүлжээнд холбогдож, гар утсанд суулгасан аппликешн програмтай хоршиж ажилладаг нь хэрэглэгчийн хувьд хэрэглэхэд хялбар, алсаас удирдах боломжтой, эдийн засаг болон цаг хугацааг хэмнэх ач холбогдолтой төхөөрөмж болсон.

VI. Ном зүй

[1] Muhammad Ansar, “GSM based Home Appliance Control” project. 2021. e-source: https://www.hackster.io/embeddedlab786/gsm-based-home-appliance-control-5de80a

[2] Tongou LLC, “Single Phase Din Rail Smart Meter – TO-Q-SYS” product, e-source: https://elcb.net/product/single-phase-din-rail-smart-meter

[3] HUIMU Electronics LLC, “MGR-1 Series Panel Mount Solid State Relay” product, e-source https://electronics.huimultd.com/Product/Solid-State-Relay/Panel-Mount-SSR/MGR-1-Series/

[4] Electronics Tutorials: “Solid State Relay”, e-source https://www.electronics-tutorials.ws/power/solid-state-relay.html

[5] А.Одгэрэл, А.Сундий “Эмбэддэд системийн өгөгдлийг шифрлэн дамжуулах нь” Эрдэм шинжилгээний өгүүлэл, “Эрдмийн чуулган-2023” МХТС-ийн эрдэм шинжилгээний бүтээлийн эмхэтгэл, хуудас. 35. 2023.

[6] Blynk веб сайт. https://blynk.io/

ХОРТОЙ URL -ИЙГ МАШИН СУРГАЛТ АШИГЛАН ИЛРҮҮЛЭХ

Н. Даваадорж[1], Ж. Өнөболд[2] , Т.Шижир-Алт[3], М. Жүгдэрнамжил, Б. Мөнхбаяр[5]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбоо Технологийн Сургууль,
Мэдээллийн сүлжээ аюулгүй байдлын салбар
И-мэйл хаяг: B200970014@must.edu.mn

***Хураангуй*—**Энэхүү судалгааны ажилд хортой URL -г илрүүлэх зорилтыг шийдвэрлэхийн тулд supervised машин сургалтын загварыг ашигласан. Энэ систем нь URL -г хортой, хоргүй гэсэн хоёр ангилалд ангилахдаа Binary Classification ерөнхий аргыг хэрэглэсэн ба үүнд Logistic Regression, SVM, KNN, Decision Tree, Random Forest аргууд багтсан. URL -г шинж чанаруудаар нь задлахдаа lexical, domain-based, content-based гэсэн 3 бүлгийн 36 шинж чанараар задалж, машин сургалтандаа ашигласан. URL -г зөв таниж байгаа эсэхийг үнэлэхдээ нийт хортой, хоргүй URL -ийнхээ 70% -ийг машин сургалт, 30% -ийг туршилтандаа ашиглахад Random Forest алгоритмын үр дүн буюу accuracy 99.70% -тай илрүүлсэн.

Түлхүүр үг— Хортой URL, Machine Learning, Random Forest

I. УДИРТГАЛ

Бидний өдөр тутмын амьдралд интернэтийн хэрэглээ өсөхийн хэрээр хортой холбоос (URL)-тай холбоотой халдлагууд дагаад ихсэж байна. Хортой URL нь фишинг халдлага, нийгмийн инженерчлэл, залилан гэх мэт кибер аюул заналхийллийн эхлэл болдог. Цахим гэмт хэрэгтнүүд зорилтот хэрэглэгчдийг мэхлэх цаашлаад хор хөнөөл учруулах арга техникийг тасралтгүй боловсруулж, халдлагын арга барилаа улам бүр боловсронгуй нарийн болгож байгаа тул түүнийг үнэн зөв илрүүлэх механизмыг хөгжүүлэх нь зайлшгүй чухал юм.

Энэхүү судалгааны ажлаар хортой URL-ийг машин сургалтын арга ашиглан илрүүлэх боломжийг танилцуулж байна. URL нь интернэтийн чухал бүрэлдэхүүн хэсэг бөгөөд халдагчид хэрэглэгчдийг хууран мэхлэхийн тулд түүний хэв маяг, бүтцийг нь жинхэнэ URL -тэй төстэй болгож үр дүнд нь тэднийг хортой вэбсайт руу чиглүүлж, эсвэл хүсээгүй ямар нэгэн үйлдлүүдийг хийхэд хүргэдэг. Машин сургалт нь шинж чанарт үндэслэн хэв маягийг таньж, ялгах чадвартай тул хортой URL -ийг тодорхойлох сайн арга юм.

II. СЭДЭЛ БОЛОН ЗОРИЛГО

Тогтмол өргөжиж буй дижитал эрин үед интернэт бидний өдөр тутмын салшгүй хэрэглээ болсон билээ. 2023 оны 7 дугаар сарын судалгаагаар интернэт хэрэглэгчдийн тоо 5.18 тэрбумд хүрсэн ба энэ нь дэлхийн нийт хүн амын 64.6% юм. Бидний хуруугаа хөдөлгөөд л олж чадах мэдээллийн хэмжээ нэмэгдэхийн хэрээр түүнийг дагасан аюул занал ч мөн төдий чинээгээр өсөж байна. Энэхүү аюул гэсэн энэ өргөн цар хүрээтэй ойлголт дунд хамгийн өргөн цар хүрээтэй, хамгийн түгээмэл сэдэв бол “Хортой URL(Uniform Resource Locator)” юм.

Уг аюул нь ихэвчлэн нийгмийн инженерчлэл (social engineeirng) болон фишинг (phishing) халдлагаар дамжуулан хувь хүн эсвэл бүлэг хүмүүсийн хувийн мэдээлэл болон дансны мэдээлэл зэргийг хууль бус байдлаар олж авч, ашиглахыг зорьдог.

Монгол Улсад интернэт хэрэглэгчдийн тоо 2012 онд 695 мянга байсан бол уг тоо 2017 онд 3.5 сая, 2018 онд 4.1 сая, 2019 онд 5.4 сая болж 2012 онтой харьцуулахад 7.8 дахин нэмэгдсэн, фэйсбүүк хэрэглэгчдийн тоогоор Ази тивд 1 дүгээрт /2.2 сая хэрэглэгч/, дэлхийд 10 дугаар байрт жагсах болсон ба цахим хэрэглээний хамрах хүрээ, хэрэглээ хурдацтай өсч байгаа нь Үндэсний статистикийн хорооны мэдээллээс харагдаж байна. [12]

[12] судалгааны ажилд манай улсад үйлдэгдсэн цахим гэмт хэргийн тоо 2018 онд 659, 2019 онд 737, 2020 онд 1795, 2021 оны эхний хагас жилд 1949 хүрсэн гэдгийг дурьдсан. Тэгвэл энэ тоо 2023 оны эхний 2-р улирлын байдлаар 3,618-т хүрээд байгаа юм. [13]

Үүнээс харахад олон улс төдийгүй манай орны хувьд ч мөн ялгаагүй интернэтийн хэрэглээ, түүнийг дагасан цахим аюул заналын тоо зэрэг нь анхаарч үзэхүйц хэмжээнд хүрээд байна.

Хортой холбоос (URL)-р дамжиж үйлдэгдэж буй халдлагууд улам бүр боловсронгуй болсноор түүнийг илрүүлэх чадамжтай байсан арга техникүүд одоогийн байдлаар бүрэн гүйцэт, үнэн зөв ажиллахад хүндрэлтэй болоод буй юм. Үүний нэг жишээ нь хар жагсаалт (Blacklisting) арга бөгөөд энэхүү арга нь бүхий л мэдэгдэж буй хортой холбоос (URL)-г өгөгдлийн санд хадгалан уг өгөгдлийн сангаас тухайн холбоос (URL)-г шүүх байдлаар хортой эсвэл хоргүй гэж ялгадаг байсан. Гэсэн хэдий ч энэхүү арга нь өгөгдлийн санд байхгүй буюу ангилал нь мэдэгдэхгүй байгаа холбоос (URL)-г хортой эсвэл хоргүй гэж ялгах боломжгүй. Тиймээс өдөр ирэх тусам нэмэгдэж, хувьсан өөрчлөгдөж буй хортой холбоос (URL)-г үнэн зөв, баталгаатай байдлаар илрүүлэх шинэ үеийн арга техникийг хөгжүүлэх шаардлагатай байгаа юм.
Үүнээс гадна хорт URL-г илрүүлэхдээ Монгол улсад хамаарагдах домэйн, холбоос (URL) зэргийг авч үзэх нь чухал бөгөөд учир нь энэ чиглэлээр хийгдсэн судалгааны ажлуудыг үзэхэд машин сургалтын өгөгдлийн багц (Dataset)-д Монгол холбоос (URL) байхгүй байгаа юм.

Мөн Кибер гэмт хэрэгтэй холбоотой мэргэжлийн болон сайн дурын, магистр, докторын зэрэг бүхий судлаачдын судалгааны ажлууд олон улсад ихээхэн хийгдэж эхэлсэн бол манай улсын хувьд харьцангуй бага байна. [12]

Тиймээс энэхүү асуудлуудад шийдэл боловсруулахын тулд бидний зүгээс хортой холбоос (URL)-р дамжигдан үйлдэгдэж буй халдлагыг үнэн зөв илрүүлэх, хүн бүхэн ашиглах боломж бүхий веб хуудас хийхийг зорьж ажилласан. Мөн энэхүү хортой холбоос (URL) илрүүлэх веб хуудсыг “extension” байдлаар ашиглах боломжийг бүрдүүлсэн ба энэ нь хэрэглэгч тухайн зочилж буй веб хуудсын холбоосыг ганцхан товч дараад л хортой эсвэл хоргүй гэдгийг ялгах боломжтой гэсэн үг юм.

Ингэхдээ өгөгдлийн багц (Dataset)-д Монгол холбоос (URL)-г тодорхой тоогоор нэмэгдүүлэх, шинж чанараар задлах үйлдлүүдийг (Feature Extraction) олшруулах, оновчтой машин сургалтын алгоритмуудыг ашиглах зэргийг зорьж ажилласан.

III. ӨМНӨ СУДЛАГДСАН АЖЛУУД

Энэ хэсэгт хортой URL буюу холбоосыг илрүүлэх болон ангилах асуудлыг шийдвэрлэхийн тулд хийгдсэн судалгааны ажлуудыг авч үзэх болно.

Гарын үсэгт суурилсан /Signature based/ буюу blacklist based, машин сургалтад суурилсан /Machine Learning based/, Контентод суурилсан /Content based/, Домэйн нэрийн системд суурилсан /DNS based/ гэх мэтчилэн аргуудыг ашиглан хортой холбоос (URL) -г илрүүлэх боломжтой хэдий ч зарим аргууд нь хурдацтай өөрчлөгдөн, илүү нарийсаж буй цахим халдлага, хортой холбоос (URL)-г бүрэн гүйцэт таних, илрүүлэх боломжгүй болоод байгаа юм.

A. SIGNATURE BASED MALICIOUS URL DETECTION

Хиймэл оюун ухаан, машин сургалт зэргийн тухай ойлголт өнөөдрийнхтэй харьцуулахад бага байсан үед гарын үсэгт суурилсан аргыг ашиглан хортой URL -г илрүүлэх тохиолдол элбэг байсан. Одоогоос 10 гаруй жилийн өмнө хийгдсэн [1] болон [2] судалгааны ажлуудаас харвал эдгээр ажлууд нь ихэвчлэн мэдэгдэж буй хортой URL холбоосуудыг ашигласан байна. Тодруулбал шалгахаар оруулсан URL холбоос нь өгөгдлийн санд хадгалагдаж буй хортой холбоостой тохирч байвал уг холбоосыг хортой гэж үзэж анхааруулга гарч ирнэ. Бусад тохиолдолд шалгахаар оруулсан URL холбоосыг хортой гэж үзэхгүй. Энэхүү аргын хамгийн том сул тал нь өгөгдлийн санд хадгалагдаагүй буюу жагсаалт дотор байхгүй шинэ хортой холбоос (URL)-г илрүүлж чадахгүй явдал юм.

B. MACHINE LEARNING BASED MALICIOUS URL DETECTION

Машин сургалтад тулгуурлан хортой URL холбоосуудыг илрүүлэх нь хамгийн үр дүнтэй гэж үзэж байгаа бөгөөд учир нь өмнөх signature based арга шиг жагсаалтад байхгүй шинэ URL холбоосыг ч алдалгүй илрүүлэх боломжтой юм. Энэ тухай хийсэн Aldwairi болон Alsalman [4] судалгаанд хортой URL холбоосыг 87% precision нарийвчлалтай илрүүлж байсан бөгөөд ингэхдээ lexical-based, content-based, network-based зэрэг feature extraction аргуудыг ашигласан. Өгөгдлийн багцын хувьд аюулгүй URL холбоосуудыг Alexa [5], хортой URL холбоосуудыг PhishTank [6] сайтуудаас тус тус авсан.
Мөн Xuan болон багийн гишүүдтэйгээ хийсэн судалгааны ажилд [3] машин сургалтын алгоритмуудыг ашиглан хортой URL холбоосыг илрүүлсэн бөгөөд нийт ашигласан алгоритмууд дотроос Random Forest алгоритм нь хамгийн өндөр хувьтай буюу 96.28% accuracy нарийвчлалтай илрүүлж байсан бөгөөд Suan болон багийн гишүүдтэйгээ хийсэн судалгааны ажил [7] нь энэ accuracy хувийг 97.36% хүртэл өсгөж чадсан. Тэдний ашигласан өгөгдлийн багцын хувьд ялгаатай байсан бөгөөд University of California Irvine Machine Learning Repository (UCI–ML) [8] ашигласан.

Yu [9] судалгааны ажилд deep belief network (DBN) болон support vector machine (SVM) гэсэн машин сургалтын алгоритмуудыг ашигласан бөгөөд өгөгдлийн багцаа Phishtank[6] -аас цуглуулсан. Үр дүнд нь DBN-SVM модел нь 99.96% accuracy маш нарийн үзүүлэлттэйгээр хортой URL холбоосыг илрүүлсэн.

Sahingoz [10] судалгааны ажилд машин сургалтын олон алгоритмуудыг ашиглан туршилт хийсэн ба онцлог нь тэдгээрийг хооронд нь хослуулан hybrid feature төрлийн аргыг ашигласан. Ингэснээр дан ганц алгоритмаар бус олон аргыг нэгтгэн турших нь илүү амжилттай ажиллаж болох юм гэдгийг харуулсан. Үр дүнд нь Random Forest алгоритмыг NLP feature -тээ хослуулсан туршилт нь 97.98% буюу хамгийн өндөр хувьтайгаар хортой URL -г илрүүлсэн ба туршилтдаа хоргүй 36400, хортой 37175 холбоос (URL) тус тус ашигласан байна.

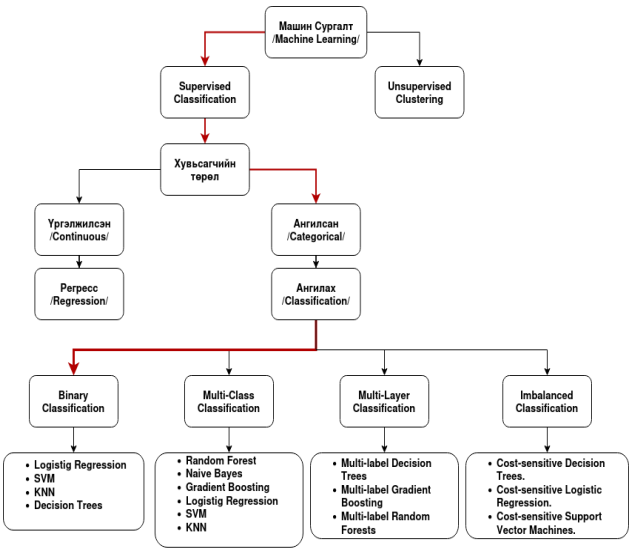
Өмнө судлагдсан ажлуудаас үзэхэд “Random Forest” алгоритм оновчлолын хувь (Accuracy) хамгийн өндөр байна.

IV. МАШИН СУРГАЛТЫН АРГУУД БА АЛГОРИТМ СОНГОЛТ

Бидний судалгааны ажлын үр дүнд хаяглагдсан өгөгдлийн багц /labeled dataset/ ашиглан шинэ /unknown/ холбоосыг хортой эсвэл хоргүй гэж ангилах боломжтой вэб хэрэгсэл хийхийг зорьж буй бөгөөд гаралтын үр дүн нь зөвхөн “хортой” эсвэл “хоргүй” гэсэн байдалтай байна. Машин сургалтын модел нь ашиглах өгөгдлийн багцаасаа хамаараад

- Supervised
- Unsupervised
- Semi-supervised
- Reinforcement

гэж ангилагдах ба бидний хийж буй судалгааны ажилд “supervised machine learning” модел нийцэх юм. Учир нь “supervised machine learning” модел нь хаяглагдсан өгөгдлийн багц /labeled dataset/ ашиглан моделоо сургаж, дараа нь уг үр дүнгээ ашиглан шинэ /unknown/ өгөгдөл дээр тооцоолол хийж гаралтыг урьдчилан таамагладаг. Supervised machine learning дотор classification болон regression гэсэн үндсэн 2 арга байх бөгөөд ангилах /classification/ аргын хувьд хувьсагчийн төрөл нь дискрет хэлбэртэй байх бөгөөд энэ төрлийн аргыг аливаа ялгаатай зүйлсийг ангилахад ашигладаг. Харин регресс/regression/ аргын хувьд хувьсагчийн төрөл үргэлжилсэн /continuous/ хэлбэртэй байх бөгөөд энэ төрлийн аргыг ашиглан өмнөх онуудын цаг агаарын өгөгдлөөс улбаалан ирээдүйн цаг агаарыг тооцоолох, зах зээлийн чиг хандлага дээр тулгуурлан орон сууцны үнийг таамаглах зэргээр ашиглаж болно. Бидний хийж буй судалгааны ажлын хүрээнд холбоос /URL/-г “хортой” эсвэл “хоргүй” гэж ангилах тул “classification” арга илүү тохиромжтой.



1-р зураг. Машин сургалтын төрлүүд ба алгоритмууд.

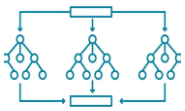
Classification арга нь дотроо мөн дараах байдлаар 4 хуваагдана.

- Binary Classification
- Multi-Class Classification
- Multi-Label Classification
- Imbalanced Classification

Binary Classification аргын хувьд оролтын өгөгдлийг эсрэгцүүлсэн 2 төрөлд ангилах зорилготой. Жишээлбэл үнэн-худал, 1-0, хортой-хоргүй гэх мэт. Үлдсэн аргуудын хувьд хоёроос олон төрлийн оролтын өгөгдлөөс үр дүнг таамаглах зорилготой. Тиймээс энэхүү Binary Classification арга нь бидний судалгааны ажилд тохиромжтой юм.

Бидний хувьд дээрх шаардлагууд дээр үндэслэн болон өмнө судлагдсан ажлууд дээр хамгийн өндөр илрүүлэлтийн хувьтай тооцоолол хийгдсэн машин сургалтын алгоритмуудыг сонгон хөгжүүлэлт, болон туршилтаа явуулсан.

1-р хүснэгт. Машин сургалтын алгоритмууд

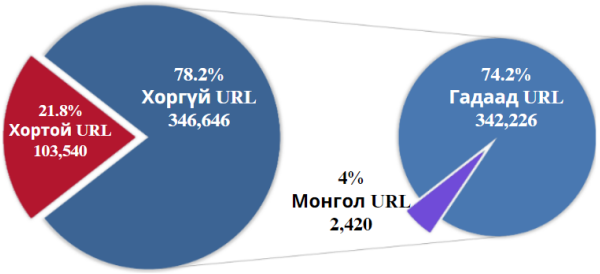
Машин сургалтын арга	**Тайлбар**	**Зурган төлөөлөл**
Support Vector Machine (SVM)	SVM нь нэг ангилалын өгөгдлийг нөгөө ангилалын өгөгдөлөөс тусгаарлах шугаман замаар өгөгдлийг ангилдаг.	
Decision Tree	Decision Tree нь хариу үйлдлийг урьдчилан таамаглах боломжийг олгодог бөгөөд урьдчилан таамаглахийн тул утгын олон салаа мөчир гаргадаг. Салаа бүрийн тоо утгыг сургалтын явцад тодорхойлно.	
Random Forest	Random forest нь нэг үр дүнд хүрэхийн тулд олон Decision Tree гаралтыг нэгтгэдэг түгээмэл хэрэглэгддэг машин сургалтын алгоритм юм. Ашиглахад хялбар, уян хатан байдал нь ангилал болон регрессийн асуудлыг хоёуланг нь зохицуулдаг.	
k-Nearest Neighbor (KNN)	KNN бол өгөгдлийн багц дахь хамгийн ойрын хөршүүдийн төлөв дээр үндэслэж объектуудыг ангилдаг загва юм. Мөн бие биеийнхээ ойролцоох объектуудыг ижил төстэй гэж үздэг ба хамгийн ойрын хөршийг олохын тулд косинус, Чебышев зэрэг зайны хэмжүүрүүдийг ашигладаг.	

V. ХОРТОЙ URL-Г МАШИН СУРГАЛТЫН АРГА АШИГЛАН ИЛРҮҮЛЭХ

A. Өгөгдлийн багц /Dataset/

Шаардлагатай өгөгдлийн багцыг бүрдүүлэхийн тулд бид kaggle хуудас дээрх өгөгдлийн багцыг ашигласан. Энэхүү өгөгдлийн багц нь [3] судалгааны ажилд дурдагдсан байдлаар буюу хортой холбоос /URL/-г Phishtank хуудаснаас, хоргүй холбоос /URL/-г Alexa хуудаснаас тус тус цуглуулсан, давтагдахгүй байдлаар 450176 ширхэг өгөгдлийг агуулсан. Үүний 77% буюу **346636** нь хоргүй холбоос /URL/, 23% буюу **103540** нь хортой холбоос /URL/ юм. Бидний олж харсан асуудал болон сэдлийн хүрээнд энэхүү өгөгдлийн багцыг Монгол холбоос /URL/-оор баяжуулахын тулд https://subdomainfinder.c99.nl/ онлайн хэрэглийг ашиглан бүх .gov.mn болон .edu.mn дэд домэйн бүхий холбоос /URL/-уудыг цуглуулж, өгөгдлийн багцад нэмж өгсөн. Бид шинээр цуглуулсан Монгол холбоос /URL/-уудаа Virustotal хэрэгслээр шалган хоргүй гэж ангилсан бөгөөд үр дүнд нь бид нийт өгөгдлийн багцад **2,420** ширхэг Монгол холбоос /URL/-ыг нэмж оруулж өгсөн.

- **Phishtank** нь phishing халдлагаас хамгаалах зорилго бүхий онлайн платформ бөгөөд мэдэгдэж байгаа phishing сайтыг өгөгдлийн санд байнга нэмэх боломжтой нь байгууллага мэргэжилтнүүдэд уг аюулаас хамгаалах боломжийг нэмэгдүүлдэг.
- **Alexa** нь Амазоны эзэмшдэг вэб сайт бөгөөд энэ нь зочдын тоо, хуудасны үзсэн байдал гэх мэт янз бүрийн хүчин зүйл дээр үндэслэн вэбсайтын ачаалал, нэр хүндийг тогтоож, эрэмбэлдэг систем юм. Энэ эрэмбэ, үнэлгээг ашиглан аюулгүй вэб сайтуудын URL -ийг цуглуулах боломжтой.
- **Kaggle** нь мэдээллийн шинжлэх ухаан, машин сургалтад өргөн хэрэглэгддэг алдартай онлайн платформ ба судалгаа, дүн шинжилгээ, машин сургалтын төслүүдэд ашиглаж болох өргөн хүрээний, олон төрлийн өгөгдлийн багцыг санал болгодог.
- **Virustotal** нь хортой программ хангамж, вэб сайтуудыг илрүүлэхийн тулд сэжигтэй файл болон URL -д дүн шинжилгээ хийдэг онлайн үйлчилгээ юм.



2-р зураг. Өгөгдлийн багцын задаргаа

B. Шинж чанараар задлах /Feature Extraction/

Бидний хийж буй судалгааны ажилд холбоос /URL/-г хортой эсвэл хоргүй гэдгийг ямар шинж чанарууд дээр нь үндэслэн таних вэ гэдэг чухал ойлголт. [11] судалгааны ажилд уг голлох шинж чанаруудыг бүлэглэн авч үзсэн бөгөөд үүний адилаар бид хортой холбоос /URL/-г таних шинж чанаруудыг дараах байдлаар 3 бүлэг болгон ангилж, бүлэг тус бүрт

шинэ шинж чанарууд нэмэхийг мөн зорьж ажилласан.

Үг зүйд суурилсан шинж чанарууд /Lexical based features/: Энэ бүлэгт холбоос /URL/-ын урт, домайн нэрийн урт, замын урт /path length/, тусгай тэмдэгтүүд агуулж байгаа эсэх гэх мэт холбоос /URL/-ын үг зүйд суурилсан буюу харагдах байдал талын шинж чанарууд орно.

Домайнд суурилсан шинж чанарууд /Domain based feature extraction/: Энэ бүлэгт тухайн холбоос /URL/-ын домайнд суурилсан шинж чанарууд буюу домайн нэрийн бичлэг /DNS record/, домайн нэрийн насжилт, домайн нэрийн статус гэх мэт шинж чанарууд багтана.

Контендэд суурилсан шинж чанарууд /Content based feature extraction/: Энэ бүлэгт тухайн холбоос /URL/-ын контент буюу агуулгад суурилсан шинж чанарууд багтана. Жишээлбэл өөр хуудас руу дахин чиглүүлж байгаа эсэх, жава скриптын код ашиглан хулганы баруун товчыг идэвхгүй болгосон эсэх гэх мэт. Энэхүү бүлгийн шинж чанарууд тухайн холбоос /URL/ дээрх вэб кодыг бүрэн ачаалсаны дараа шинж чанаруудыг гаргаж авах тул бусад шинж чанаруудтай харьцуулахад бага зэргийн хүндрэлтэй.

ЁЁЁ Зурагт бүлэг тус бүрт бидний зүгээс шинээр нэмсэн шинж чанаруудаа “*” тэмдэглэгээгээр тэмдэглэв.

2-р хүснэгт. Холбоос /URL/-уудыг задлах шинж чанарууд

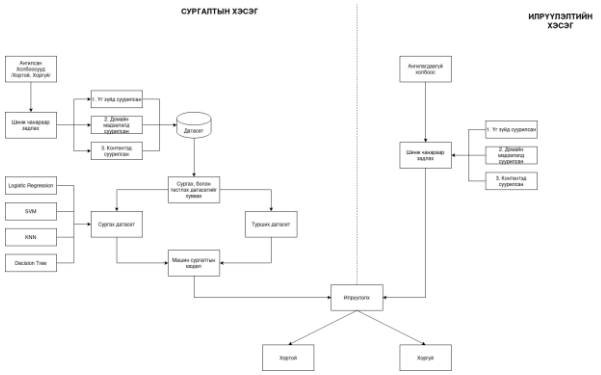
№	Group-н шинж чанар	Шинж чанар	Төрөл	Тайлбар
1	Lexical	URL_length	Тоон утга	Холбоосын уртыг тоолох
2		Hostname_length	Тоон утга	Хостын нэрийн уртыг тоолох
3		Path_length	Тоон утга	Замын уртыг тоолох
4		fd_lengthя	Тоон утга	First domain-ы уртыг тоолох
5		tld_length	Тоон утга	Top level domain-ы уртыг тоолох
6		count '-'	Тоон утга	Домайны дундуур зураасыг тоолох
7		count '@'	Тоон утга	"@" тэмдэгтийг тоолох
8		count '?'	Тоон утга	Тухайн домайн ашиглаж буй parameter-г тоолох
9		count '%'	Тоон утга	URL Encoding хийж байгааг шалгах (%20 зай авах encoding)
10		count '.'	Тоон утга	Цэгийг тоолж Sub Domain-г тодорхойлох
11		count','	Тоон утга	Таслалыг тоолох.
12		count'#'	Тоон утга	"#" тэмдэгтийг тоолох.
13		count'&'	Тоон утга	"&" тэмдэгтийг тоолох.
14		count'http'	Тоон утга	"http" тоолж хамгаалагдсан байдлыг шалгах
15		count'https'	Тоон утга	"https" тоолох хамгаалагдсан байдлыг шалгах
16		count'digits'	Тоон утга	Зөвхөн цифрыг тоолох
17		count'www'	Тоон утга	"www" тоолох
18		count'letters'	Тоон утга	Зөвхөн үсэг тоолох
19		count'dir'	Тоон утга	Хавтас тоолох
20		short_url	Логик	Хураангуйлсан url шалгах
21		use_of_ip	Логик	IP ашигласан эсэхийг шалгах
22		*Has keyword 'client'	Логик	"client" түлхүүр үг байгаа эсэх
23		*Has keyword 'admin'	Логик	"admin" түлхүүр үг байгаа эсэх
24		*Has keyword 'server'	Логик	"server" түлхүүр үг байгаа эсэх
25		*Has keyword 'login'	Логик	"login" түлхүүр үг байгаа эсэх
26		*Shannon entropy	Тоон утга	Үг зүй дээр тулгуурласан хортой байх магадлал
27	Domain-based	DNS Record	Логик	DNS бичлэг
28		Website traffic	Логик	Вебийг ачаалуулж байгаа эсэх
29		Age of domain	Тоон утга	WHOIS database, домайны насжилт
30		End period of domain	Логик	Домайн нэрийн хугацаа дууссан эсэхийг шалгах
31		*Status of domain	Тоон утга	Whois дээрх домайны статусыг мөрийг тоолох
32	Content-based	Iframe redirection	Логик	HTML Iframe bar ашиглаж харагдахгүй болгосон эсэх
33		Status Bar Customization	Логик	Худал веб харуулж байгаа эсэх
34		Disabled rigth click	Логик	JS rigth click button-г идэвхигүй болгосон эсэх
35		Website forwarding	Логик	Өөр веб хуудас руу шилжиж байгаа эсэх
36		*Count	Тоон утга	Redirect хийж байгаа домайныг тоолох

Өөрсдийн нэмсэн шинж чанаруудыг * тэмдэгээр тэмдэглэв.

C. Аргачлал

Бидний хийсэн судалгааны ажил нь сургалтын хэсэг болон илрүүлэлтийн хэсэг гэсэн үндсэн 2 хэсгээс бүрдэнэ. Сургалтын хэсэгт бид Монгол холбоос /URL/-уудаар өргөтгөсөн өгөгдлийн багц /Dataset/ оруулж, нэмж тодорхойлсон 3 бүлэг бүхий 36 шинж чанаруудаар холбоос /URL/ бүрийг задалж /Feature Extraction/, эцсийн өгөгдлийн багцаа үүсгэнэ. Улмаар сонгосон машин сургалтын алгоритмууд ашиглан моделоо сургаж, илрүүлэлтийн хувийг шалгана. Ингэхдээ сургах болон шалгах өгөгдлийн багцын харьцаа 70% болон 30% байхаар хуваана.

Илрүүлэлтийн хэсэгт шинэ холбоос /unknown URL/ оролт болгон авч, түүнийг тодорхойлсон 3 бүлэг бүхий шинж чанаруудаар задалж, дараа нь сургаж бэлтгэсэн моделийг ашиглан хортой эсвэл хоргүй гэж ангилна.



3-р зураг. Бүтцийн схем

VI. УР ДҮН

Үр дүнг тооцоолохдоо доорх хүчин зүйлсийг тусгаж үзнэ.

- TP хортой холбоос /URL/-г зөв тодорхойлсон тоо
- TN хоргүй холбоос /URL/-г зөв тодорхойлсон тоо
- FP хоргүй холбоос /URL/-г буруу тодорхойлсон тоо
- FN хортой холбоос /URL/-г буруу тодорхойлсон тоо

3-р хүснэгт. Confusion Matrix

	Таамагласан хортой URL	Таамагласан хоргүй URL
Бодит хортой URL	TP	FN

Бодит хоргүй URL	FP	TN

Ерөнхий нарийвчлал /Accuracy/ нь программын зөв ажилласан хувь юм.

$$\text{Ерөнхий нарийвчлал} = \frac{TP+TN}{TP+FN+FP+FN} \times 100\% \quad (1)$$

Precision нь эерэг утгуудын хувьд хортой холбоос /URL/-г зөв тодорхойлсон хувь юм.

$$Precision = \frac{TP}{TP+FP} \times 100\% \quad (2)$$

Recall нь үнэн зөв утгуудын хувьд хортой холбоос /URL/-г зөв тодорхойлсон хувь юм.

$$Recall = \frac{TP}{TP+FN} \times 100\% \quad (3)$$

F1 score нь Precision болон Recall утгуудын гармоник дундаж юм. F1 score нь их байх тусам тухайн алгоритм сайн гэсэн үг.

$$F1\ score = \frac{2 \times Precision \times Recall}{Precision+Recall} \quad (4)$$

FPR - False Positive Rating нь худал дохиоллын түвшин юм.

$$FPR = \frac{FP}{FP+TN} \times 100\% \quad (5)$$

Өгөгдлийн багц /Dataset/ дахь холбоос /URL/-уудыг шинж чанараар задалж, машин сургалтын моделоо сургаж бэлдсэний дараа ялгаатай алгоритмууд дээр туршилт хийж үр дүнг гаргасан бөгөөд доорх хүснэгтүүдэд үр дүнг харуулав.

Бид эхний байдлаар 4670 ширхэг өгөгдлийн багц (Dataset) дээр холбоос (URL)-н 21 шинж чанарыг задлан туршилтуудаа явуулсан бөгөөд машин сургалтын моделоо нийт өгөгдлийн багцын 30% дээр сургаж, 70% дээр шалгаж үзсэн. Үр дүнд нь Random Forest алгоритмын оновчлолын хувь (Accuracy) 89.79% -тай гарсан.

4-р хүснэгт. Үр дүнгийн хүснэгт 1

Сургах болон, шалгах харьцаа	**Машин сургалтын алгоритм**	**Зөв ажилласан хувь /Accuracy/**	**Өгөгдлийн багц (Dataset) хэмжээ**
Сургах 30% Шалгах 70%	Logistic regression	77.5%	4670 ширхэг
Сургах 30% Шалгах 70%	Decision Tree	86.74%	4670 ширхэг
Сургах 30% Шалгах 70%	Random Forest	**89.79%**	4670 ширхэг

Дээрх хүснэгтэд 4670 ширхэг өгөгдлийн багц дээр 21 шинж чанарыг задлан машин сургалтын моделийг 30 болон 70 хувийн харьцаатай сургаж шалгасан үр дүнг харуулав.

Үүний дараа нийт өгөгдлийн багцын 70% дээр моделоо сургаж, 30% дээр шалгаж үзсэн бөгөөд үр дүнд нь бүх алгоритмын оновчлолын хувь (Accuarcy) нэмэгдсэн бөгөөд энэ үед Random Forest алгоритм 89.85% ажилласан бөгөөд 30:70 харьцаатай сургаж шалгасантай харьцуулахад оновчлолын хувь (Accuracy) 0.06%-иар өссөн.

5-р хүснэгт. Үр дүнгийн хүснэгт 4

Сургах болон, шалгах харьцаа	**Машин сургалтын алгоритм**	**Зөв ажилласан хувь /Accuracy/**	**Өгөгдлийн багц (Dataset) хэмжээ**
Сургах 70% Шалгах 30%	Logistic regression	77.65%	4670 ширхэг
Сургах 70% Шалгах 30%	Decision Tree	88.37%	4670 ширхэг
Сургах 70% Шалгах 30%	Random Forest	**89.85%**	4670 ширхэг

Дээрх хүснэгтэд 4670 ширхэг өгөгдлийн багц дээр 21 шинж чанарыг задлан машин сургалтын моделийг 70 болон 30 хувийн харьцаатай сургаж шалгасан үр дүнг харуулав.

Нийт 21 шинж чанар дээр үндэслэн туршилтуудаа явуулсаны дараа үүн дээр 3 шинэ шинж чанар нэмж туршив. Үр дүнд нь 21 шинж чанар дээр үндэслэн ажилласан оновчлолын хувь бүх алгоритм дээр тодорхой хувиар өссөн бөгөөд энэ үед Random Forest алгоритмын оновчлолын хувь (Accuracy) 90.67% болж өмнөх 21 шинж чанар дээрх оновчлолын хувиас 0.82%-иар өссөн.

6-р хүснэгт. Үр дүнгийн хүснэгт 3

Сургах болон, шалгах харьцаа	**Машин сургалтын алгоритм**	**Зөв ажилласан хувь /Accuracy/**	**Өгөгдлийн багц (Dataset) хэмжээ**
Сургах 70% Шалгах 30%	Logistic regression	80.24%	4670 ширхэг
Сургах 70% Шалгах 30%	Decision Tree	89.23%	4670 ширхэг
Сургах 70% Шалгах 30%	Random Forest	**90.67%**	4670 ширхэг

Дээрх хүснэгтэд 4670 ширхэг өгөгдлийн багц дээр 24 шинж чанарыг задлан машин сургалтын моделийг 70 болон 30 хувийн харьцаатай сургаж шалгасан үр дүнг харуулав.

Дээрх үр дүнгүүдийг гаргаж авсаны дараа бид цуглуулсан нийт өгөгдлийн сан буюу гадаад болон Монгол холбоос (URL)-с бүрдэх 450176 ширхэг өгөгдлийн багц дээр ажиллуулж дараах үр дүнг үзүүлэв.

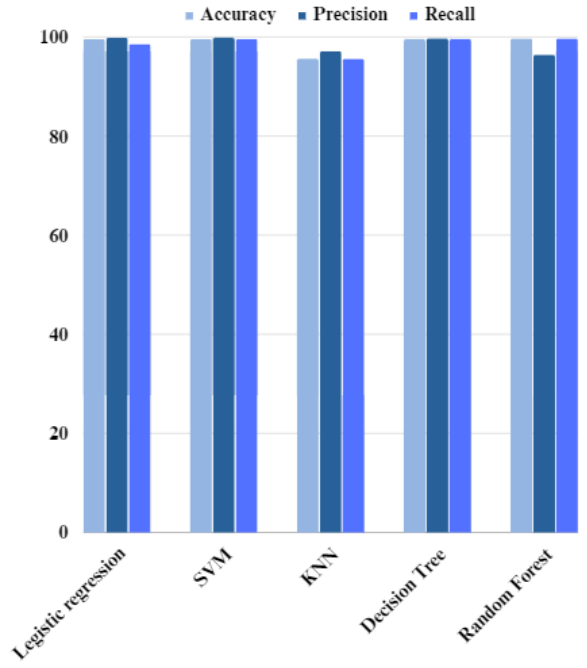
Үүнд нийт холбоос (URL)-н 36 шинж чанар дээр тулгуурлан, хамгийн өндөр оновчлолын хувь үзүүлэх боломжтой, тохирох машин сургалтын алгоритмуудыг ашиглан 450176 ширхэг өгөгдлийн багцын 70% -ийг сургаж, 30% дээр шалгасан.

Үр дүнд Random Forest алгоритм хамгийн өндөр оновчлолын хувь (Accuracy) буюу 99.70% -тай ажилласан ба SVM (Support Vector Machine) алгоритм 99.61% оновчлолын хувь (Accuracy)-тай сайн ажилласан.

7-р хүснэгт. Үр дүнгийн хүснэгт 4

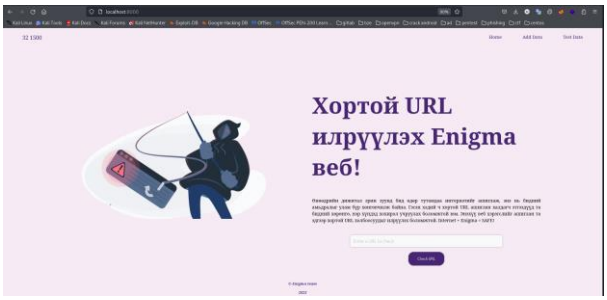
Сургах болон, шалгах харьцаа	**Машин сургалтын алгоритм**	**Зөв ажилласан хувь /Accuracy/**	**Precision**	**Recall**	**Өгөгдлийн багц (Dataset) хэмжээ**
Сургах 70% Шалгах 30%	Logistic regression	99.59%	99.88%	98.58%	450176 ширхэг
Сургах 70% Шалгах 30%	SVM	99.61%	99.87%	99.61%	450176 ширхэг
Сургах 70% Шалгах 30%	KNN	95.61%	97.14%	95.61%	450176 ширхэг
Сургах 70% Шалгах 30%	Decision Tree	99.58%	99.67%	99.58%	450176 ширхэг
Сургах 70% Шалгах 30%	Random Forest	**99.70%**	96.44%	99.7%	450176 ширхэг

Дээрх хүснэгтэд 450,176 ширхэг өгөгдлийн багц дээр 36 шинж чанарыг задлан машин сургалттын моделийг 70 болон 30 хувийн харьцаатай сургаж шалгасан үр дүнг харуулав.

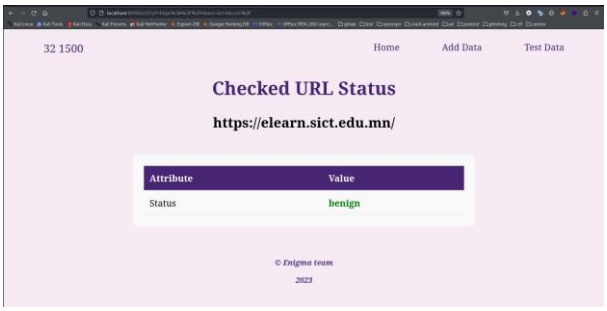


4-р зураг. Илрүүлэлтийн хувь. (*График байдлаар*)

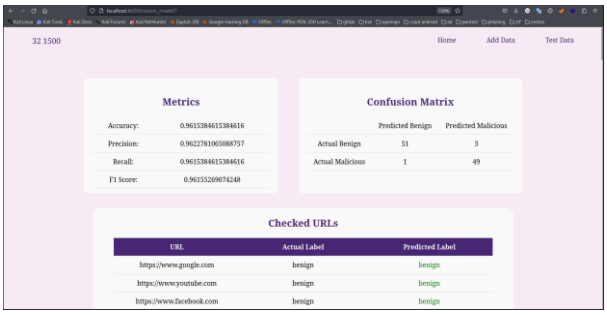
Улмаар бид гаргасан үр дүн дээрээ тулгуурлан, хэрэглэхэд хялбар, өнгө үзэмж сайтай веб хуудсанд суурилсан хортой холбоос /URL/-г илрүүлэх хэрэгсэл хөгжүүлсэн бөгөөд ерөнхий харагдах байдал, ажиллагааг зурагт харуулав.



5-р зураг. Хортой URL илрүүлэх Enigma веб



6-р зураг. Хортой URL илрүүлэх Enigma веб (*шинэ URL илрүүлсэн байдал*)



7-р зураг. Хортой URL илрүүлэх Enigma веб (*илрүүлэлтийн хувийг дүрсэлж харуулсан байдал*)

VII. ДҮГНЭЛТ

Энэхүү судалгааны ажилд машин сургалтын арга ашиглан хортой холбоос /URL/ илрүүлэх ажлыг хийж гүйцэтгэсэн бөгөөд, өгөгдлийн багц /dataset/, мөн шинж чанарууд нь ерөнхий нарийвчлал /accuracy/-д шууд нөлөөлж байсан. Цаашид уг ажлыг веб хуудсанд суурилсан холбоос /URL/-н хортой байх магадлалыг график байдлаар харуулах байдлаар илүү нарийн хөгжүүлэх боломжтой. Мөн контентод суурилсан бүлгийн шинж чанаруудыг нэмж хөгжүүлэн ашиглаж, улмаар орж ирсэн URL холбоосыг задалж тухайн веб хуудас ямар төрлийн веб хуудас болохыг тодорхойлох, нийт шинж чанар машин сургалтын алгоритмын үндсэн ажиллагааг ашиглан аливаа веб сервисийн лог бүртгэлийг хортой эсвэл хоргүй гэж ангилах, спам и-мэйлийг ангилах зэрэг байдлаар хөгжүүлэх бүрэн боломжтой.

НОМ ЗҮЙ

[1] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang, “An empirical analysis of phishing blacklists,” in Proceedings of Sixth Conference on Email and Anti-Spam (CEAS), 2009.

[2] C. Seifert, I. Welch, and P. Komisarczuk, “Identification of malicious web pages with static heuristics,” in Telecommunication Networks and Applications Conference, 2008. ATNAC 2008. Australasian. IEEE, 2008, pp. 91–96.

[3] C. Do Xuan, H. D. Nguyen, and T. V. Nikolaevich, ‘‘Malicious URL detection based on machine learning,’’ Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 1, pp. 148–153, 2020, doi: 10.14569/ijacsa.2020.0110119

[4] M. Aldwairi and R. Alsalman, ‘‘MALURLS: A lightweight malicious website classification based on URL features,’’ J. Emerg. Technol. Web Intell., vol. 4, no. 2, pp. 128–133, May 2012, doi: 10.4304/JETWI.4.2.128-133.

[5] Alexa | Web Information Company’s Website. Accessed: Oct. 18, 2021.[Online]. Available: https://www.alexa.com

[6] PhishTank—Join the Fight Against Phishing. Accessed: Jan. 1, 2022.[Online]. Available: https://www.phishtank.com

[7] A. Subasi, E. Molah, F. Almkallawi, and T. J. Chaudhery, ‘‘Intelligent phishing website detection using random forest classifier,’’ in Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA), Jun. 2018, pp. 1–5, doi: 10.1109/ICECTA.2017.8252051.

[8] M. Rami, M. Lee, and T. Fadi. (2015). UCI Machine Learning Repository: Phishing Websites Data Set. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/phishing+websites

[9] X. Yu, ‘‘Phishing websites detection based on hybrid model of deep belief network and support vector machine,’’ IOP Conf. Earth Environ.Sci., vol. 602, no. 1, Nov. 2020, Art. no. 012001, doi: 10.1088/1755-1315/602/1/012001.

[10] Sahingoz, Ozgur Koray, et al. "Machine learning based phishing detection from URLs." *Expert Systems with Applications* 117 (2019): 345-357.

[11] D. Sahoo, C. Liu, S.C.H. Hoi, “Malicious URL Detection using Machine Learning: A Survey”. CoRR, abs/1701.07179, 2017 Japan, p. 301, 1982].

[12] Lkhagva, Odonchimeg. (2022). КИБЕР ГЭМТ ХЭРГИЙГ МАШИН СУРГАЛТЫН АРГААР ТААМАГЛАН ИЛРҮҮЛЭХ НЬ.

[13] https://ikon.mn/n/2y8j

МИНИ ХҮЛЭМЖИНД ХЭРЭГЛЭХ АППЛИКЕЙШН ХӨГЖҮҮЛЭЛТ

[1]Б.Алтаншагай, [2]Г.Ганчимэг

[1,2]Компьютерын ухаан салбар, Мэдээлэл, Холбооны Технологийн Сургууль, ШУТИС, Монгол улс

[1]altanshagaibattulga.ba@gmail.com, [2]ganaa@must.edu.mn

***Хураангуй*— Манай орны агаарын бохирдол жилээс жилд нэмэгдэж буй энэ үед модыг их хэмжээгээр тарьж ургуулах нь чухал юм. Мод тарьж ургуулах нь экологийн тэнцвэрт байдлыг бий болгож хүлэмжийн хийг багасгана. Мод тарих нь чухал боловч түүнийг амжилттай ургуулах нь илүү чухал юм. Бид энэ өгүүлэлд гэрийн нөхцөлд мод үрслүүлж, ургуулах боломжтой мини хүлэмжийг түүнийг удирдах аппликейшны хамт хөгжүүлж хэрэглэх боломжийн талаар өгүүлнэ.**

Түлхүүр үг*— *Мини, хүлэмж, мод, үрслүүлэх, аппликейшн

I. Удиртгал

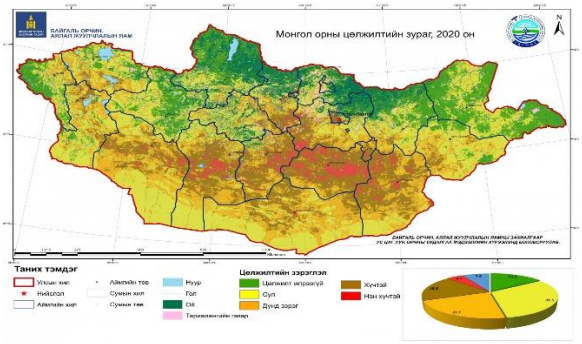
Монгол улсын нийт хүн амын бараг тал хувь нь оршин суудаг Улаанбаатар хот нь дэлхийн хамгийн агаарын бохирдол ихтэй нийслэл хотуудын нэг юм [1].

Зураг 1. Улаанбаатар хотын агаарын бохирдол [2]

Манай улсын агаарын бохирдлын гол эх үүсвэр нь гэр хорооллын айл өрхүүдийн яндангийн утаа болон аж ахуйн нэгжүүдийн халаалтын зуухны яндангийн утаа 80 орчим хувь эзэлдэг бол тээврийн хэрэгслийн яндангийн утаа 10 хувь, дулааны цахилгаан станцын яндангийн утаа 6 хувь эзэлдэг байна. Улаанбаатар хотын нийт хүн амын 60 гаруй хувь гэр хороололд амьдарч байна [3]. Жилийн хамгийн хүйтэн сарууд болох 12 сард PM2.5 бохирдлын өдрийн дундаж шоо метрт 687 микрограм хүрч байгаа нь ДЭМБ-ын зөвлөж буй аюулгүй төвшнөөс 27 дахин их байна [1, 4].

Агаарын бохирдолтой тэмцэх гол хүчин зүйлүүдийн нэг нь мод их хэмжээгээр тарьж, ургуулах юм. Үүний хүрээнд дэлхийн уур амьсгалын өөрчлөлтийн нөлөөллийг бууруулах, ой, усны нөөцийг хамгаалж, нэмэгдүүлэх, экологийн тэнцвэрт байдлыг хангах зорилгоор “Тэрбум мод” үндэсний хөдөлгөөн манай оронд сүүлийн жилүүдэд өрнөж байна [5]. Монгол Улсын нийт газар нутгийн 76.9 хувь нь цөлжилтөд нэн хүчтэй өртсөн байна гэсэн тооцоо, судалгаа бий [6].

Модыг их хэмжээгээр тарьж ургуулбал цөлжилтөд нэн хүчтэй өртсөн 129 сая га талбайг 4 хувиар бууруулах тооцоо байдаг. Манай газар нутгийн 7.9 хувь нь ойгоор бүрхэгдсэн байдаг [7] ба модыг зөв тарьж ургуулснаар хүлэмжийн хийн ялгарлыг бууруулахад тустай юм.

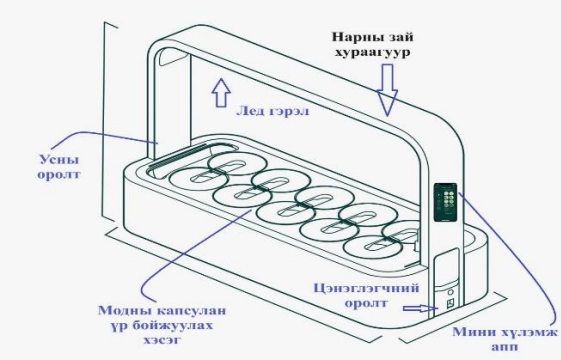


Зураг 2. Цөлжилт явагдаж буй байдал [8]

II. Мини хүлэмж

Манай орны хувьд мод үржүүлгийн газрууд цөөн тоогоор үйл ажиллагаагаа явуулдаг ба эдгээр газрууд шинэ технологи аргачлалыг хараахан нэвтрүүлж, туршиагүй байна. Иймд бид тус судалгааны ажлаар иргэдэд мод болон модлог ургамлыг гэрийн нөхцөлд болон хашаандаа суулгаж, үрслүүлэн соёолуулахаас эхлүүлэн модны ургах бүхий л үйл явцыг тусган хэрхэн услах, арчлах зааварчилгаатай аппликейшнтэй хослож ажиллах мини хүлэмж боловсруулах технологийг гаргахыг зорьсон [9-13]. Ингэснээр илүү бүтээлч байдлаар модыг үндэслүүлж ургуулан байгаль орчноо дэмжих боломжтой юм. Эхний ээлжинд мини хүлэмж бүтээх шийдлийн загвар гарган зургийг боловсруулж 3 дугаар зурагт үзүүлсэн. Мөн мини хүлэмжийг бүтээхдээ усалгааг дээрээс биш доороос хийхээр тооцоолсон. Ингэж модны үрсэлгээг усалснаар байгаль дээр ургаж буй моднуудын нэгэн адилаар байгалийн аргаар усаа шингээж хурдан ургах боломжийг бүрдүүлнэ. Усны заагчийг усны хэсэгт байршуулснаар хэрэглэгч хэзээ услагаа шаардлагатай болохоо мини хүлэмжтэй хосолж ажиллах аппликейшнээрээ хянах боломж бүрдэнэ. Мөн 3 дугаар зураг дээр харагдаж буй бариултай төсөөтэй хэсэг нь доод талаараа лед

гэрлүүдийг байршуулж өгөх ба үүнээс хангалттай нарны гэрэл авч чадаагүй ургамлууд лед гэрлийн тусламжтай фотосинтез явуулах боломжийг бүрдүүлж өгнө. Уг бариул хэсгийн дээд хэсэгт нарны зайн хураагуур суулгаж өгснөөр уг төхөөрөмж нь цэнэглэгчний порттой байхаас гадна өөрөө өөрийгөө цэнэглэж хэрэглэгчийн оролцоог багасгаж өгнө.



Зураг 3. Шинээр бүтээх мини хүлэмжийн шийдэл

Тус шийдлийн хүрээнд капсуланд тухайн үрийг тусгай зориулалтын хөрсөнд суулгаж ургаж буй үйл явцад хяналт тавьж хэзээ услах шаардлагатай байдаг, тэр үеүдэд нь услах цагийн сэрүүлэг болоод тухайн ургамалд витаминжуулах, цэвэрлэгээ хийх, бордох өдрүүдийг календар дээрээ тусган өөрсдийн хийж буй аппликейшнээрээ дамжуулан тухайн ургамлын ургах үйл явцыг хянана. Мөн иргэдэд байгалиа хамгаалах, арчлах, хайрлах аргачлалыг түгээн дэлгэрүүлнэ. *Үрийг яагаад тус тусад нь байршуулж байгаа вэ?* гэхээр 10 өөр төрлийн ургамлыг хөрс, сорт өөрчлөгдөх боломжгүйгээр тарих ба тус ургамал нь зөвхөн өөрийнхөөрөө ургах боломжтой, дээрээс нь үүн дээр таг хийж өгснөөр ургамалд наалдах хортон шавьж нараас сэргийлэх ба чийгнээс үүсэх төрөл бүрийн өвчнүүдээс хамгаална. Бид тухайн мини хүлэмжийг бүтээх төсвийг олохын тулд инновацын шийдлийг санхүүжүүлдэг уралдаан тэмцээнд төслөө танилцуулж байгаа бөгөөд MonX үндэсний хөтөлбөрт бүтээлийн танилцуулгаа илгээсэн.

III. Аппликейшн хөгжүүлэлт

Бид мини хүлэмжинд зориулсан аппликейшн хөгжүүлж түүнд мод үрслүүлэх аргуудын онцлогуудыг тусгасан үйлдлүүдийг функц болгон бичиж байна. Мөн тусгай зориулалтын бордоо болоод үрийг суулгах капсулын хөгжүүлэлтийг хянах функцийг хийхийг зорьж байгаа. Жишээ нь: Модлог ургамлуудын өөрсдийн гэсэн ургах нөхцөл болон орчин, усжилтаас эхлэн бүхий л мэдээллийг ялгаатайгаар оруулж өгөх ба капсулыг мини хүлэмжний дотор байршуулан зундаа нарны гэрэлд өвөлдөө лед гэрэл тусган шаардлагатай гэсэн бордоо амин дэмүүдийг календар дээр тусгаж өгснөөр тухайн ургамал нь төвөггүй ургаж эхлэнэ. Мөн дан ганц модлог ургамал гэлтгүй гэрийн тасалгааны нөхцөлд ногоон сонгино, байцаа, яншуй гэх мэт эко ургамлыг тарьж ургуулан өөрсдийн өрхийн хэрэглээнд хэрэглэх боломжийг хангахыг зорьж нэмэлт функцүүдийг аппликейшндээ программчилж өгнө.

Зураг 4. Боловсруулж буй мини хүлэмж аппликейшны харагдах байдал

Эхний ээлжинд бид программын функцуудыг тодорхойлж аппликейшны загвараа боловсруулж эхний хөгжүүлэлтүүдийг хийж байна.

Дүгнэлт

Мини хүлэмж нь модыг үр хэлбэрээс нь ургаа мод хүртэл нь шаардлагатай бүхий л үеүдэд тухайн суулгасан үрийг таатай нөхцөлд үндэслүүлэн байгальд суулгах боломжтой үе хүртэл нь модлог ургамлуудыг үрслүүлнэ. Мөн мод арчлах аргачлалуудын мэдээллийг агуулсан аппликейшнтэй хосолж ажиллана. Түүнчлэн ургамал тарьж арчлан ургуулж буй хэн ч өөрийн тарьж буй ургамал нь амжилттай урган торниж байгааг харснаар байгаль орчноо хайрлах сэтгэлгээг бусдад түгээх болно.

Ном зүй

[1] https://www.iqair.com/world-air-quality-ranking

[2] https://www.nogoonhutuch.mn/a/179

[3] https://audit.mn/archive/wp-content/uploads/2018/10/tsewer-agaar-san.pdf

[4] https://aqicn.org/city/ulaanbaatar

[5] https://terbummod.mn/

[6] https://www.montsame.mn/ru/read/298349

[7] Байгаль орчин, Аялал жуулчлалын яам, 2021 он https://www.mne.mn/?p=15177.

[8] https://isee.mn/n/51196

[9] What is thermal imaging, https://www.pyrosales.com.au/blog/thermal-imaging/what-is-thermal-imaging-and-how-important-is-it-in-temperature-measurement/

[10] https://www.google.com/url?sa=i&url=https%3A%2F%2Fflir.custhelp.com%2Fci%2Ffattach%2Fget%2F119551%2F0%2Ffilename%2FSolarPanel-PV-Inspection-Radiometry.pdf&psig=AOvVaw0DJy14jafeGRMUjQdEqwBY&ust=1679098916408000&source=images&cd=vfe&ved=0CA4QjhxqFwoTCIjQ5YfZ4f0CFQAAAAAdAAAAABAI

[11] Thermal imaging camera and night vision, https://pulsar-nv.com/useful-information/thermal-vs-night-vision/

[12] Utilities inspection, https://www.dslrpros.com/thermal-drones.html

[13] https://www.facebook.com/people/%D0%94%D0%B0%D1%88%D0%B1%D0%B0%D1%82%D1%8B%D0%BD-%D0%A5%D0%B0%D1%82%D0%B0%D0%BD%D0%B1%D0%B0%D0%B0%D1%82%D0%B0%D1%80/100063756511652/

МУЛЬТИМЕТРИЙН ХЭРЭГЛЭЭНД ЗОРИУЛСАН ӨРГӨТГӨСӨН БОДИТ БАЙДЛЫГ ИДЭВХЖҮҮЛСЭН МЭДЭЭЛЛИЙН ШИЛ

Баянмөнх Батболд [1], Дэлгэр Зуунбаатар [2], Тэнгис Цэрэндондог
[1]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны Технологийн Сургууль, Электроникийн салбар
Холбоо барих зохиогчийн и-мэйл хаяг:ghoul0311@gmail.com[1], dek.623713@gmail.com[2], tengis@must.edu.mn

***Хураангуй*: Энэхүү судалгааны гол зорилго нь нүдний шил дээр мультиметрийн өгөгдлийг харуулах явдал юм. Үүнийг хэрэгжүүлэхийн тулд B35T+Bluetooth мультиметрийг HC-05 Bluetooth модультай холбож мэдээлэл дамжуулах протоколын судалгааг хийх шаардлагатай юм. Энэхүү судалгаа нь AT горим болон AT командуудын судалгааг багтаасан бөгөөд Bluetooth модулийг зохицуулдаг протокол болон түүний үндсэн ойлголтуудыг ойлгоход чиглэв. Мультиметрийн өгөгдлийг дамжуулахаас гадна тухайн өгөгдлийг хүний нүдэнд харагдах боломжтой болгох үүднээс гэрлийн хугарал болон гэрэл ойлголт, шингээлт болон тархах загваруудын судалгааг хийсэн болно. Эцэст нь график дэлгэц болох OLED дэлгэцийг програмчилж тухай дэлгэц дээрх өгөгдлийг мэдээллийн шил дээр гаргах замаар хэрэглэгчийг ажуулгүй хэмжилт хийх нөхцөлийг бүрдүүлсэн төхөөрөмжийн загварыг гарган авсан болно.**

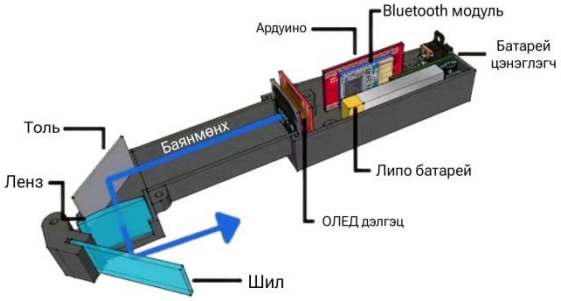
Түлхүүр үг – нүдний шил, bluetooth, arduino, OLED, Lipo battery, мэдээллийн протокол

I. УДИРТГАЛ

Технологийн инновац нь бодит ертөнцийн хэрэглээтэй уялдаа холбоотой байдаг эрин үед бид мультиметрийн ердийн хэрэглээг өөрчлөхөд чиглэсэн алсын хараатай шийдэл болох "Мэдээллийн шил"-ийг нэвтрүүлэх ер бусын аялалд гарч байна. Уламжлалт мультиметрийн хэрэглэгчид төхөөрөмж дээрх хэмжилтийг уншихын тулд ажлаасаа түр зуур харцаа шилжүүлдэгт гол бэрхшээл оршдог [1, 2]. Хэдийгээр гэм зэмгүй мэт санагдах энэ үйлдэл нь ихэвчлэн анхаарал сарниулахад хүргэдэг бөгөөд санамсаргүйгээр ажуулгүй байдлын ноцтой эрсдэлд хүргэж болзошгүй юм. Өндөр хүчдэлийн төхөөрөмж дээр ажиллаж байгаа хүмүүсийн хувьд үр дагавар нь маш аймшигтай бөгөөд гэмтэл бэртэл, бүр үхэлд хүргэдэг. Мэдээллийн шилний бодит хэрэглээг доорх Зурагт 1-д үзүүлэв.

1-р зураг. Мэдээллийн шилний бодит хэрэглээ

Энэ төсөлд бид B35T+ Bluetooth мультиметрийг сонгож авч ашигласан [3, 5]. Bluetooth модуль дээр хийгдсэн гол судалгаа нь AT горим болон AT командуудыг нарийн судалснаар Bluetooth модулийн протоколыг тайлах судалгааны ажлын чухал хэсэг болж байна. OLED дэлгэц нь судалгааны нэг тулгуур бөгөөд мультиметрийн өгөгдлийг дэлгэц дээр дүрслэх чухал үүрэгтэй юм [6, 7]. Бидний бүтээж буй мэдээллийн шилний ажиллах ерөнхий загварыг доорх Зураг 2-т үзүүлэв.



2-р зураг. Мэдээллийн шилний мэдээлэл дамжуулалт

Инженер хүний ажуулгүй ажиллах нэг нөхцөл нь хэмжилтийн багажаас ирж буй мэдээллийг ямар нэгэн саадгүй хүлээн авах явдал юм. Хамгийн түгээмэл хэрэглэгддэг багаж нь мультиметр юм [1, 3, 5]. Хэмжилт хийх явцад инженер мультиметрийн дэлгэц руу байнга харах хүндрэл гардаг. Бидний систем энэхүү ажлыг хялбарчлах болно. Bluetooth модультай мультиметр нь хэмжилтийн утгаа мэдээллийн шил дэх Bluetooth модуль руу илгээнэ. Энэхүү өгөгдлийг Arduino контроллер хүлээн авч OLED дэлгэц дээр хэвлэнэ. Дэлгэцээс гарч буй гэрэл гэрлийн хугарах, ойх болон цацрах физик үндсэн дээр тулгуурлан шингээж шил дээр дүрслэгдэнэ. Энэхүү өгөгдлийг инженер харах боломжтой юм.

II. МЭДЭЭЛЛИЙН ШИЛД ХЭРЭГЛЭГДЭХ ЭЛЕМЕНТҮҮДИЙН СУДАЛГАА

Бидний судалгаанд гол хэрэглэгдэх элементүүд бол OLED 0.66, Arduino Nano, HC05 bluetooth модуль, Lipo баттерей болно [9 - 11].

OLED дэлгэц нь 64x48 пикселийн нягтаршилтай 0.66 инчийн хэмжээтэй юм [6]. LCD-ээс ялгаатай нь OLED нь шууд гэрэл цацруулдаг тул арын гэрэлтүүлэг шаарддаггүй. Үүний үр дүнд илүү гүн хар өнгө, илүү сайн тодосгогч харьцаа, нимгэн дэлгэцийн модулиуд бий болно. OLED технологийн ачаар дэлгэц нь зөвхөн асаж байгаа пикселийн эрчим хүчийг зарцуулдаг. Эдгээр дэлгэцүүд нь ихэвчлэн I2C эсвэл SPI зэрэг цуваа интерфейсүүдийг хэрэглэн микроконтроллертой холбогддог. Бидний хэрэглэж буй дэлгэцийг доорх зурагт үзүүлэв.

3-р зураг. OLED 066 дэлгэц

Энэхүү дэлгэц нь 3.7В тэжээлийг хэрэглэдэг ба зарцуулдаг гүйдлийн хэмжээн нь 21 мА байдаг. Ажиллах температур нь -40°C –ээс +85°C хооронд байна.

Arduino Nano нь ATmega328P микроконтроллер дээр суурилсан жижиг, олон талт микроконтроллерийн юм. Нано нь нэлээд авсаархан учир хязгаарлагдмал зайтай төслүүдэд тохиромжтой. Энэ нь ойролцоогоор 45 мм x 18 мм хэмжээтэй байна. Arduino нь 14 дижитал оролт/гаралтын хөл, 8 аналог оролт, 6 импульсийн өргөн модуляц (PWM) хөлтэй. ATmega328P нь 16 МГц давтамжтайгаар ажилладаг бөгөөд 32 кБ флаш санах ойтой, өгөгдөл хадгалахад 2 кБ SRAM мөн өгөгдөл хадгалахад зориулагдсан 1 КБ EEPROM-той юм. Зураг 4-т Arduino Nano-г үзүүлэв.

4-р зураг. Ардуйно Нано

OLED дэлгэц нь Arduino Nano-той I2C интерфейс ашиглан холбогдоно.

HC05 Bluetooth 2.0 ба EDR дээр суурилсан модуль ба микроконтроллер болон бусад төхөөрөмжүүдийн хооронд утасгүй холболт хийхэд ашиглагддаг төхөөрөмж юм [7]. Модуль нь ихэвчлэн 3.3V дээр ажилладаг боловч 5V-д тэсвэртэй оролтыг дэмждэг. HC-05 модулийн AT командыг ашиглан тохируулж, удирдаж болно. Эдгээр командууд нь цуваа интерфейсээр илгээгдэж, тохиргоо болон горимыг өөрчлөх боломжийг олгоно. Доорх Зураг 5-д HC05 Bluetooth модулийг үзүүлэв.

5-р зураг. HC05 Bluetooth модуль

HC05 Bluetooth модулийг Arduino Nano-той цуваа интерфейс болох USART-р холбогдоно.

III. AT КОМАНД БОЛОН BLUETOOTH МОДУЛИЙН ПРОТОКОЛ

"AT горим" гэдэг нь ихэвчлэн AT (Анхаарал) командыг хүлээн авах боломжийг олгодог төхөөрөмжийн ажиллах горимыг хэлдэг. Энэ горимыг ихэвчлэн модем, микроконтроллер эсвэл команд дээр суурилсан интерфейстэй холбооны модулиуд зэрэг төхөөрөмжүүдэд ашигладаг. AT командыг ихэвчлэн UART (Universal Asynchronous Receiver/Transmitter) гэх мэт цуваа интерфейсээр дамжуулан текст мөр хэлбэрээр илгээдэг. Тушаалд суурилсан харилцан үйлчлэл: AT горимд төхөөрөмж нь урьдчилан тодорхойлсон форматаар тодорхой AT командуудыг хүлээн авахыг хүлээдэг. Эдгээр командыг параметрүүдийг тохируулах, мэдээлэл хайх, төхөөрөмжийн ажиллагааг хянахад ашиглаж болно. AT командуудыг явуулахаасаа өмнө эхлээд AT горимд оруулах хэрэгтэй.

Бидний судалсан энэ AT командуудыг доорх Хүснэгт 1-д үзүүлэв.

СУДАЛСАН AT КОМАНДУУД,

1-р хүснэгт

AT+ROLE1	Эхлээд модулийг төв рүү тохируулах
AT+RESET	Дахин тохируулах
AT+SHOW1	Bluetooth нэрийг харуулах
AT+IMME0	Автоматаар холбогдох
AT+FILT0	Төхөөрөмжүүдийг хайх
AT+DISC?	Төхөөрөмжүүдийг харуулах

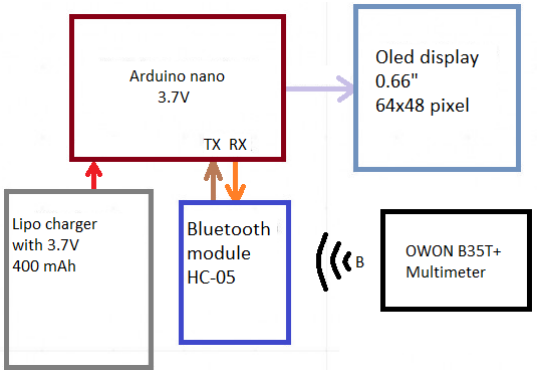
Дээрх AT командуудыг bluetooth модуль болон bluetooth Multimeter хоёрыг хооронд нь холбоход ашиглагдах командууд юм. Bluetooth модулийн протоколын хувьд OWON B35T+ multimeter-ын ямар дохио явуулж байгааг задалж ойлгосон болно. Өгөгдлийн бүтцийг доорх Зураг 6-д үзүүлэв.

6-р зураг. Дамжуулж буй өгөгдлийн бүтэц

Анхны цифр болох усан цэнхэр өнгөтэй тоо нь эерэг болон сөрөг тэмдэгтийг илэрхийлдэг. Хэрвээ эхний цифр нь 43 гэж орж ирвэл эерэг тэмдэгт харин 45 гэж орж ирвэл сөрөг тэмдэгтийг илэрхийлдэг. Дараагийн 4 цифр нь орж ирж буй утгыг илэрхийлнэ (0000-9999). Ногоон дээр бичигдсэн 32 гэсэн тоо нь зайг илэрхийлдэг (space). Үзмэн ягаан дээр байх 52 гэсэн тоо нь цэгийн байрлалыг илтгэдэг. Улбар шар дээр байх цифр нь хэрвээ 49 бол DC auto mode, 17 - DC manual mode, 41 - AC auto mode, 09 - AC manual mode байна. Цагаан дээр байх цифр нь null. Улаан дээр байх хоёр цифр нь 64 болон 128 байвал mV-ийг илэрхийлнэ (0 128 = V) (0 32 = Ohm) (32 32 = KOhm) (16 32 = MOhm) (0 64 = A) (64 64 = mA) (128 64 = uA) (0 2 = Grad) (0 1 = Fahrenheit) (0 8 = HZ) гэж тус тус нэгжийг илэрхийлнэ. Ягаан дээр байх цифр нь тодорхойгүй. Харин хамгийн сүүлийн хоёр цифр нь дараагийн мөрлүү шилжүүлэх тоог илэрхийлнэ.

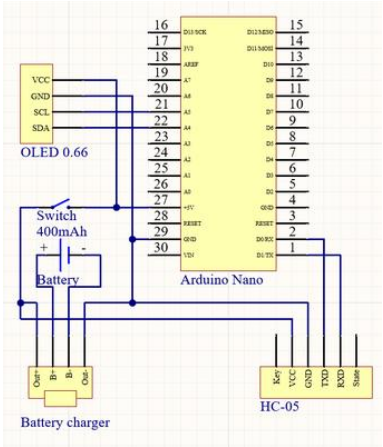
IV. СИСТЕМИЙН БҮТЭЦ БОЛОН ПРОГРАММЫН АЛГОРИТМ

Бидний бүтээсэн мэдээллийн шилний бүтцийн схемийг доорх Зураг 7-д үзүүлэв.



7-р зураг. Системийн бүтэц

Бидний хийсэн төхөөрөмжийн зарчмын схемийг Зураг 8-д үзүүлэв.



8-р зураг. Системийн зарчмын схем

Чадлын тооцоо хийхдээ бид эхлээд Arduino nano, bluetooth модуль болон ОЛЕД дэлгэцийн тус бүрийнх нь техникийн үзүүлэлтийг нь судалсан.

$$P_{OLED} = 21\text{mA} * 3.7 = 77.7\text{mW} \quad (1)$$

$$P_{BL} = 50\text{mA} * 3.7 = 185\text{mW} \quad (2)$$

$$P_{ard} = 19\text{mA} * 3.7 = 70.3\text{mW} \quad (3)$$

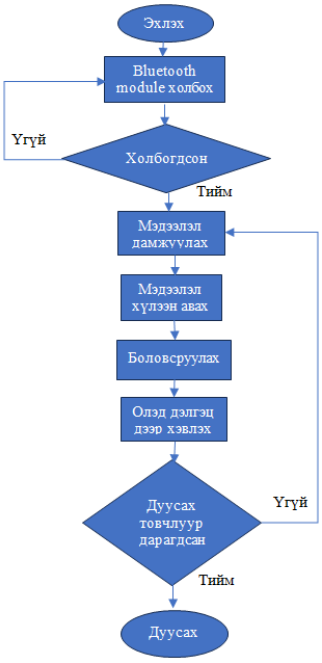
$$P_{all} = P_{OLED} + P_{BL} + P_{ard} = 333\text{mW} \quad (4)$$

$$P_{battery} = 400\text{mA} * 3.7 = 1480\text{mW} \quad (5)$$

$$work\ hour = \frac{1480}{333} \approx 4 \quad (6)$$

Уг төхөөрөмж нь тасралтгүй ажиллалаа гэхэд хамгийн ихдээ 4 цаг гаруй ажиллах бүрэн чадалтай гэдгийг бид тооцооллоо.

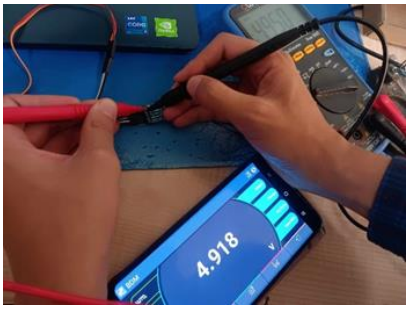
Төхөөрөмжийн программын алгоритмыг Зураг 9-д үзүүлэв.



9-р зураг. Программын алгоритм

V. ТУРШИЛТ БА ҮР ДҮН

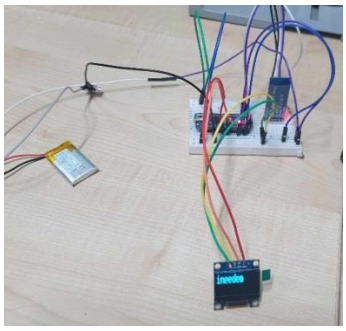
Бид эхлээд B35T+ bluetooth мультиметрийг гар утастай холбож өгөгдлийг нь авч харж үзсэн бөгөөд энд бага зэргийн хугацааны алдагдалтай байгааг тодорхойлсон. Үүнийг Зураг 10-т үзүүлэв.



10-р зураг. Мультиметр болон гар утас хоёрын хоорондох холболтын туршилт

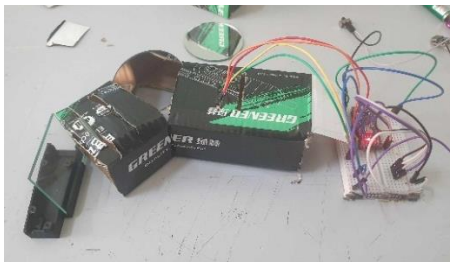
Бидний сонгож авсан multimeter-ийг бүтээсэн компани нь multimeter-ийн утгыг авч болох аппликейшн хийсэн байсан учир аппликейшнийг нь ашиглаж үзсэн.

Дараа нь бид ОЛЕД дэлгэцийг програмчилж дэлгэц дээр тоо болон үгс хэвлэж үзсэн. Үүнийг Зураг 11-с харж болно.



11-р зураг. OLED дэлгэцийн туршилт

Үүний дараа бид картонон хайрцгийг сав болгож толь, томруулдаг шил болон энгийн шил ашиглаж гэрлийн хугарлыг туршиж үзсэн.



12-р зураг. Гэрлийн хугарлын туршилт

Доорх зурган дээр харагдаж байгаачлан өдрийн болон шөнийн цагаар төхөөрөмжөө ажиллуулж туршилт хийж хүний нүдээр яаж харагдах талаар туршсан.

13-р зураг. Өдөр болон шөнийн туршилт

Нүдний шил дээр төхөөрөмжөө байрлуулж хэрхэн харагдах туршилт хийсэн. Үүнийг доорх Зураг 14-т үзүүлэв.

14-р зураг. Нүдний шил дээр тусах туршилт

Доорх Зураг 15-д төхөөрөмжийн анхны загварыг үзүүлэв. Уг төхөөрөмжид зориулж Solid дээр зурж 3D принтерээр хэвлэсэн.

15-р зураг. Анхны туршилтын загвар

ДҮГНЭЛТ

Энэхүү судалгааны ажлаар бид мэдээллийн шил зохион бүтээхийг зорилоо. Мэдээллийн шил нь ухаалаг нүдний шил эсвэл нэмэгдүүлсэн бодит байдлын (AR) нүдний шил гэж ихэвчлэн нэрлэгддэг тоон мэдээлэл эсвэл график дүрсийг үзүүлдэг зүүдэг төхөөрөмж юм. Эдгээр нүдний шил нь тунгалаг эсвэл хагас тунгалаг дэлгэцтэй бөгөөд хэрэглэгчийн хараанд саад учруулахгүйгээр мэдээлэл, зураг, видео үзүүлэх боломжтой юм. Энэхүү судалгаагаар бид дараах ажлыг хийж гүйцэтгэсэн:

- Bluetooth модультай мультиметрийн өгөгдлийн протоколыг судалсан
- OLED дэлгэцийн програмчлалыг хийж гүйцэтгэсэн
- Гэрлийн хугарлыг туршиж үзсэн
- Техникийн болон программ хангамжийн шийдлийг гаргасан
- Мэдээллийн шилний анхны загварыг гаргасан

Цаашид мультиметрийн өгөгдлийг хүлээн авч дэлгэцэд бүрэн дүрслэхээр ажиллаж байна

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] Amana , Bhaveshb and Rahulc “A Comprehensive Review of Smart Glasses Technology- Future of Eyewear”. Vol.12 No.2 (2021), 15-26

[2] G. Soundarajan , R. Vijayan “Smart wearable glasses—future data center management” 2015 EMC Proven Professional Knowledge

[3] A. Deshmukh, A. Chavan, R. Marath , P. Shinde, “Smart Data Glasses For Multimeter”, International Volume:02, Conference on Communication and Information Processing (ICCIP-2020)

[4] N. Zuidhof1, S. Ben Allouch, O. Peters, P. Verbeek, “Defining Smart Glasses: A Rapid Review of State-of-the-Art Perspectives and Future Challenges From a Social Sciences’ Perspective,” 18 October 2021

[5] MLT-BT05 4.0 Bluetooth module, AT instruction Set

[6] OLED display manual, 2022

[7] HC-05Serial Bluetooth Products, User Instructional Manual

[8] https://github.com/godstale/retrowatch

[9] https://www.youtube.com/watch?v=ein6UX9sFAY

[10] https://www.pcbway.com

[11] https://hackaday.io/project/12211/instructions

.

Detective Iconan - Фишинг вэбсайтийг хайлтын систем ашиглан урьдчилан илрүүлэх хэрэгсэл хөгжүүлэх нь

Г. Тэнгис[1], Л. Билгүүнзаяа[1], Ж. Мөнхсайхан[1], Б. Мөнхбаяр[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбоо Технологийн сургууль,
Мэдээллийн Сүлжээ, Аюулгүй байдлын салбар
xyptonize@gmail.com, munkhbayar.b@must.edu.mn

Хураангуй*—Өнөөгийн дижитал эрин үед цахим залилан буюу фишинг вэб сайтуудыг илрүүлэх нь кибер аюулгүй байдлын салбарт тулгамдсан асуудал хэвээр байна. Уламжлал ёсоор хуурамч вэбсайтыг илрүүлэхийн тулд машин сургалт болон гүн сургалтын арга техникийг ашигладаг байсан ч тэдгээрийн нарийн төвөгтэй байдал, нөөцийн шаардлага нь практик хэрэглээнд саад учруулж болзошгүй юм. Энэхүү судалгаа нь вэб сайттай холбоотой логоны өвөрмөц шинж чанарыг ашиглан фишинг илрүүлэх шинэлэг хандлагыг судлан түүнд тулгуурлан хэрэгсэл хөгжүүлэх болно. Нарийн төвөгтэй алгоритмд найдахын оронд энэ арга нь лого хэш шинжилгээнд тулгуурладаг. Энэхүү техник нь вэбсайтын лого буюу фавикон зургаас MD5 эсвэл MMH3 хэш гэх мэт хэш утгыг үүсгэх явдал юм. Энэхүү хэш нь логоны визуал шинж чанарыг багтаасан бөгөөд өөр өөр вэбсайтыг харьцуулах боломжийг олгодог. Үйл явц нь хэд хэдэн үе шаттайгаар явагдана. Нэгдүгээрт, зорилтот вэбсайтын логоны хэшийг тооцоолно. Дараа нь энэ хэшийг Shodan, ZoomEye, Censys гэх мэт тогтсон мэдээллийн сангаас хайдаг. Ижил лого хэшийг хуваалцаж буй вэбсайтыг илэрцээр гаргаж ирэх ба үүнд тухайн байгууллагаас өөр илэрц гарж ирж байвал энэ нь фишинг хийж буй боломжит үйл ажиллагаа гэсэн үг юм. Холбогдох домэйнүүд болон IP хаягуудыг цааш нь шинжилснээр залилан мэхлэх үйлдлийг харуулсан хэв маягийг илрүүлэх замаар ажиллана.

Түлхүүр үг—залилан, хэш, Shodan, ZoomEye, Censys

I. Удиртгал

Энэхүү судалгаа нь лого хэш шинжилгээгээр фишинг вэб сайтуудыг тодорхойлох шинэ технологийг ашиглах явдал юм. Судалгаа нь логоны төрөлхийн өвөрмөц байдлыг ашиглаж, мэдээллийн өгөгдлийн сан ашигласнаар машин сургалтад суурилсан илрүүлэлтийн нарийн төвөгтэй байдлаас илүүтэйгээр прагматик хувилбарыг санал болгож ажиллаж буй хэрэгсэл юм. Олон давхаргат аюулгүй байдлын стратегийн нэг хэсэг болгон энэхүү хэрэгслийг бусад хэрэгсэлтэй хослуулан ажилуулах нь байгууллагын системийг илүү аюулгүй байлгахад өндөр хувь нэмэр оруулах болно. Уламжлал ёсоор хуурамч вэбсайтуудыг илрүүлэхийн тулд машин сургалт болон гүн сургалтын арга техникийг ашигладаг байсан ч тэдгээрийн нарийн төвөгтэй байдал, нөөцийн шаардлага нь практик хэрэглээнд саад учруулж болзошгүй юм. Тиймээс өөрийн нөөцөөс маш багийг ашиглаж бэлэн нөөцийг хамгийн хямдаар ашиглан нарийн төвөгтэй модел сургах бус лого хэш шинжилгээнд тулгуурлан фишинг вэбсайтыг илрүүлэх санаа төрсөн ба үүнийг хэрэгжүүлэхдээ Censys, Zoomeye, Shodan гэх интэрнет шинжилгээний өгөгдлийн сангуудыг ашиглан хийж боломжтой юм.

II. Онолын хэсэг

Фишинг халдлагыг хүргэх замаар нь Email Phishing, Vishing and Smishing, Social Media Phishing гэж ангилах ба эцэст нь өөрсдийн нийтийм сүлжээнд тавьсан жинхэнэ байгууллагыг дуурайлган хийсэн хуурамч вэбсайтруу хөтлөх юм. Халдагч нь хуурамч вэбсайтыг жинхэнэ вэбсайттай ижил болгохын тулд тухайн вэбсайтыг clone буюу хуулбарлах эсвэл ашиглаж буй жинхэнэ лого зургийг нь ашигладаг. Иймд тухайн зургийг хайлтын системүүдээс хайх замаар хийгдэнэ. Зургийн хэш гэдэг нь зургийн пикселийн өгөгдлөөс үүссэн өвөрмөц дижитал гарын үсэг эсвэл хурууны хээ юм. Энэ нь зургийн бүрэн бүтэн байдлыг шалгах, аливаа хөндлөнгийн оролцоо, өөрчлөлтийг илрүүлэхэд ашиглагдаж болно.

Хэш функц: Хэш функц нь оролт (энэ тохиолдолд зураг) авч, хэш утга гэж нэрлэгддэг тогтмол урттай тэмдэгтүүдийг үүсгэдэг. Оролтын өчүүхэн өөрчлөлт ч гэсэн мэдэгдэхүйц өөр хэш утгыг бий болгох ёстой.

Бүрэн бүтэн байдлыг шалгах: Эх зургийн хэшийг тооцоолж, өөрчилсөн гэж сэжиглэж буй зургийн хэштэй харьцуулснаар та зураг өөрчлөгдсөн эсэхийг хурдан тодорхойлох боломжтой. Хэрэв хэшүүд таарахгүй бол энэ нь дүрсийг өөрчилсөн гэсэн тод шинж тэмдэг юм.

Хурдан бөгөөд үр дүнтэй: Зургийн хэш нь харьцангуй жижиг хэмжээтэй бөгөөд хурдан үүсдэг тул энэ нь зургийн бүрэн бүтэн байдлыг шалгах, ялангуяа олон тооны зурагтай ажиллахад практик арга юм.

Жинхэнэ байдлыг баталгаажуулах: Зургийн хэшийг дижитал нотлох баримтын жинхэнэ эсэхийг шалгахын тулд дижитал шүүх шинжилгээнд ихэвчлэн ашигладаг.

Өгөгдөл дамжуулах: Интернетээр зураг илгээхдээ эх зургийг хэш болгож, зургийн хамт хэш утгыг илгээх боломжтой. Дараа нь хүлээн авагч хэшийг тооцоолж, дамжуулсан хэш утгатай харьцуулах замаар хүлээн авсан зураг нь эх зурагтай таарч байгаа эсэхийг шалгаж болно.

Агуулга тааруулах: Зургийн хэшийг мөн контент дээр суурилсан зураг хайх, хуулбарлахад ашигладаг. Хэшийг харьцуулснаар та мэдээллийн сангаас давхардсан эсвэл ижил төстэй зургийг олох боломжтой.

Мэдээллийн шахалт: Зургийн хэшийг зураг шахах алгоритмд ашигладаг бөгөөд ижил төстэй зургуудыг ижил эсвэл ижил төстэй хэшээр төлөөлдөг бөгөөд үр дүнтэй хадгалах, сэргээх боломжийг олгодог.

Гэсэн хэдий ч зургийн хэш нь ямар ч үргэлж баттай үнэн биш гэдгийг анхаарах нь чухал юм. Чадварлаг халдагчид хэш нь ижил эсвэл бага зэрэг ялгаатай байхаар зургийг өөрчлөх боломжтой. Нэмж дурдахад зарим төрлийн шахалт эсвэл хэмжээг өөрчлөх нь хэшийг ямар ч хорлонтой зорилгоүйгээр өөрчлөх боломжтой. Тиймээс зургийн хэшийг илүү өргөн хүрээний аюулгүй байдлын стратегийн нэг хэсэг болгон ашиглах нь зүйтэй учраас зургийн хэшийн Агуулга тааруулга аргачлал дээр суурьлсан аргаар хэрэгсэл судалгаа цааш үргэлжилнэ.

III. СУДАЛГААНЫ ХЭСЭГ

Фишинг халдлага гэдэг нь таны нууц үг болон энэ төрлийн хувийн мэдээллийг хулгайлах зорилготой бөгөөд хакерууд фишинг халдлагын тусламжтайгаар хэрэглэгчийн нэр, нууц үг, регистрийн дугаар болон бусад холбогдох мэдээллийг цуглуулж, тухайн мэдээллийг хууль бус үйлдэлд ашиглах замаар өөр төрлийн халдлагууд хийх тохиолдол их байдаг. 2004 оноос эхлэн дэлхий даяар фишинг төрлийн халдлага ихэсч байгаа бөгөөд сүүлийн жилүүдэд байгууллагууд алсын зайнаас ажиллаж буйтай холбоотойгоор эрчимтэй өсөж, учруулж байгаа хохирлын хэмжээ ч тэр хэмжээгээр нэмэгдсэн талаар Computer Fraud & Security сэтгүүлийн 2020 оны 9 дүгээр сарын дугаарын “Why is phishing still successful?” өгүүлэл, Wiley хэвлэлийн газрын Internet technology letters сэтгүүлийн 2020 оны 10 дугаар сарын “COVID-19 pandemic cybersecurity issues”[3] өгүүлэл, IEEE Xplore-д 2021 оны 1 дүгээр сард хэвлэгдсэн “Phishing Web Page Detection Methods: URL and HTML Features Detection”[2] өгүүлэл зэрэг олон эх сурвалжид онцолсон байна. Мөн хэрэглэгчдийн хувьд ялгаатай системүүдэд ижил нууц үг ашигладаг нь тухайн халдлагын тоо болон хор хохирол буурахгүй байгаатай шууд холбоотой хэмээн судлаачид үзсэн байдаг. Энэхүү халдлагыг илрүүлэхэд хамгийн их хүндрэл үзүүлж буй зүйл нь халдлага гарсны дараа тэрхүү халдлага гарсан гэдгийг илрүүлж байгаа явдал юм. Фишинг халдлагыг хүргэх замаар нь Email Phishing, Vishing and Smishing, Social Media Phishing гэж ерөнхий ангилна. Тэдгээрийн эцсийн зорилго нь хохирогчийг өөрсдийн тусгайлан бэлдсэн хуурамч вэбсайтруу хөтлөх юм. Хохирогч этгээд итгэж хуурамч вэбсайтруу орж өөрийн мэдээллийг оруулах замаар халдлагад өртдөг. Гэвч тэрхүү халдлага гархаас өмнө буюу хуурамч вэбсайтыг үйлдэж public буюу нийтийн сүлжээнд тавих үед нь таслан зогсоох боломжтой гэхдээ энэ нь маш их нөөцийг шаардана. Иймээс бидний хийж буй судалгаа нь уг таслан зогсоох арга дээр тулгуурлан судалгаа хийж хэрэгсэл хөгжүүлэх явдал юм.

Ихэнх фишинг халдлага нь бидний өдөр тутам ашигладаг интернэт банк, нийгмийн сүлжээний сайтын нэр, логог ашиглан, тэдгээртэй ижил төстэй мэдээллийн агуулгатайгаар цахим шуудан илгээдэг. Халдагч нь хуурамч вэбсайтыг жинхэнэ вэбсайттай ижил болгохын тулд тухайн вэбсайтыг clone буюу хуулбарлах эсвэл ашиглаж буй жинхэнэ лого зургийг нь ашигладаг. Тэгвэл бид тэрхүү зургаар нь хайх шийдлийг “Kang Leng Chiew, Jeffrey Soon-Fatt Choo,San Nah Sze and Kelvin S. C. Yong ‘Leverage Website Favicon to Detect Phishing Websites’,”[1] уг эрдэм шинжилгээний судалгаанаас санаа авсан ба үүнд Google-ийн зурган хайлтыг системийг ашигласан ба энэ нь тийм ч үр дүнтэй биш учраас өөр хаанаас зургаар нь боломжтой хайлтын систем байгаа тал дээр цааш судалсан. Судалгааны үр дүнд дараах 3 хайлтын системийг сонгон авсан.

Shodan: Shodan нь нийтийн сүлжээнд холбогдсон буюу интернэтэд холбогдсон бүхий л төхөөрөмжийн нийтэд нээлттэй мэдээллүүдийг индексжүүлэн өгөгдлийн сандаа хийх замаар ажилладаг ба хэрэглэгчдээ түүнээс мэдээлэл хайх боломжоор хангадаг. Үүнээс бидний ашиглах гол мэдээллийн сангийн хайлт нь *http.favicon.hash* хайлтын утга юм.

Censys: Censys нь мөн нийтийн сүлжээнд холбогдсон буюу интернэтэд холбогдсон бүхий л төхөөрөмжийн нийтэд нээлттэй мэдээллийг индексжүүлэн ажиллах ба нэмэлтээр түүн дээр эмзэг байдлын энгийн шалгалтуудыг явуулах замаар ажилладаг эмзэг байдлын хайлтын систем юм. Ашиглах хайлтын утга нь *services.http.response.favicons.md5_hash*

Zoomeye: Zoomeye нь Censys-тэй мөн адил нээлттэй мэдээллүүдийг индексжүүлэн эмзэг байдлын шалгалт хийдэг ба бидний ашиглах мэдээллийн сангаас хайх утга нь *iconhash* утга юм.

Дээр дурдсан хайлтын утгууд нь тухайн хайлтын системүүдээс ижил лого буюу фавикон зургийг хэш утгаар нь хайх боломжоор хангадаг. Үүн дээр тулгуурлан бид Python програмчлалын хэл дээр автоматжуулан хэрэгсэл хөгжүүлэх шийдлийг олсон.

IV. СУДАЛГААНЫ АЧ ХОЛБОГДОЛ

Цахим залилан нь онцгой буюу халдлага, хохирол гарсны дараагаар мөрдлөг хийн илрүүлэх боломжтой халдагын төрөл юм. Гэвч уг судалгааг ашигласнаар урьдчилан илрүүлэх боломжтой. Мөн энэхүү судалгааг хийж хэрэгсэл хөгжүүлснээр цахим залилан буюу фишинг халдлагыг бууруулах боломж бүрдэнэ. Хэрэгслийг ашигласнаар ямар ч хэмжээний буюу жижиг бизнесээс том байгууллагууд хурдан шуурхай, өөрсдийн нөөцийг ашиглахгүй, хямд өртгөөр нэр хүнд, санхүү, хувийн мэдээллийн хохирлоос зайлсхийх боломж бүрдэнэ.

V. СЭДВИЙН СУДЛАГДСАН БАЙДАЛ

Google зураг хайлтын системийг ашиглан вэбсайтын фавибок буюу лого дээр тулгуурлан хайлт хийх аргачлалыг сонгосон. Favicon нь вэбсайтын брэндийг төлөөлдөг тул сонгосон. Нэмж дурдахад вэб хуудсан дээр гарч буй динамик контент (жишээ

нь, зар сурталчилгаа) фавиконд нөлөөлөхгүй. Хэн болохыг тодорхойлохын тулд Google зургийн хайлтын системийг ашиглан favicon-ийн талаарх мэдээллийг буцаана. Google зургийн хайлтын системийг энэ ажилд зориулж сонгосон бөгөөд учир нь энэ нь зургийг (жишээ нь, фавикон) мэдээлэл хайх хайлтын асуулга болгон ашиглах боломжийг олгодог. Мөн индексжүүлсэн хамгийн олон хууль ёсны вэбсайттай учраас Google хайлтын систем нь маш зохимжтой.

Kang Leng Chiew, Jeffrey Soon-Fatt Choo,San Nah Sze and Kelvin S. C. Yong “Leverage Website Favicon to Detect Phishing Websites”, 06 Mar 2018[1]

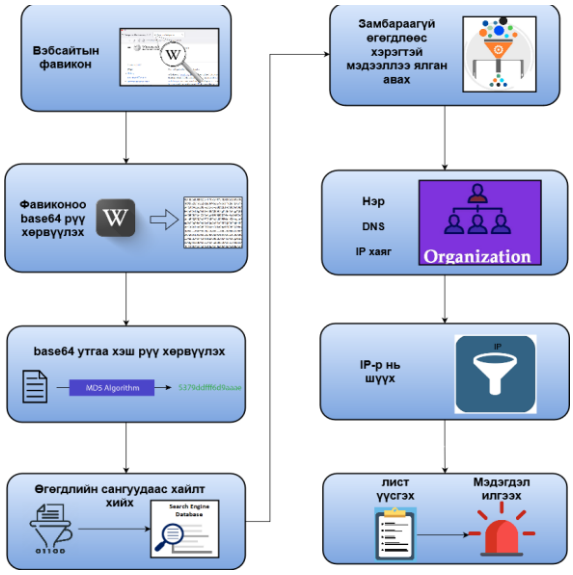
VI. ХЭРЭГСЭЛ ХӨГЖҮҮЛЭЛТ

Detective-Iconan нь ямар нэгэн вэбийг халдагч этгээд клон хийн ямар нэгэн public хандалттай сервер дээр тавигдсан эсэхийг шалгадаг хэрэгсэл юм.

Уг хэрэгсэл нь ажиллахдаа үндсэн вэбийн логоний хэшийг аваад өргөн хүрээн скан хийдэг хайлтын системүүдийг ашиглан тухайн хэшийг тулган олох зарчмаар ажиллана. Тухайн тулгасан хэшүүдэд үндсэн вэб багтах ба үүнийг өөрийн байгууллагын сүлжээний subnet-г оруулж филтердэж өгснөөр гадны вэбүүдийг шүүн авч цахим шуудан болгон мэдэгдэл илгээнэ.

Хайлтын системүүдэд: Shodan, Censys, Zoomeye зэрэг системүүдийн Python санг ашигласан.

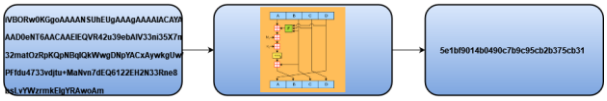
1-Р СХЕМ. БҮТЦИЙН СХЕМ



2-Р СХЕМ. ФАВИКОНОО BASE64 РУУ ХӨРВҮҮЛЭХ

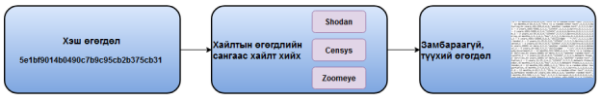
Favicon гэдэг нь тухайн вэбсайт руу хандалт хийхэд вэб хөтөч дээр харагддаг тухайн вэбсайтын лого юм.Detective Iconan хэрэгслийг ажиллуулахын тулд хамгийн эхэнд скан хийх вэбсайтийнхаа логоны замыг олох шаардлагатай үүнийг олохдоо source code буюу эх кодоос нь олж мэдэх боломжтой. тухайн олсон зам дээрх зургийг base64-руу хөрвүүлэх нь тухайн зургийн хэш утгыг гаргаж авахад хялбар болгоно. Учир нь замчлал дээр буй зургийн хэшийг гаргаж авахын тулд татаж авах шаардлагатай. Харин base64 encode хийхэд татах шаардлаггүй болно.

3-Р СХЕМ. BASE64 ХЭШ РУУ ХӨРВҮҮЛЭХ



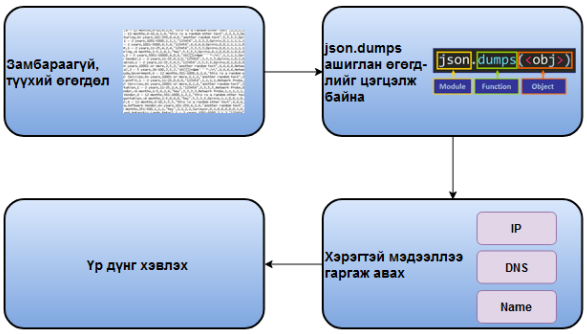
Хөрвүүлсэн base64 өгөгдлийг MD5 болон MMH3 төрлийн хэш утгууд болгоно. Ингэснээр тухайн зургийг өгөгдлийн сангаас хайхад бэлэн болно

4-Р СХЕМ. ХАЙЛТ ХИЙН ӨГӨГДӨЛ ГАРГАЖ АВАХ



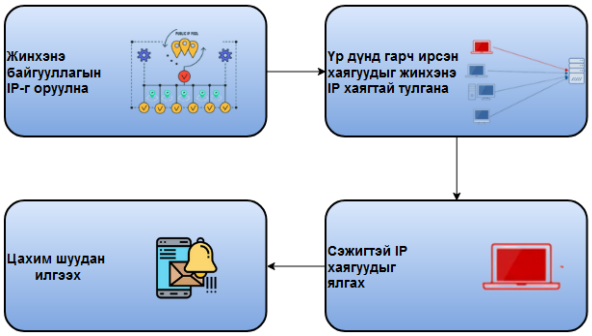
Хэш утгыг датабазуудаас хайснаар тухайн хэш утгыг агуулж буй илэрцүүдийг гаргаж ирэх ба ингэснээр тухайн зургийг агуулж буй вэбсайтуудыг олох боломж бүрдэнэ.

5-Р СХЕМ. ӨГӨГДЛӨӨСӨӨ МЭДЭЭЛЛЭЭ ЯЛГАН АВАХ



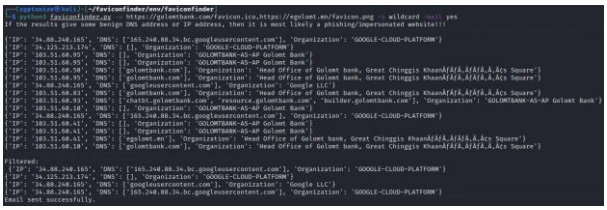
Хайлтын илэрцэд гарч ирсэн замбараагүй өгөгдлийг цэгцтэй болгож задлах буюу parsing үйлдлийг хийнэ.

6-Р СХЕМ. СЭЖИГТЭЙ ХАЯГУУДЫГ ЯЛГАХ

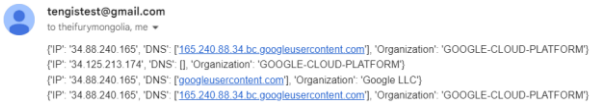


Ялгаж авсан өгөгдлүүдээс сэжигтэй вэбсайтийг ялгахын тулд бодит байгууллагын IP хаягуудыг хэрэгсэлдээ оруулж өгснөөр сэжигтэй IP-тай харьцуулан салгаж шүүлтүүр хийх боломж бүрдэнэ. Шүүлтүүр хийсний дараагаар боломжит сэжигтэй хаягууд үлдэх ба тэдгээрийг цахим шуудан болгож мэдэгдэл илгээнэ.

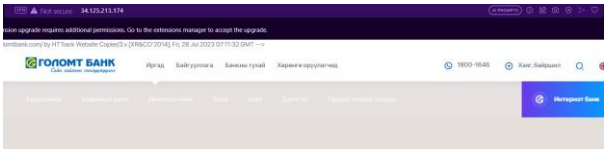
Үр дүн: Дурын үүлэн системийн үйлчилгээ үзүүлдэг газар вэб клондон тавьхад ихдээ 1-ээс 2 хоногын дотор олдож байсан. Хамгийн хурдандаа 4цагт илрүүлсэн.



1-р зураг.Ажиллаж буй байдал



2-р зураг. Сэжигтэй байх боломжит IP хаягуудыг цахим шуудан болгон илгээсэн байдал



3-р зураг. Ирсэн сэжигтэй хаягруу орж шалгасан байдал

НОМ ЗҮЙ

[1] Kang Leng Chiew, Jeffrey Soon-Fatt Choo,San Nah Sze and Kelvin S. C. Yong “Leverage Website Favicon to Detect Phishing Websites”, 06 Mar 2018

[2] Humam Faris, Setiadi Yazid “Phishing Web Page Detection Methods: URL and HTML Features Detection” 23 February 2021

[3] Bernardi Pranggono, Abdullahi Arabo “COVID-19 pandemic cybersecurity issues” 03 October 2020

DNSSEC ТҮЛХҮҮР БАТАЛГААЖУУЛАЛТЫН ҮЙЛ ЯВЦЫГ ХЯНАХ СУДЛАХ REPORT ГАРГАХ ТҮҮЛ ХӨГЖҮҮЛЭЛТИЙГ САЙЖРУУЛАХ

М.Хулан[1], Ж.Нямсамбуу[1] , Э. Хангал[1], Г.Долгормаа[1], Б.Мөнхбаяр[2]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл Холбоо Технологийн сургууль,
Мэдээллийн Сүлжээ, Аюулгүй байдлын салбар
nymaan1020@gmail.com, munkhbayar.b@must.edu.mn

***Хураангуй*— Domain Name System Security Extensions (DNSSEC) нь интернэтийн дэд бүтцийн үндсэн бүрэлдэхүүн хэсэг болох Domain Name System (DNS) бүрэн бүтэн байдал, жинхэнэ байдлыг сайжруулах зорилготой аюулгүй байдлын чухал протокол юм. Энэхүү баримт бичиг нь DNSSEC-ийн байршуулалтын өнөөгийн байдлын тоймыг харуулсан бөгөөд энэ нь cache poisoning, man-in-the-middle, DNS spoofing зэрэг DNS-тэй холбоотой аюул заналыг эсэргүүцэхэд чухал ач холбогдолтой. DNSSEC нь тоон гарын үсгээр DNS бүртгэлд гарын үсэг зурснаар DNS-д аюулгүй байдлын нэмэлт давхаргыг нэмдэг. Эдгээр тоон гарын үсэг нь DNS-ийн хариултыг баталгаажуулах боломжийг олгодог бөгөөд DNS-ээс авсан өгөгдөл өөрчлөгдөөгүй бөгөөд эрх бүхий эх сурвалжаас авсан эсэхийг баталгаажуулдаг. Гэсэн хэдий ч DNSSEC-ийг байршуулах нь үндсэн удирдлага, үйл ажиллагааны туршлага, хэрэглэгчийн мэдлэг зэрэг янз бүрийн сорилт, төвөгтэй байдлыг бий болгодог. Түлхүүр баталгаажуулалт нь DNS-ийн бичлэгт гарын үсэг зурахад ашигладаг криптограф түлхүүрүүд найдвартай эсэхийг баталгаажуулдаг тул DNSSEC-ийн байршуулалтын чухал хэсэг юм. 2023 оны байдлаар DNSSEC байршуулалтын түвшин маш бага хэвээр байна. Үүнд, Домэйнуудаас top-level домэйнууд руу DNSSEC төгсгөл хүртэл байрлуулах нь маш бага хэвээр байгаа юм. Бид DNSSEC түлхүүр баталгаажуулалтын үйл явцыг хянах судлах report гаргах түүл хөгжүүлэлтийг сайжруулах, замаар энэхүү төвөгтэй байдлыг багасгах боломжийг хайсан.**

Түлхүүр үг—DNSSEC, DNS, криптограф, бичлэг, man-in-the-middle, cache poisoning, top-level domain , n3map,

I. УДИРТГАЛ

Domain Name System Security Extensions (DNSSEC) нь орчин үеийн интернетийн чухал хүчин зүйл болох Domain Name System (DNS) бэхжүүлэх чухал үе шат юм. DNSSEC-ийг амжилттай ашиглах нь гол удирдлага, гарын үсэг үүсгэх, DNS хариуг баталгаажуулах зэрэг найдвартай хэрэгсэл, програм хангамжийн шийдлүүдээс ихээхэн хамаардаг. DNSSEC-ийн хэрэгслүүд нь DNSSEC-ийн аюулгүй байдлыг хэрэгжүүлэх нарийн төвөгтэй үйл явцыг хялбарчлахад чухал үүрэг гүйцэтгэдэг. Энэхүү баримт бичиг нь нээлттэй эхийн програм хангамж, командын шугамын хэрэгслүүд, хэрэглэгчдэд хялбар DNSSEC хэрэгслүүдийн хөгжүүлэлт, сайжруулалтыг судлах болно. Бид DNSSEC-ийн байршуулалт, менежментийг оновчтой болгож, DNSSEC-ийг интернетийн оролцогч талуудад илүү хүртээмжтэй болгоход эдгээр хэрэгслүүдийн гүйцэтгэх үүргийн талаар ярилцах болно.

DNS халдлагын нөлөө маш хүчтэй, DNS-ийн санал болгож буй аюулгүй байдлын хамгаалалт маш хязгаарлагдмал байгаа тул хэрэглэгчид DNS шийдүүлэгчээс хүлээн авсан IP хаяг нь тэдний хүссэн домэйнд зориулагдсан эсэхийг баталгаажуулах арга зам хэрэгтэй. DNS-тэй холбоотой халдлагуудтай холбоотой эмзэг байдлыг багасгадаг DNSSEC болон DNS өгөгдлийн бүрэн бүтэн байдал, жинхэнэ байдлыг хамгаалах зорилготой криптографийн механизмуудыг өөрсдийн түүл хөгжүүлэлтэнд багтаасан. DNSSEC-ийн байршуулалт ба түлхүүрийн баталгаажуулалт, түүнчлэн DNSSEC хэрэгслийн хөгжүүлэлт гэсэн хоорондоо холбоотой бидний судалгааны үе шат арван долоон хоногийн туршид үргэлжилсэн.

II. ОНОЛЫН ХЭСЭГ

DNS нь 30 жилийн өмнө, аюулгүй байдал нь интернэтийн анхаарлын төвд ороогүй байхад бүтээгдсэн юм. Нэмэлт хамгаалалтгүйгээр MITM халдагчид бүртгэлийг хуурамчаар үйлдэж, хэрэглэгчдийг фишинг сайт руу хөтлөх боломжтой. DNSSEC нь үүнийг зогсоодог бөгөөд үүнийг асаахад хялбар байдаг. DNS систем нь хүсэлтийн хариуг хуурамчаар өгөөгүй, эсвэл халдагчийн үйл явцын бусад хэсгийг таслаагүй гэдгийг баталгаажуулах аргуудыг агуулаагүй болно. Хэрэглэгч таны вэбсайттай холбогдохыг хүссэн тохиолдолд домэйн нэрээ ашиглах боломжтой IP хаяг болгон хөрвүүлэхийн тулд DNS хайлт хийх шаардлагатай болдог тул энэ нь асуудал юм. Хэрэв хэрэглэгч кофе шоп гэх мэт найдваргүй газраас холбогдож байвал хорлонтой халдагчид холбогдох боломжтой дунд нь сууж, DNS бүртгэлийг хуурах. Энэ халдлага нь IP хаяг А бичлэгийг өөрчлөх замаар хэрэглэгчдийг хортой хуудас руу чиглүүлэх боломжийг олгож магадгүй юм.

Тоон гарын үсэг: DNSSEC нь DNS мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг шалгахын тулд тоон гарын үсгийг ашигладаг. DNS нөөцийн бүртгэл бүр (жишээлбэл, A бичлэг, MX бичлэг) домэйны эзэмшигчийн тоон гарын үсэгтэй байдаг. Эдгээр гарын үсгийг криптографийн түлхүүр ашиглан бүтээдэг.

Public Key Infrastructure: DNSSEC нь криптограф түлхүүрүүдийн шаталсан системд тулгуурладаг. DNS шатлалын дээд хэсэгт бүс гарын үсэг зурах түлхүүрүүд (ZSKs) болон түлхүүрийн гарын үсэг зурах түлхүүрүүд (KSKs) байдаг. KSK нь ZSK-д гарын үсэг зурахад ашиглагддаг бөгөөд энэ нь эргээд нөөцийн бодит бүртгэлд гарын үсэг зурдаг.

Chain of trust: DNSSEC нь DNS шатлалын үндэс (root zone)-ээс тодорхой домэйний эрх бүхий DNS сервер хүртэл итгэлцлийн гинжин хэлхээг бий болгодог. Энэ нь хэд хэдэн криптограф гарын үсгийг ашиглан баталгаажуулах боломжтой тул DNS өгөгдөлд найдвартай байх болно.

Resource Record Signatures: DNSSEC нь ижил нэр, төрөл бүхий DNS нөөцийн бүртгэлүүдийн цуглуулга болох Resource Record Sets (RRsets) -ийг танилцуулж байна. RRset бүр нь RRset-ийг бүхэлд нь хамарсан холбогдох гарын үсгийн бүртгэлтэй (RRSIG). Эдгээр RRSIG нь мэдээллийн бүрэн бүтэн байдлыг шалгахад ашиглагддаг.

Криптографийн алгоритмууд: DNSSEC нь тоон гарын үсэг үүсгэх, DNS өгөгдлийг хамгаалахын тулд янз бүрийн криптограф алгоритмуудыг ашигладаг. Эдгээр алгоритмууд нь аюулгүй байдлыг хангах үүднээс үе үе шинэчлэгддэг.

DNSSEC байршуулалт нь дараах алхмуудыг агуулна.

Zone Signing: Домэйн эзэмшигч нь бүс гарын үсэг зурах түлхүүрүүдийг (ZSKs) ашиглан DNS өгөгдөлдөө дижитал гарын үсэг зурж, холбогдох RRSIG бичлэгүүдийг үүсгэдэг. Үүнийг ихэвчлэн домэйн бүртгэгч эсвэл DNS хостинг үйлчилгээ үзүүлэгчид хийдэг.

Delegation Signer (DS) Records: Итгэлцлийг бий болгохын тулд DS бүртгэлийг эх домэйнд (жишээлбэл, дээд түвшний домэйн эсвэл дээд түвшний домэйн) үүсгэж, хүүхдийн домэйний KSK руу чиглүүлдэг.

Баталгаажуулалт: DNS шийдүүлэгчид (жишээлбэл, интернэтийн үйлчилгээ үзүүлэгчийн ажиллуулдаг) DNSSEC баталгаажуулалтыг гүйцэтгэдэг. Тэд DNS өгөгдлийн тоон гарын үсгийг шаардаж, баталгаажуулж, хөндлөнгийн оролцоогүй эсэхийг шалгадаг.

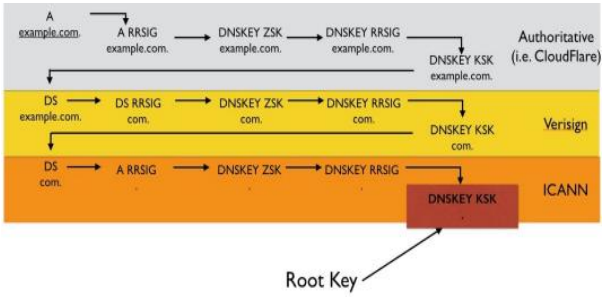
DNSSEC нь DNS дэд бүтцийн аюулгүй байдал, найдвартай байдлыг ихээхэн сайжруулж, DNS-д суурилсан янз бүрийн халдлагад илүү тэсвэртэй болгодог. Энэ нь интернэт хэрэглэгчдэд зориулсан хамгаалалтын чухал давхаргыг хангаж, зөвшөөрөлгүй этгээд DNS өгөгдөлд хөндлөнгөөс оролцохоос сэргийлж, хэрэглэгчид зөв веб сайт, үйлчилгээнд хүрэхэд тусалдаг.

Кэшийг хордуулах халдлагад халдагч DNS хариу багцыг хууран мэхлэх замаар DNS шийдүүлэгч нь халдагчийн "хордуулсан" өгөгдлийг хүлээн авч кэш хийх болно, тухайлбал, довтолж буй серверийн IP хаягийг зааж буй хүчинтэй эзэмшигчийн нэр бүхий A RR. Шийдвэрлэгч нь энэ хордлоготой өгөгдлийг эцсийн хэрэглэгчдэд өгч, нийтлэг домэйн нэрийн хүсэлтийг (жишээ нь www.google.com) хууль ёсны серверээс халдаж буй серверүүд рүү шилжүүлдэг.

Man-in-theddle халдагчид нь хохирогчийн сүлжээний пакетуудыг унших, бичих эрхтэй халдагчид юм. Энэ хувилбарт халдагч орон нутгийн рекурсив шийдэгчээс алслагдсан DNS бүсүүдэд тавьсан асуулгыг сонсож, алслагдсан бүсүүдээс хуурамч хариултуудыг оруулах боломжтой. DNS нь шифрлэгдээгүй тул халдагч этгээд зөв TXID-г хуулж, хуурамч DNS хариултыг үүсгэх нь маш энгийн бөгөөд энэ нь рекурсив шийдэгчийн кэшийг хордуулна.

III. СУДАЛГААНЫ ХЭСЭГ

DNSSEC нь одоо байгаа DNS-ийн өргөтгөл бөгөөд DNS асуулгын хариуг шалгах механизмыг хангадаг. Өндөр түвшинд DNSSEC баталгаажуулалтыг DNSKEY бичлэг буюу нийтийн түлхүүр ашиглан хийж, RRSIG бичлэгийн кодыг тайлж (одоо байгаа бичлэг бүрд байдаг) болон тооцоолох боломжтой. хүчинтэй бүртгэлтэй таарах хэшүүд. Нийтийн түлхүүр нь өөрөө эх бүс хүртэл гарын үсэг зурдаг, мөн эцэг бүсийн нийтийн түлхүүр нь үндсэн бүс хүртэл. Энэ нь 1-р зурагт үзүүлсэн шиг DNSSEC бүртгэлийг баталгаажуулах итгэлцлийн хэлхээг бий болгож байна. Мөн хүүхдийн бүсэд гарын үсэг зурах, бүртгэл байгаа эсэхийг нотлох механизмтай холбоотой бусад бүртгэлүүд байдаг ч эдгээр нь бидний мөрдөн байцаалтын хүрээнд хамаарахгүй.



Зураг 1. DNSSEC нь үндсэн DNSKEY түлхүүр гарын үсэг зурах түлхүүр (KSK) хүртэл итгэлцлийн хэлхээг бий болгодог.

Top 100 domain нэр дээр хийсэн туршилт DNSSEC-ийн бүтцээс шалтгаалан зөвхөн домэйн DNSSEC-ийг хэрэгжүүлэхээс гадна DNS сервер, итгэлцлийн гинжин хэлхээний бүх серверүүд болон TLD-д шаардлагатай байдаг. Үүнийг харгалзан Trickest DNS Resolver өгөгдлийн багцын 67,177 DNS шийдэгчээс бүрдсэн том санг ашигладаг. Эдгээр шийдүүлэгчдийн аль нь ч ажиллахгүй эсвэл хугацаа дуусах босгон дотор хариу өгөхгүй. Итгэмжлэгдсэн шийдүүлэгчдийн энэ өгөгдлийн багц дотор тусдаа жагсаалт байгаа боловч одоогоор зөвхөн 35 шийдүүлэгчээр хязгаарлагдаж байна. Энэ хязгаарлалтыг харгалзан бид том жагсаалтыг ашиглаж, асуулгын хариу өгөхгүй байгаа шийдүүлэгчдийг устгадаг.

Delv программын гол зорилго нь DNSSEC гинжийг баталгаажуулахад ашиглаж болно. Үүнийг Internet Systems Consortum (ISC) боловсруулсан бөгөөд сайн мэддэг багаж хэрэгслийн залгамжлагч юм. Delv ашиглахын нэг давуу тал нь DNSSEC-ийг баталгаажуулахад ашигладаг механизмууд нь BIND9 DNS сервертэй нягт уялдаатай байдаг. Тиймээс, delv-ээр дамжуулан бидний асуулга нь доод урсгалын шийдүүлэгч DNSSEC-ийг хэрхэн баталгаажуулахыг нарийвчлан харуулах болно.

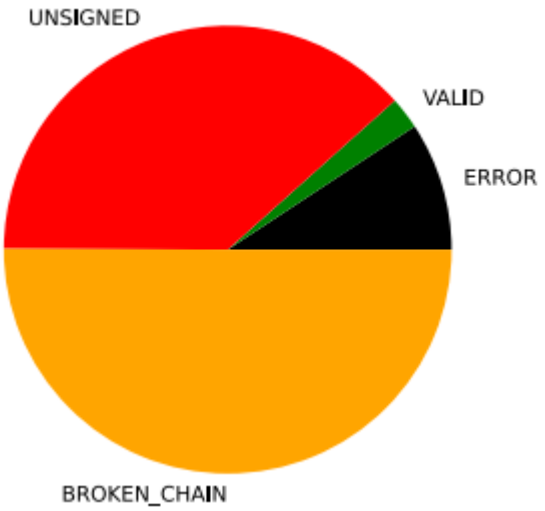
• **Valid**. Сайт нь зөв DNSSEC илэрцтэй байна. Энэ шийдүүлэгч DNSSEC-ийг зөв хэрэгжүүлдэг.

• **Unsigned**. Хариулт нь RRSIG-г оруулаагүй болно. Энэ сайт DNSSEC-ийг хэрэгжүүлдэггүй.

• **Broken Chain.** "DNSKEY бүртгэл нь эцэг эхийн бүсийн DS бичлэгтэй тохирохгүй байна, бүртгэлд хүлээгдэж байснаас өөр түлхүүрээр гарын үсэг зурсан эсвэл DNSKEY бүрэн байхгүй байна." DNS шийдүүлэгч нь DNSSEC-ийг зөв хэрэгжүүлээгүй байх магадлалтай.

• **Timeout** Шийдвэрлэгч нь заасан хугацаанд хариулт өгч чадсангүй.

• **Error** Тест нь онцгой тохиолдол гаргасан эсвэл дээр дурдсанаас өөр үр дүнг буцаасан.



Error	227862	9%
Valid	56921	2%
Unsigned	942271	38%
Broken Chain	1230146	50%

Зураг2. Шилдэг 100 сайт болон домэйн бүрийн үр дүнг буцаасан 24,572 DNS шийдүүлэгчийг ашиглан <site, resolver> хос бүрийн бүх үр дүнг нэгтгэсэн.

IV. СЭДВИЙН СУДЛАГДСАН БАЙДАЛ

	Судалгаанууд	Асуудлууд
1	DNSSEC with NSEC3 2010	DNS шатлалын чухал хэсгүүд, тэр дундаа root zone-г cache-poisoning хадлага гэх мэт эмзэг байдал.
2	Measuring the Practical Impact of DNSSEC Deployment 2013	DNSSEC-ийн байршуулалт нэлээд удаан явагдаж байна. Үйлчлүүлэгчдийн 3-аас бага хувь нь DNSSEC-ийн гарын үсэг зурсан нөөцийг хүчинтэй авч чадахгүй байна.
3	View of the DNSSEC Ecosystem 2017	Сул хуваалцсан түлхүүрүүдийн өргөн хэрэглээн эргэлдэж буй DNS resolvers олон байдаг.
4	DNSSEC as a service – A prototype implementation 2020	
5	The Sad Story of DNSSEC 2023	Домэйнуудаас top-level домэйнууд руу, DNS шийдүүлэгч рүү DNSSEC-ийг төгсгөл хүртэл байрлуулах нь маш бага хэвээр байгаа

V. ХЭРЭГСЭЛ ХӨГЖҮҮЛЭЛТ

nsec3map - DNSSEC бүсийн тоологч n3map нь DNSSEC NSEC эсвэл NSEC3 бичлэгийн хэлхээнд тулгуурлан DNS бүсийн оруулгуудыг тоолох боломжтой хэрэгсэл юм.

n3map нь үндсэндээ NSEC3 нь бүсийн тооллогын эсрэг хамгаалалтыг санал болгодоггүй гэдгийг харуулах зорилгоор бичигдсэн. Python хэл дээр бичигдсэн хурдан бөгөөд бүсүүдийг (сая ба түүнээс дээш оруулгатай) тоолох чадвартай.

Энэ нь мөн олж авсан NSEC3 хэшийг хаахад ашиглаж болох энгийн John the Ripper залгаасыг агуулдаг.

NSEC Zone Walking - Тодорхой бүсийг (жишээ нь: example.com) тоолж, олж авсан NSEC/NSEC3 бичлэгүүдийг example.com.zone файлд хадгалах.

-v шилжүүлэгчийг зөвхөн дэлгэрэнгүй мэдээлэл өгөхөд ашигладаг.

Avoiding Sub-Zones – Дэд бүсийн (бидний тоолохыг хүссэн children zone) талаар олон анхааруулгыг хэвлэх болно.

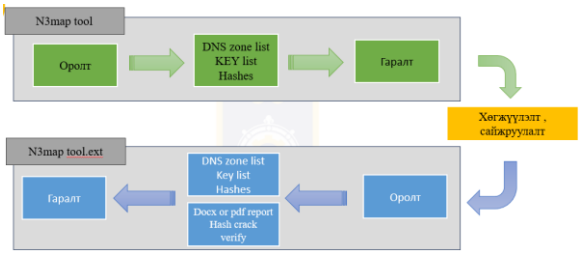
NSEC3 Zone Enumeration- nsec3map өмнө нь хүлээн авсан өөр бичлэгтэй давхцаж буй NSEC3 бичлэгийг хүлээн авах үед тооллогыг цуцлахгүй.

Cracking NSEC3 Hashes

Нэмэлт өгөгдлүүдгүйгээр nsec3map нь тухайн бүс нь NSEC эсвэл NSEC3-ийг ашиглаж байгаа эсэхийг автоматаар илрүүлж, холбогдох тоолох аргыг ашигладаг. Мөн бүсийн нэрийн серверүүдийг өөрөө хайдаг. Зарим нэрийн серверүүд NSEC-ийн хүсэлтийг хүлээн авдаггүй. Ийм тохиолдолд оронд нь --query-mode A (богино -A) ашиглаж болно.

Тодорхой бүсээс NSEC3-ийн зарим бичлэгийг авсны дараа Жон Риппер болон нийлүүлсэн NSEC3

түүлийг ашиглан эвдэж болно.NSEC3 бичлэгүүдийг JtR ашигладаг өөр формат руу хөрвүүлэх шаардлагатай.



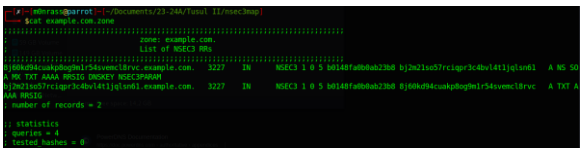
1-Р СХЕМ. БҮТЦИЙН СХЕМ

2-Р СХЕМ. N3MAP ТҮҮЛИЙН АЖИЛЛАГААНЫ ПРОЦЕСС

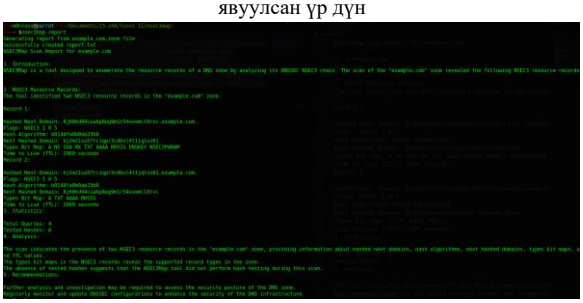
3-Р СХЕМ. N3MAP.EXT ТҮҮЛИЙН АЖИЛЛАГААНЫ ПРОЦЕСС

Үр дүн: N3map түүлийн хэрэглээн дээр тулгуурласан тайлан гаргах хөгжүүлэлт хийгдэж байгаа уг түүлийг тогтсон тайлангийн загвар ашиглаж шаардлагатай мэдээллүүдийг аудит болон нэвтрэлтийн шалгалт хийх процессд хялбаршуулах байдалтайгаар туршихад текст файлын үр дүнг буцааж байгаа.

1-р зураг. N3map түүл Google-н nameserver ашиглан example.com домэйн дээр ажиллаж буй байдал



2-р зураг. N3map түүлийн example.com домэйн дээр enumerate явуулсан үр дүн



3-р зураг. N3map түүлийн текст файлаар гаргасан

НОМ ЗҮЙ

[1] A Security Evaluation of DNSSEC with NSEC3∗ [Jason Bau Stanford University Stanford, CA, USA jbau@stanford.edu, John C. Mitchell Stanford University Stanford, CA, USA mitchell@cs.stanford.edu], 2010

[2] Measuring the Practical Impact of DNSSEC Deployment [Wilson Lian, University of California, San Diego; Eric Rescorla, RTFM, Inc.; Hovav Shacham and Stefan Savage, University of California, San Diego], 2013

[3] A Longitudinal, End-to-End View of the DNSSEC Ecosystem [Taejoong Chung, Northeastern University; Roland van Rijswijk-Deij, University of Twente and SURFnet bv; Balakrishnan Chandrasekaran, TU Berlin; David Choffnes, Northeastern University; Dave Levin, University of Maryland; Bruce M. Maggs, Duke University and Akamai Technologies; Alan Mislove and Christo Wilson, Northeastern University], 2017

[4] DNSSEC as a service – A prototype implementation [Adnath Hemanthindra School of Computing, Middlesex University Mauritius, Flic-en-Flac, Mauritius, Amreesh Phokeer Research & Innovation Dept., AFRINIC, Ebene, Mauritius], 2020

[5] The Sad Story of DNSSEC [Alexander Elliott∗ aelliott41@gatech.edu Georgia Institute of Technology Atlanta, Georgia, USA, John Moxley∗ jmoxley@gatech.edu Georgia Institute of Technology Atlanta, Georgia, USA] 2023

ГҮН ХҮЧ НЭМЭГДҮҮЛСЭН СУРГАЛТЫН АРГААР ХУВЬЦААНЫ АРИЛЖААГ АВТОМАТЖУУЛАХ

[1]Н.Сүхтөмөр, [2]Г.Ганчимэг

[1,2]*Компьютерын ухаан салбар, Мэдээлэл, Холбооны Технологийн Сургууль, ШУТИС, Монгол улс*

[1]*haruschatten@gmail.com,* [2]*ganaa@must.edu.mn*

***Хураангуй*— Гүн хүч нэмэгдүүлсэн сургалтын (DRL) арга нь хувьцааны арилжааг автоматжуулахад ирээдүйтэй машин сургалтын техник юм. DRL агентууд хөрөнгийн зах зээлийн симуляцын орчинтой харилцаж, ашигтай арилжаа хийснийхээ төлөө шагнал хүртэх замаар хувьцааны арилжаа хийж сурах боломжтой. Цаг хугацаа өнгөрөхөд агент нь хүлээгдэж буй шагналаа нэмэгдүүлэх арилжааны стратеги боловсруулж, сурдаг. Энэ өгүүлэлд автоматжуулсан хувьцааны арилжаанд гүнзгий хүч нэмэгдүүлсэн сургалтын (DRL) арга ашиглах боломжтойг үзүүлсэн ба туршилтын үр дүнгүүдээр баталсан.**

Түлхүүр үг— Гүн, хүч, нэмэгдүүлсэн, сургалт, арилжаа, хувьцаа

I. Удиртгал

Гүн хүч нэмэгдүүлэх сургалтын арга (DRL) нь хувьцааны арилжааг автоматжуулахад чухал хэрэгцээтэй машин сургалтын техник юм. DRL агентууд хөрөнгийн зах зээлийн симуляцын орчинтой харилцаж, ашигтай арилжаа хийснийхээ төлөө шагнал хүртэх замаар хувьцааны арилжаа хийж сурах боломжтой. Цаг хугацаа өнгөрөхөд агент нь хүлээгдэж буй шагналаа нэмэгдүүлэх арилжааны стратеги боловсруулж сурдаг. DRL бол хувьцааны арилжааны төрөл бүрийн ажлыг автоматжуулахад ашиглаж болох хүчирхэг хэрэгсэл юм. DRL алгоритмууд улам боловсронгуй болж, улам бүр өргөн хэрэглэгдэж байгаа тул DR аргад суурилсан арилжааны алгоритмууд хөрөнгийн зах зээлд улам бүр чухал үүрэг гүйцэтгэж байна. DRL аргад суурилсан арилжааны алгоритмууд нь уламжлалт арилжааны стратегиас хэд хэдэн давуу талтай байдаг [1-3]. *Үүнд:*

- DRL агентууд хүний оролцоогүйгээр динамик зах зээлийн орчинд хувьцаа худалдаж *(арилжих)* сурах боломжтой.
- DRL агентууд олон хувьцааг нэгэн зэрэг арилжихаас гадна үнийн түүхэн мэдээлэл, зах зээлийн өнөөгийн нөхцөл байдал, мэдээний үйл явдлууд зэрэг олон хүчин зүйлийг харгалзан үзэх боломжтой.
- Түүнчлэн DRL агентуудыг хөрөнгийн зах зээлийн дууриамал орчинд сургах боломжтой бөгөөд энэ нь судлаачдад бодит мөнгөний эрсдэлгүйгээр худалдааны стратегиа туршиж, боловсронгуй болгох боломжийг олгодог.

Гэсэн хэдий ч DRL аргыг бодит орчинд автоматжуулсан хувьцааны арилжаанд өргөнөөр нэвтрүүлэхээс өмнө шийдвэрлэх шаардлагатай зарим бэрхшээлүүд байдаг. Үүнд:

- DRL агентуудыг сургахад тооцооллын хувьд үнэтэй байж болно.
- DRL агентууд шагналын функц болон симуляцын орчны дизайнд мэдрэмтгий байж болно.
- DRL агентуудыг нарийн тодорхой тайлбарлахад хэцүү байж болох бөгөөд энэ нь тэдний шийдвэрт итгэхэд хэцүү болгоно.

Хэдийгээр сорилт бэрхшээлийг үл харгалзан хэрэглэвэл DRL нь автоматжуулсан хувьцааны арилжааны шинэ хандлага юм [1]. Судлаачид дээр дурдсан сорилтуудыг шийдвэрлэхийн тулд идэвхтэй ажиллаж байгаа бөгөөд ойрын ирээдүйд DRL аргад суурилсан арилжааны алгоритмуудыг бодит орчинд ашиглаж болохыг үзүүлэхийг зорьж байна [2]. DRL аргыг хувьцааны автомат арилжаанд хэрхэн ашиглаж болох тодорхой жишээг дурьдвал:

- **Зах зээлийг бий болгох:** DRL агентуудыг зах зээлийн динамик орчинд ашигтай арилжаа хийж сурахад ашиглаж болно. Энэ нь зах зээлийн хөрвөх чадварыг сайжруулж, арилжаа эрхлэгчдэд хувьцаа худалдаж авах, борлуулахад хялбар болгоно.
- **Багцын оновчлол**: DRL агентуудыг хөрөнгө оруулалтын оновчтой багцыг барьж, удирдаж сурахад ашиглаж болно. Үүнийг хөрөнгө оруулагчдад эрсдлээ багасгахын зэрэгцээ ашиг орлогоо нэмэгдүүлэхэд нь туслах зорилгоор ашиглаж болно.
- **Захиалгын гүйцэтгэл:** DRL агентуудыг гүйлгээний зардлыг бууруулж, багцын нийт

ашиг орлогыг нэмэгдүүлэх арга замаар арилжаа хийж сурахад ашиглаж болно.

- **Өндөр давтамжийн арилжаа**: DRL агентуудыг өндөр давтамжийн арилжааны орчинд ашигтай арилжаа хийж сурахад ашиглаж болох бөгөөд арилжаа нь милл секундээр хийгддэг [3].

II. DRL аргад суурилсан арилжаа

DRL аргад суурилсан арилжааны агентийн ерөнхий бүтэц нь дараах байдалтай байна [4-5]. *Үүнд*:

- **State Encoder** нь хөрөнгийн зах зээлийн өнөөгийн байдлыг бодлогын сүлжээнд ашиглаж болох шахсан дүрслэл болгон хувиргах үүрэгтэй. Төлөвийн кодлогчийг хиймэл мэдрэлийн сүлжээ, давтагдах мэдрэлийн сүлжээ, эргэлтийн мэдрэлийн сүлжээ зэрэг машин сургалтын төрөл бүрийн техникийг ашиглан хэрэгжүүлж болно. State Encoder багтсан онцлог шинж чанарууд нь төлөөлөгчийн гүйцэтгэхээр төлөвлөж буй хувьцааны арилжааны тусгай даалгавраас хамаарна. Жишээ нь: DRL аргад суурилсан зах зээл үүсгэгч агент нь хувьцааны одоогийн үнэ, санал хүсэлтийн зөрүү, захиалгын дэвтэр зэрэг функцуудыг агуулж болно. Мөн оновчлолын агент нь багцын бүх хувьцааны одоогийн үнэ, хувьцаа тус бүрийн үнийн түүхэн мэдээлэл, зах зээлийн өнөөгийн нөхцөл байдал зэрэг функцуудыг агуулж болно.
- **Policy network** нь шахсан төлөвийн дүрслэлийг оролт болгон авч, боломжит арилжааны үйлдлүүдийн магадлалын хуваарилалтыг гаргадаг. Агент нь арилжаа хийх арга хэмжээг сонгохдоо магадлалын хуваарилалтыг ашигладаг. Policy network хиймэл мэдрэлийн сүлжээ, давтагдах мэдрэлийн сүлжээ зэрэг машин сургалтын төрөл бүрийн техникийг ашиглан хэрэгжүүлж болно. Бодлогын сүлжээний өвөрмөц бүтэц нь арилжааны боломжит үйл ажиллагааны тоо, төрийн төлөөллийн нарийн төвөгтэй байдлаас хамаарна.
- **Шагналын функц** нь арилжааны тодорхой арга хэмжээ авсны төлөө агентаас авдаг шагналыг тодорхойлдог. Шагналын функц нь агентыг хүлээгдэж буй өгөөжөө нэмэгдүүлэх арилжааны стратегийг сурахад нь туслах зорилготой юм. Шагналын функцийг янз бүрийн аргаар хэрэгжүүлж болно. Жишээ нь: Урамшууллын энгийн функц нь агентийг ашигтай арилжаа хийсний төлөө урамшуулах боломжтой. Илүү боловсронгуй урамшууллын функц нь арилжааны эрсдэл, гүйлгээний зардал зэрэг хүчин зүйлсийг харгалзан үзэж болно.
- **Сурах алгоритм** нь агентийн хөрөнгийн зах зээл дээрх туршлага дээр үндэслэн бодлогын сүлжээг шинэчилдэг. Сурах алгоритмын зорилго нь төлөөлөгчийн хүлээгдэж буй шагналыг нэмэгдүүлэх явдал юм. Сурах алгоритмыг Q-сургалт, бодлогын градиент, гүнзгий Q-сүлжээ зэрэг машин сургалтын төрөл бүрийн техникийг ашиглан хэрэгжүүлж болно. Ашиглаж буй сургалтын тодорхой алгоритм нь төрийн төлөөлөл болон бодлогын сүлжээний нарийн төвөгтэй байдлаас хамаарна [6].

III. Туршилтын үр дүн

Энэхүү судалгаанд бид хувьцааны автомат арилжаанд зориулсан хэд хэдэн DRL аргын гүйцэтгэлийг уламжлалт арилжааны стратегитай харьцуулсан. DRL аргад суурилсан стратегитай харьцуулж болох хэд хэдэн уламжлалт арилжааны стратегийг эхлэл болгон ашиглаж болно. Тодруулбал, бид дараах стратегиудыг харьцуулж үзсэн. *Үүнд*:

- **Идэвхгүй худалдан авах ба хадгалах**: Энэ стратеги нь тодорхой хэмжээний хувьцааг худалдан авч, тодорхой хугацаанд хадгалах явдал юм.
- **Дундаж хэлбэлзэл**: Энэ стратеги нь багцын хэлбэлзлийг багасгахын зэрэгцээ хүлээгдэж буй өгөөжийг нэмэгдүүлэх хувьцааны багцыг сонгох явдал юм.
- **Моментийн арилжаа**: Энэ стратеги нь сүүлийн үед сайн байсан хувьцааг худалдаж авах, муу гүйцэтгэлтэй хувьцааг зарах явдал юм.
- D**RL аргад суурилсан стратеги**: Энэхүү туршилтанд Proximal Policy Optimization (PPO) алгоритмыг ашиглан түүхийн мэдээлэлд үндэслэн хувьцааны арилжаа хийж сурах боломжтой агентуудыг сургасан.

Бид DOW 30 индексийг сонгосон бөгөөд энэ нь АНУ-ын хөрөнгийн зах зээлийн гүйцэтгэлийг илэрхийлдэг, хүмүүс сайн мэддэг, өргөн дагаж мөрддөг индекс юм. Хөрөнгийн арилжаанд түгээмэл хэрэглэгддэг хөдөлгөөнт дундаж болон харьцангуй хүч чадлын индекс (RSI) зэрэг техникийн үзүүлэлтүүдийг тооцоолох замаар бид өгөгдлийг урьдчилан боловсруулсан. Дараа нь бид өгөгдлийг сургалт, туршилтын багц болгон хуваж, сургалтын багц нь 2010-2020 он, туршилтын багц нь 2020-2023 оны өгөгдөл юм. Бид сургалтын багцыг ашиглан DRL агентуудыг сургаж, гүйцэтгэлийг нь үнэлсэн ба дараах хэмжүүрүүдийг хэмжсэн. *Үүнд*:

Хуримтлагдсан өгөөж: Энэ хэмжүүр нь туршилтын хугацаанд оруулсан хөрөнгө оруулалтын нийт өгөөжийг хэмждэг.

Sharpe харьцаа: Энэ хэмжүүр нь багцын хэлбэлзлийг харгалзан эрсдэлд тохируулсан өгөөжийг хэмждэг.

Хамгийн их хасалт: Энэ хэмжигдэхүүн нь багцын оргил цэгээс доод цэг хүртэлх хамгийн их алдагдлыг

хэмждэг. Бид эдгээр хэмжүүрүүдийг ашиглан өөр өөр стратегиудын гүйцэтгэлийг харьцуулж, дараагийн хэсэгт үр дүнд дүн шинжилгээ хийнэ.

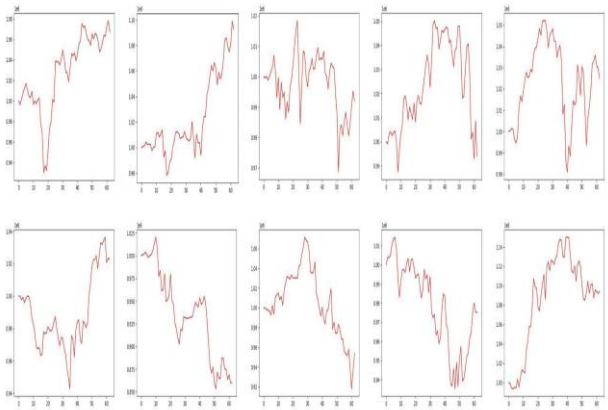
Өгөгдөл бэлтгэх: Өгөгдөл бэлтгэх эхний алхам бол мэдээлэл цуглуулах явдал юм. Энэ тохиолдолд бид DOW 30 индексийн түүхийн хувьцааны өгөгдлийг ашигласан. Мэдээллийг Yahoo Finance эсвэл Quandl гэх мэт янз бүрийн эх сурвалжаас цуглуулж болно. Мэдээллийг цуглуулсны дараа алдаа, зөрчлийг арилгахын тулд тэдгээрийг цэвэрлэх шаардлагатай. Үүнийг давхардсан өгөгдлийг арилгах, дутуу утгыг бөглөх, алдааг засах замаар хийж болно. Дараагийн алхам бол өгөгдлөөс онцлог шинж чанаруудыг боловсруулах явдал юм. Онцлогууд нь DRL агентыг сургахад ашиглагдах хувьсагч юм. Эдгээр нь хувьцааны үнэ гэх мэт энгийн байж болно, эсвэл хувьцааны үнэ болон хувьцааны дундаж үнийн зөрүү гэх мэт илүү төвөгтэй байж болно. Эцсийн алхам бол өгөгдлийг сургалт, баталгаажуулалт, туршилтын багц болгон хуваах явдал юм. Сургалтын багц нь DRL агентийг сургахад, баталгаажуулалтын багц нь агентийн гүйцэтгэлийг үнэлэхэд, туршилтын багц нь үл үзэгдэх өгөгдөл дээр агентийн гүйцэтгэлийг шалгахад ашиглагддаг.

DRL алгоритмууд нь уламжлалт машин сургалтын аргуудыг ашиглан шийдвэрлэхэд хэцүү эсвэл боломжгүй асуудлуудыг шийдвэрлэхэд ихэвчлэн ашиглагддаг. Хамгийн алдартай DRL алгоритмуудын заримаас дурдвал [7-8]:

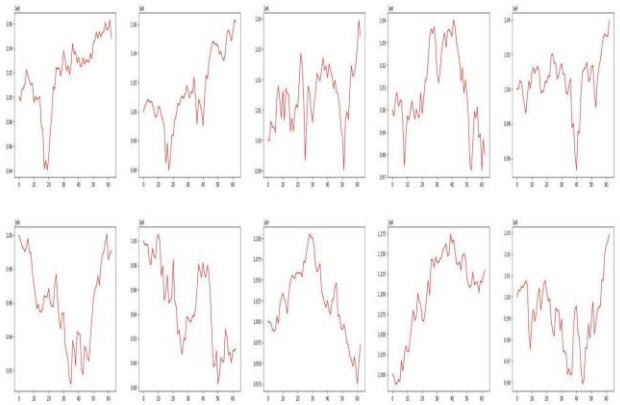
- Proximal Policy Optimization (PPO) нь бодлогын шинэчлэлтүүд хэт том биш байхын тулд итгэлцлийн бүсийг ашигладаг бодлогын градиент алгоритм юм. Энэ нь PPO алгоритмыг Deep Q-Learning гэх мэт бодлогын градиент алгоритмуудаас илүү тогтвортой болгодог.
- Гүн Q сургалт нь хүснэгтийг сурдаг үнэ цэнэд суурилсан алгоритм бөгөөд төлөв байдлын хосыг хүлээгдэж буй урамшуулалтай харьцуулдаг.
- Advantage Actor-Critic (A2C) нь тухайн төлөвт тодорхой арга хэмжээ авах үнэ цэнийг тооцоолохын тулд давуу талын функцийг ашигладаг бодлогын градиент алгоритм.
- Trust Region Policy Optimization (TRPO) нь бодлогын шинэчлэлтүүд хэт том биш байхын тулд итгэлцлийн бүсийг ашигладаг бодлогын градиент алгоритм.
- Deep Deterministic Policy Gradient (DDPG) нь детерминист бодлогыг ашигладаг бодлогын градиент алгоритм [6].

III. Туршилтын үр дүн

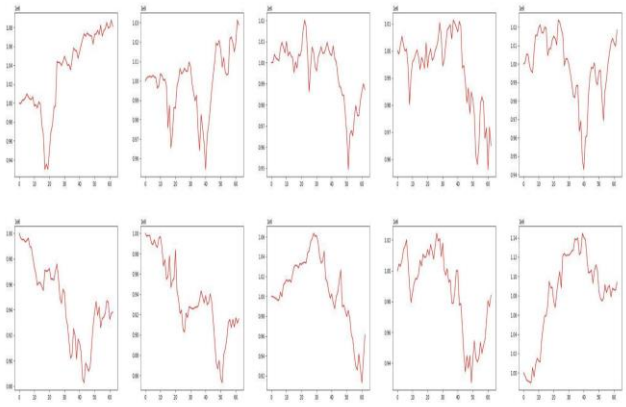
Туршилтын үр дүнг үзүүлсэн 1-4 дүгээр зургаас харахад DRL аргад суурилсан стратегиуд нь хуримтлагдсан өгөөж, sharpe харьцаа, хамгийн их өгөөжийн хувьд уламжлалт стратегиас илүү гарсан байна. Тодруулбал, DRL аргад суурилсан стратегиуд хуримтлагдсан өгөөж нь 7.71%, sharpe харьцаа 0.27, хамгийн их бууралт -27.45% байсан бол уламжлалт стратегиуд хуримтлагдсан өгөөж 10.5% ба түүнээс бага, sharpe харьцаа 0.6 эсвэл бага, хамгийн их таталт -21.94% ба түүнээс дээш байна. Эдгээр үр дүн нь DRL аргад суурилсан стратеги нь автоматжуулсан хувьцааны арилжаанд үр дүнтэй байж, альфа үүсгэж, хэлбэлзлийг бууруулж, зах зээлийн уналтад тэсвэртэй байдлыг сайжруулж чадна гэдгийг харуулж байна.



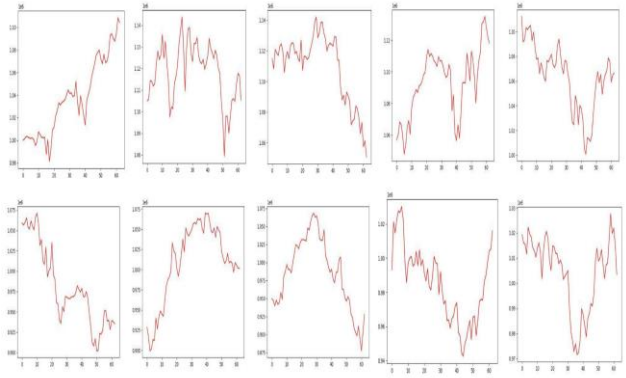
Зураг 1. Дансны үнэ цэнийн баталгаажуулалт A2C



Зураг 2. Дансны үнэ цэнийн баталгаажуулалт DDPG

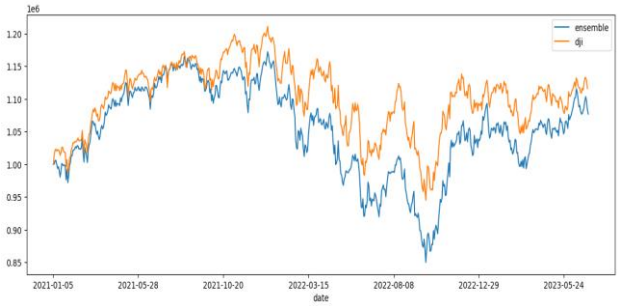


Зураг 3. Дансны үнэ цэнийн баталгаажуулалт PPO



Зураг 4. Дансны үнэ цэнийн баталгаажуулалт Ensemble

Туршилтын хугацаанд өгөөжийн хуваарилалт болон жилийн өгөөжийг судлах замаар бид DRL аргад суурилсан стратегийн гүйцэтгэлд дүн шинжилгээ хийсэн. 5 дугаар зурагт үзүүлсэн бидний үр дүнгээс харахад DRL аргад суурилсан стратеги нь уламжлалт стратегитай харьцуулахад илүү тогтвортой, өгөөжтэй болохыг харуулж байна. Мөн бид стратегийн жилийн хэлбэлзэл, хамгийн их хасалтыг хэмжсэн бөгөөд DRL аргад суурилсан стратегиуд нь ердийн стратегиас бага хэлбэлзэлтэй, хамгийн их бууралттай байгааг олж мэдсэн.



З*ураг 5: Хувьцааны арилжааны гүйцэтгэл*

Ерөнхийдөө бидний үр дүнгээс харахад гүнзгий хүч нэмэгдүүлэх сургалт нь автоматжуулсан хувьцааны арилжааны ирээдүйтэй арга бөгөөд сургалтын алгоритмд бидний санал болгож буй өөрчлөлтүүд нь илүү тогтвортой, ашигтай арилжааны стратегид хүргэж болохыг харуулж байна.

Дүгнэлт

Бидний ажил нь автоматжуулсан хувьцааны арилжаанд гүнзгий хүч нэмэгдүүлсэн сургалтын (DRL) арга ашиглах боломжтойг харуулсан. Бид ганц агент стратеги болон ensemble стратеги зэрэг хэд хэдэн DRL аргуудын гүйцэтгэлийг харьцуулах туршилт хийсэн. Үр дүн нь DRL аргад суурилсан стратегиуд нь хуримтлагдсан өгөөж, sharpe харьцаа, хамгийн их өгөөжийн хувьд уламжлалт стратегиас давж гарсан болохыг үзүүлсэн. Ensemble стратеги нь хамгийн сайн гүйцэтгэлийг үзүүлсэн бөгөөд хуримтлагдсан өгөөж нь 10.5%, sharpe харьцаа 0.6 байна.

Бидний санал болгож буй сургалтын алгоритмын өөрчлөлтүүд нь санхүүгийн арилжаанд илүү тохиромжтой. Бид хувьцааны үр ашгийг дээшлүүлэхийн тулд гүйлгээний зардал болон нэн тэргүүнд тавигдсан үр дүнг дахин тооцдог буферыг тооцдог урамшууллын функцийг ашигласан. Энэ нь илүү тогтвортой, ашигтай арилжааны стратегийг бий болгосон. Энэ судалгааны ажлын үр дүн нь автоматжуулсан хувьцааны арилжааны салбарт оруулж буй томоохон хувь нэмэр болно гэж бид үзэж байна.

Ном зүй

[1] Deep Reinforcement Learning for Automated Stock Trading: An Ensemble Strategy by Hongyang Yang, Xiao-Yang Liu, Shan Zhong, and Anwar Walid (2022).

[2] Logic-guided Deep Reinforcement Learning for Stock Trading by Zhiming Li, Junzhe Jiang, Yushi Cao, Aixin Cui, Bozhi Wu, Bo Li, Yang Liu (2022).

[3] Deep Reinforcement Learning for Active High Frequency Trading by Antonio Briola, Jeremy Turiel, Riccardo Marcaccioli, Alvaro Cauderan, and Tomaso Aste (2021).

[4] Reinforcement Learning for Market Making in a Multi-agent Dealer Market by Sumitra Ganesh, Hua Zheng, Nelson Vadori, Prashant Reddy, Mengda Xu, and Manuela Veloso (2023).

[5] Deep Stock Trading: A Hierarchical Reinforcement Learning Framework for Portfolio Optimization and Order Execution by Rundong Wang, Hongxin Wei, Bo An, Zhouyan Feng, and Jun Yao (2021).

[6] FinRL: Deep Reinforcement Learning Framework to Automate Trading in Quantitative Finance by Xiao-Yang Liu, Hongyang Yang, Jiechao Gao and Christina Dan Wang (2021).

[7] Explainable Deep Reinforcement Learning for Portfolio Management: An Empirical Approach by Xiao-Yang Liu and Mao Guan (2021).

[8] Deep Reinforcement Learning for Trading by Zihao Zhang, Stefan Zohren, and Stephen Roberts (2020).

ДОТООД ОРЧНЫ РАДИО ДОЛГИОН ТАРХАЛТЫН ЧАНАРЫГ АЛХАХ ТЕСТЭЭР ОНОВЧЛОХ

(Отгонбаярын Тэгшжаргал[1]) (Оюунчимэгийн Өлзийхутаг[2])

[1]Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл холбоо технологийн сургууль, Холбооны салбар

Холбоо барих зохиогчийн и-мэйл хаяг: o.tegshjargal@yahoo.com[1]

Хураангуй*: Дотоод орчны радио долгион тархалтын таамаглал нь гадна орчны радио долгионоос зарим талаараа ялгаатай байдаг. Гадна орчны адил зорилго нь шаардлагатай талбайг үр ашигтайгаар хамрах (эсвэл цэгээс цэгийн системийн хувьд найдвартай замыг хангах), саад бартаанаас зайлсхийх явдал юм. Гэсэн хэдий ч доторх орчинд хамрах хүрээ нь барилгын геометрээр, материалаар тодорхойлогддог бөгөөд барилгын хамрах хүрээ нь өөрөө тархалтад нөлөөлнө. Маш богино хүрээ, миллиметрийн долгионы давтамж алдагдаж байна гэдэг нь ойр орчмын жижиг өөрчлөлтүүд нь тархалтын шинж чанарт ихээхэн нөлөөлдөг. Эдгээр хүчин зүйлсийн нарийн төвөгтэй шинж чанараас шалтгаалан дотоод радио системийн тусгай төлөвлөлтийг хийх гэж байгаа бол тухайн сайтын талаар нарийвчилсан мэдлэг шаардагдана, жишээ нь геометр, материал, тавилга, хүлээгдэж буй ашиглалтын хэв маяг гэх мэт. Гэсэн хэдий ч системийн эхний төлөвлөлтийн хувьд тухайн нутаг дэвсгэрт тархсан хөдөлгөөнт станцуудыг хамрах суурь станцын тоог тооцоолох, бусад үйлчилгээ эсвэл системүү- дийн хооронд үүсч болзошгүй саад тотгорыг тооцоолох шаардлагатай. Энэ- хүү хавсралтад голчлон талбайгаас хамааралгүй ерөнхий загварууд болон дотоод орчинд учирч буй тархалтын саатлын талаарх чанарын зөвлөмжийг тусгасан болно.

Түлхүүр үг: ДОТООД ОРЧНЫ РАДИО ДОЛГИОН ТАРХАЛ- ТЫН ЧАНАРЫГ ҮНЭЛЭХ АЛХАХ ТЕСТИЙГ ОНОВЧЛОХ)

I. ДОТООД ОРЧНЫ РАДИО СИСТЕМИЙН ТАРХАЛТЫН БУУРАЛТ БА ЧАНАРЫН ХЭМЖҮҮР

Дотоод орчны долгион тархалтын доголдол нь голчлон доорх шалтгаануудаас үүдэлтэй байдаг:

- Дотоод орчны объектуудын (хана, шалыг оруулаад) эргэн тойрон дахь тусгал, дифракц
- Хана, шал болон бусад саад тотгороор дамжин өнгөрөх дамжуулалтын алдагдал;
- Эрчим хүчний суваг, ялангуяа өндөр давтамжтай коридорт;
- Өрөөн доторх хүмүүс ба объектуудын хөдөлгөөн;
- Замын алдагдал зөвхөн чөлөөт орон зайн алдагдал төдийгүй барилгын материалын саад бэрхшээлээс үүдэлтэй нэмэлт алдагдал;
- Долгионы ойсон болон дифракцийн бүрэлдэхүүн хэсгүүдийн олон замт нөлөө;
- Хөдөлгөөнт терминалыг санамсаргүй байдлаар тохируулсны улмаас үүсэх туйлшралын таарамжгүй байдал

II. САЙТЫН ЕРӨНХИЙ ЗАГВАРУУД

Ерөнхий загвар нь зам эсвэл сайтын мэдээлэл бага шаарддаг бөгөөд дотоод орчны радио замын алдагдал нь замын дундаж алдагдал болон түүнтэй холбоотой сүүдэр бүдгэрэх статистик үзүүлэлтээр тодорхойлогддог. Дотоод орчны долгион тархалтын замын алдагдлын загвар нь олон хана, эсвэл олон давхраар дамжих дохионы чадлын бууралтыг тооцдог. Энэ хэсэгт тайлбар- ласан загвар нь давхруудын хооронд давтамжийг дахин ашиглах зэрэг шинж чанаруудыг хангахын тулд олон давхраас гарах алдагдлыг тооцдог. Доор өгөгдсөн зайн эрчим хүчний алдагдлын коэффициентүүд нь хана, саад тотгороор дамжих мөн барилгын нэг давхарт учирч болзошгүй бусад алдагдлын механизмыг далд хэлбэрээр тооцдог.

Талбайд зориулсан загварууд нь зайн загварт оруулахын оронд хана тус бүрээс учирсан алдагдлыг тодорхой тооцох боломжтой.

Үндсэн загвар нь дараах томъёо байна

$$L_{total}=20\log 10f+N\log 10d+Lf \quad (n)$$

(1.1)

N : зайны чадлын алдагдлын коэффициент;

f : давтамж (МГц);

d : суурь станц ба зөөврийн терминал хоорондын зай (d > 1м байх үед); Lf : шалны нэвтрэлтийн алдагдлын коэффициент (дБ);

n : суурь станц ба зөөврийн терминалын хоорондох давхрын тоо

(n 1)

Орон сууцны барилгад чадлын алдагдлын коэффициентийг заагаагүй бай- вал оффист өгсөн утгыг ашиглаж болно.

Дохио нь олон давхарт нэвтрэлтийн алдагдлаас шалтгаалж нийт алдагдал багатай холбоосыг дуусгах бусад гаднах замыг олж болно.

III. ТАРХАЛТЫН СААТЛЫН ЗАГВАРУУД

- **Олон зам**:

Хөдөлгөөнт/зөөврийн радио тархалтын суваг нь цаг хугацаа, давтамж, орон зайн шилжилтээс хамаарч өөр өөр байдаг. Дамжуулагч ба хүлээн авагч нь тогтмол байдаг статик тохиолдолд ч тараагч ба цацруулагч хөдөлгөөнд байх магадлалтай тул суваг нь динамик байж болно. Олон зам гэсэн нэр томъёо нь тусгал, дифракц, сарнил зэргээр дамжуулан радио долгион нь нэвтрүүлэгчээс хүлээн авагч руу олон замаар дамждагтай холбоотой юм. Замын урттай пропорциональ эдгээр зам тус бүртэй холбоотой цаг хугацааны саатал бай- даг. Эдгээр саатсан дохио тус бүр нь хамрах хүрээтэй бөгөөд цаг хугацааны хувьд өөр өөр шинж чанартай шугаман шүүлтүүр үүсгэдэг.

- **Импульсийн хариу үйлдэл**

Сувгийн загварчлалын зорилго нь радио холболт, системийн загварчлалд ашиглах радио тархалтын үнэн зөв математик дүрслэлийг бий болгоход оршино. Радио суваг нь шугаман байдаг тул импульсийн хариу үйлдэлээр бүрэн дүрслэгдсэн байдаг. Импульсийн хариу үйлдэл тодорхой болмогц радио сувгийн ямар ч оролтод үзүүлэх хариу үйлдэлийг тодорхойлж болно. Энэ нь холбоосын гүйцэтгэлийн симуляцийн үндэс суурь юм.

Импульсийн хариу үйлдлийг ихэвчлэн эхний илрүүлж болох дохиотой харь- цуулахад илүүдэл саатлын функцээр чадлын нягтралаар илэрхийлдэг.

Сувгийн импульсийн хариу үйлдэл нь хүлээн авагчийн байрлалаас хамаарч өөр өөр байдаг ба цаг хугацаанаас хамаарч өөр өөр байж болно. Тиймээс дохио шуугианы нөлөөллийг багасгахын тулд нэг долгионы уртаар хэмжсэн хэмжилтийн дундажаар эсвэл орон зайн дундажийг тодорхойлохын тулд хэд хэдэн долгионы уртаар хэмжиж мэдээлдэг. Аль дундажийг хэлж байгаа дун- дажийг хэрхэн гүйцэтгэсэн талаар тодорхойлох нь чухал. Дундажлах про- цедур нь дараах байдлаар статистик загвар үүсгэх явдал юм: Импульсийн хариу үйлдлийн тооцоолол (чадлын саатлын түвшин) тус бүрийн хувьд TD дундаж саатлын өмнөх ба дараах хугацааг олох, үүнээс цааш чадлын оргил нягтын хувьд тодорхой утгуудаас (–10, –15, –20, –25, 30 дБ) хэтрэхгүй байна.

- ***Дундаж тархалтын саатал***

Чадлын саатлын түвшинг нь дээр дурдсанчлан ихэвчлэн нэг буюу хэд хэдэн параметрээр тодорхойлогддог. Эдгээр параметрүүдийг хэд хэдэн дол- гионы уртын хэмжээс бүхий талбайн дундаж үзүүлэлтээр тооцоолно. Дуу чимээг хасах босго буюу хүлээн авах шалгуур, жишээлбэл профайлын оргилоос 30дБ доогуур байвал энэ нь босго хэмжээнээс хамаарч үүссэн тархалтын саатлын хамт мэдээлнэ.

Хэдийгээр дундаж тархалтын саатлыг маш өргөн ашигладаг боловч энэ нь үргэлж хангалттай шинж чанартай байдаггүй. Тархалтын саатал нь тэмдгийн үргэлжлэх хугацаанаас хэтэрсэн олон замт орчинд, фазын шилжилтийн модуляцын битийн алдааны харьцаа нь дундажаас бус хүссэн долгионы хүсээгүй хүлээн авсан чадлын харьцаанаас хамаарна. Энэ нь ялангуяа өндөр тэмдэгтийн хурдтай системд тод илэрдэг боловч олон замын бүрэлдэхүүн хэсгүүдийн дунд хүчтэй давамгайлах дохио тэмдэгтийн түвшин бага байгаа үед ч илэрдэг.

Дундаж тархалтын саатал ашиглах давуу тал нь загварын гаралтын параметрын загварыг энгийн хүснэгт хэлбэрээр илэрхийлэх боломжтой. Ердийн тархалтын саатал параметрүүдийг тооцоолсон гурван дотоод орчны саат- лын дундаж үзүүлэлтийг Хүснэгт 1-д үзүүлэв. Эдгээр утгууд нь 1900 МГц ба 5.2 ГГц-ийн бүх чиглэлтэй антеннуудын хэмжилт дээр үндэслэсэн болно. Хүснэгт 1-д А багана нь ихэвчлэн тохиолддог бага (маш бага бус) утгыг илэрхийлнэ, В багана нь байнга тохиолддог дундаж утгыг илэрхийлнэ С багана нь ховор тохиолддог маш өндөр саатлын утгыг илэрхийлнэ. Хүснэгтэнд өгөгдсөн утгууд нь орчин бүрт таарч болох хамгийн том өрөөний хэмжээг илэрхийлнэ.

Барилга дотор антеннуудын хоорондох зай ихсэх тусам тархалтын саатал өсөх хандлагатай байдаг улмаар замын алдагдал ихсэнэ. Антеннуудын хоорондох зай ихсэх тусам зам саад болж хүлээн авсан дохио нь бүхэлдээ тархай бутархай замаас бүрдэх болно.

Давтамж	Орчин	A	B	C
1 900 МГц	Орон сууц дотор	20	70	150
1 900 МГц	Оффис дотор	35	100	460
1 900 МГц	Үйлчилгээний төв дотор	55	150	500
5.2 ГГц	Оффис дотор	45	75	150

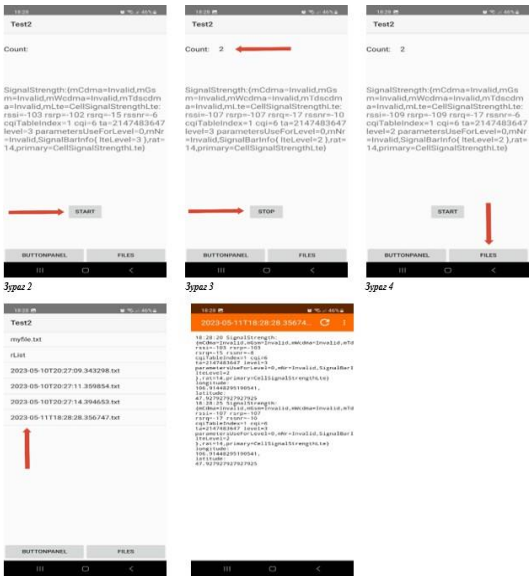
Хүснэгт 1: Дундаж тархалтын саатлын параметрүүд

Статистик загварууд нь олон тооны хэмжилтийн үр дүнг дамжуулах симу- ляцид ашиглаж болох байдлаар нэгтгэн дүгнэдэг. Жишээлбэл, симуляцийг салангид өргөн суурин хамааралгүй тараалтын (WSSUS) сувгийн загвараар хийж болно. Үүнийг хийх нэг арга бол бодит сувгт байж болох олон тархай бутархай замыг загварт хэдхэн олон замт бүрэлдэхүүнээр солих явдал юм. Дараа нь n загварын олон замт бүрэлдэхүүн хэсгийн сааталтай n ойролцоо сааталтайгаар янз бүрийн өнцгөөс ирж буй шийдэгдээгүй олон замт бүрэлдэхүүн хэсгүүдийн суперпозицийг Гауссын цагийн нарийн төвөгтэй хувилбар боловсруулдаг

IV. Төслийн үр дүн

Дотоод орчны радио долгион тархалтын чанарыг үнэлэх, оновчлох алхах тестийн судалгаа" дипломын сэдвийн судалгаанд үндэслэн радио долгион тархалтын чанарыг үнэлэх алхах тестийг гүйцэтгэ- хийн тулд зохион бүтээсэн аппликэйшн ба туршилтын үр дүнтэй танилцана уу.

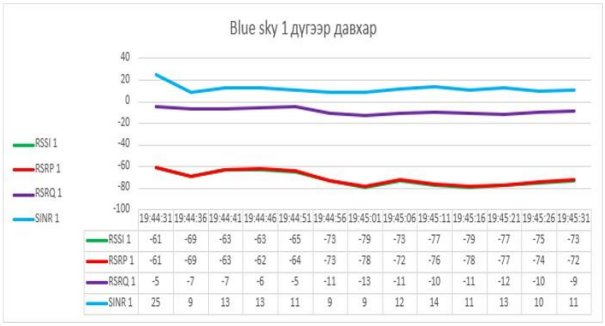
1 Дотоод орчны радио долгион тархалтын чанарыг үнэлэх алхах тестийн аппликэйшн



Зураг 2 Зураг 3 Зураг 4

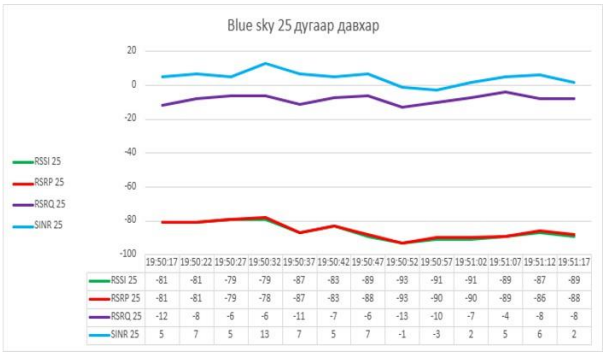
Зураг 1.1: Аппликэйшн ашиглан хийсэн туршилтын үр дүн

2 Аппликэйшн ашиглан хийсэн туршилтын үр дүн



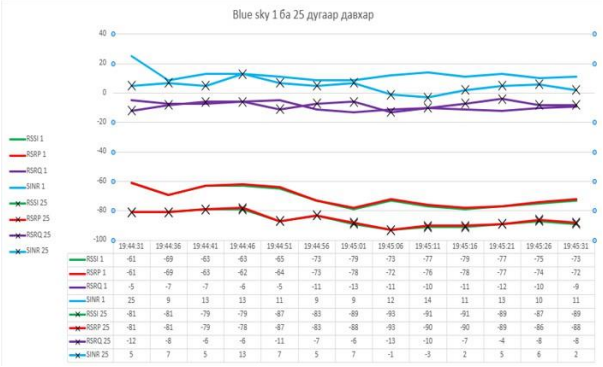
	19:44:31	19:44:36	19:44:41	19:44:46	19:44:51	19:44:56	19:45:01	19:45:06	19:45:11	19:45:16	19:45:21	19:45:26	19:45:31
RSSI 1	-61	-69	-63	-63	-65	-73	-79	-73	-77	-79	-77	-75	-73
RSRP 1	-61	-69	-63	-62	-64	-73	-78	-72	-76	-78	-77	-74	-72
RSRQ 1	-5	-7	-7	-6	-5	-11	-13	-11	-10	-11	-12	-10	-9
SINR 1	25	9	13	13	11	9	9	12	14	11	13	10	11

Зураг 2.1: Blue sky 1 дүгээр давхар



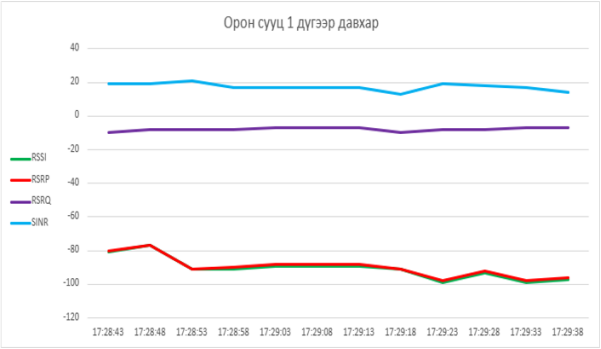
	19:50:17	19:50:22	19:50:27	19:50:32	19:50:37	19:50:42	19:50:47	19:50:52	19:50:57	19:51:02	19:51:07	19:51:12	19:51:17
RSSI 25	-81	-81	-79	-79	-87	-83	-89	-93	-91	-91	-89	-87	-89
RSRP 25	-81	-81	-79	-78	-87	-83	-88	-93	-90	-90	-89	-86	-88
RSRQ 25	-12	-8	-6	-6	-11	-7	-6	-13	-10	-7	-4	-8	-8
SINR 25	5	7	5	13	7	5	7	-1	-3	2	5	6	2

Зураг 2.2: Blue sky 25 дугаар давхар



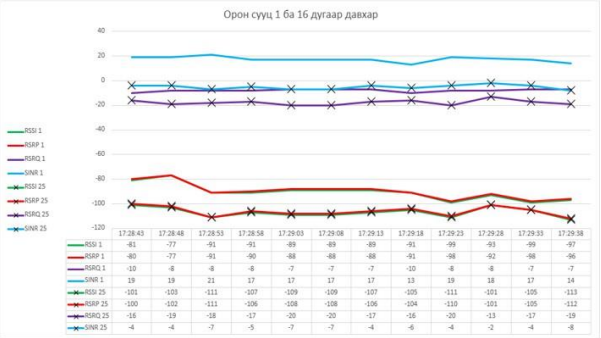
	19:44:31	19:44:36	19:44:41	19:44:46	19:44:51	19:44:56	19:45:01	19:45:06	19:45:11	19:45:16	19:45:21	19:45:26	19:45:31
RSSI 1	-61	-69	-63	-63	-65	-73	-79	-73	-77	-79	-77	-75	-73
RSRP 1	-61	-69	-63	-62	-64	-73	-78	-72	-76	-78	-77	-74	-72
RSRQ 1	-5	-7	-7	-6	-5	-11	-13	-11	-10	-11	-12	-10	-9
SINR 1	25	9	13	13	11	9	9	12	14	11	13	10	11
RSSI 25	-81	-81	-79	-79	-87	-83	-89	-93	-91	-91	-89	-87	-89
RSRP 25	-81	-81	-79	-78	-87	-83	-88	-93	-90	-90	-89	-86	-88
RSRQ 25	-12	-8	-6	-6	-11	-7	-6	-13	-10	-7	-4	-8	-8
SINR 25	5	7	5	13	7	5	7	-1	-3	2	5	6	2

Зураг 2.3: Blue sky 1 ба 25 дугаар давхар



Зураг 2.1: Орон сууц 1 дүгээр давхар

Зураг 2.2: Орон сууц 16 дугаар давхар



Зураг 2.3: Орон сууц 1 ба 16 дугаар давхар

ДҮГНЭЛ

Сэдвийн хүрээнд бүтээсэн аппликейшнийг ашиглан дотоод орчинд цуглуулсан өгөгдлийн мэдээллээр хийсэн дүн шинжилгээ нь сүлжээний нөхцөл байд- лын бодит дүр төрхийг харуулдаг бөгөөд төлөвлөлт, дизайнаас эхлээд систе- мийг оновчтой болгох, засвар үйлчилгээ хийх сүлжээний чанар, багтаамж, хамрах хүрээг нэмэгдүүлэх зэрэг хэд хэдэн чиглэлээр асуудал шийдхэд ашиг- лаж болно.

1-р давхар ба 25-р давхрын сүлжээний утгууд -20дБм зөрүүтэй байгаа нь бааз станцын байрлал, барилгын материал, тавилгуудын үзүүлэх нөлөө, хө- дөлгөөнт объектуудын нөлөө, хана, шал болон бусад саад тотгороор дамжин өнгөрөх дамжуулалтын алдагдал зэргээс шалтгаалж буйг туршилтын үр дүн харуулж байна.

АШИГЛАСАН МАТЕРИАЛ, НОМ ЗҮЙ

[1] P Series. “Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz”. **in***Recommendation ITU-R*: (2012), **pages** 1238–7.

[2] Telco Antennas. 4G LTE Signal Strength Reference Guide. 2021.

ВЕБ АППЛИКЕЙШН ДЭЭРХ RACE CONDITION ЭМЗЭГ БАЙДЛЫГ ИЛРҮҮЛЭХ, АШИГЛАХ НЬ

Удирдагч багш: Б.Мөнхбаяр (Ph.D)
Л.Уламбаяр[1], О.Оюумаа[1], Б.Хулан[1], М.Отгонбаяр[1]
Монгол улс, Улаанбаатар, ШУТИС, Мэдээлэл, Холбооны технологийн сургууль, Мэдээллийн Сүлжээ, Аюулгүй байдлын салбар

Хураангуй

Интернет орчинд ашиглаглагддаг гол хэрэгсэл бол вебсайтууд юм. Вебсайт болгоны зорилго, хамрах хүрээ өөр өөрийн онцлогтой ч тухайн вебсайтуудад алдаа дутагдал, эмзэг байдлууд хөгжүүлэгч болон өөр бусад хүчин зүйлсээс шалтгаалан олон бий. Тэдгээр эмзэг байдлууд нь байгууллагыг тухайн вебсайтын үзүүлэх үйлчилгээ, хэрэглэгчдэд нөлөөлөх байдал цаашлаад санхүүгийн олон төрлийн асуудалд оруулж болох эрсдэлтэй. Бид энэ асуудлыг авч хэлэлцэн ялангуяа худалдааны зорилгоор үйлчилгээ явуулдаг вебсайтууд дээр түгээмэл байдаг эмзэг байдал болох Race Condition эмзэг байдлыг судлан, үзүүлэх нөлөөлөл, үүсч болох эрсдэл, хохиролуудыг багасгахын тулд судалгаа, туршилтын ажил хийсэн.

Хугацаа болоод кодын алдаатай логик ажиллагаанаас болж энэхүү эмзэг байдал үүсдэгийг туршилтаар нотлов.

Түлхүүр үг: Race condition, уралдааны нөхцөлт эмзэг байдал, уралдааны цонх

I. УДИРТГАЛ

Харилцаа холбоо, худалдаа болон бусад олон чухал үйлчилгээнүүдийн тулгуур болж байгаа мэдээллийн технологийн эрин үед вэб программын аюулгүй байдал хэзээ ч ийм чухалд тооцогдон яригдаж байгаагүй билээ. Бүх зүйлс интернетээр дамжин хөгжиж, дэлхийн өнцөг булан бүрт интернет хэрэглээ, цахим худалдаа үйлчилгээний салбарууд нэмэгдэн эрчимтэй хөгжиж байна. Интернет ертөнц ингэж хурдацтай хөгжихийн хэрээр интернет орчинд асар их мөнгөний урсгал бий болоод түүнийг хамарсан зүйлс рүү чиглэсэн аюул заналхийлэл, халдлага өдөр тутам бүр цаг минут тутамд нэмэгдэж байна. Техник технологи хөгжсөн орчин үед худалдаа үйлчилгээний газрууд бүгд цахим хэлбэр /вебсайт/ рүү шилжин үйл ажиллагаагаа явуулж байна.

Мэдээллийн эрин зуунд халдагчдийн хийж буй үйлдлүүдийн 95% нь вэбсайтууд руу чиглэсэн байна [1]. Вэбсайт дотроо хамгийн их хувь эзэлж байгаа нь цахим худалдааны чиглэлээр үйл ажиллагаа явуулдаг газрууд байна [2]. Худалдан авагчид ч мөн цагаа хэмнэн аль болох хэрэгцээт зүйлсээ хялбараар онлайн дэлгүүрүүдээс захиалан авахыг эрмэлзэх болжээ. Цахим хэлбэрээр өөрийн хүссэн бараа бүтээгдэхүүн, эд зүйлсээ захиалж худалдан авалт хийх нь цаг хэмнэх давуу талтай ч тухайн барааг худалдаалж буй вебсайт, аппликейшн дээр байж болохуйц эмзэг байдлууд нь санхүүгийн алдагдал үүсгэж болно. Үүний нэгэн жишээ нь сүүлийн жилүүдэд ихээхэн хохирол амсуулаад байгаа халдлагын нэг болох RACE CONDITION ATTACK буюу "уралдааны нөхцөлт халдлага" юм. Орчин үеийн вэб программуудын ихэнх нь асинхрон програмчлал тэр дундаа JavaScript код ашиглах замаар хөгжүүлэлт, шинэчлэлт хийн бидний ашигладаг вэб хуудас, онлайн үйлчилгээний хөгжүүлэлтийг хийж байна. Энэ нь хэрэв хөгжүүлэгч тухайн вэб программд аюулгүй байдлын хамгаалалт хийгээгүй тохиолдолд бидний төслийн ажил болох уралдааны нөхцөлт халдлага хэрэгжих боломжтой болж байгаа гэсэн үг юм.

II. ОНОЛЫН ХЭСЭГ

Race condition буюу уралдааны нөхцөл нь бизнесийн логик алдаатай нягт холбоотой нийтлэг эмзэг байдал юм. Энэ нь вэбсайтууд зохих хамгаалалтгүйгээр хүсэлтийг нэгэн зэрэг боловсруулах болон илгээх үед үүсдэг бөгөөд ижил өгөгдөлтэй хугацааны хувьд нэгэн зэрэг харилцан үйлчлэлцэх хэд хэдэн ялгаатай урсгал явагдсаны, улмаар 'мөргөлдөөн' үүсч, тухайн програмд тооцоологдоогүй үйлдэл хийхэд хүргэдэг. Уралдааны нөхцөл байдлын халдлага нь санаатай мөргөлдөөн үүсгэж, энэхүү санамсаргүй үйлдлийг хорлонтой зорилгоор ашиглахын тулд цаг хугацааны хувьд нарийн тохируулсан хүсэлтийг ашигладаг.

Вэб програмууд дахь уралдааны нөхцөлийг сервер талын болон хэрэглэгч талын уралдааны нөхцөл гэж хоёр төрөлд ангилдаг.

- Хэрэглэгч талын уралдааны нөхцөл: JavaScript вэб программууд сервер-үйлчлүүлэгчийн харилцаанд AJAX-г ашиглах үед клиент уралдааны нөхцөл үүсч болно. Асинхрон хүсэлт (асинхрон скрипт, гадаад эх сурвалжид хандах хүсэлт гэх мэт) нь хэрэглэгчийн уралдааны нөхцлийг үүсгэдэг.
- Сервер талын уралдааны нөхцөл: Олон процессууд хангалттай синхрончлолгүйгээр нийтлэг өгөгдөлд нэвтэрч, ядаж нэг нь нийтлэг өгөгдөл дээр бичихээр төлөвлөж байгаа үед үүсдэг.

Ихэнх вэб сайтууд олон урсгалыг ашиглан нэгэн зэрэг хүсэлтийг зохицуулдаг бөгөөд бүх хүсэлтүүийг нэгдсэн мэдээллийн сангаас уншиж, бичдэг. Веб болон аппликешны кодыг зэрэгцүүлэн ашиглах эрсдэлийг бодолцож бүтээх нь хөгжүүлэгчдийн хувьд ховор байдаг тул уралдааны нөхцөл байдал нь вэбийн сул тал болж байна.

Техник хангамжийн түвшинд уралдааны нөхцөл байдлыг ашиглан дараах байдлаар эмзэг байдал үүсгэж болно.

Хоёр урсгал нь глобал бүхэл тоон хувьсагчийн утгыг 1-ээр нэмэгдүүлнэ гэж бодъё. Хамгийн тохиромжтой нь дараах үйлдлүүдийн дараалал хийгдэнэ.

thread 1	thread 2		integer value
			0
read value		<-	0
increase value			0
write back		->	1
	read value	<-	1
	increase value		1
	write back	->	2

Хүснэгт 1. Бүхэл тоон урсгалыг 1-ээр нэмэгдүүлэх үеийн энгийн үйлдлийн дараалал.

Дээр үзүүлсэн тохиолдолд эцсийн утга нь 2 байна. Гэсэн хэдий ч, хэрэв хоёр хэлхээг түгжих эсвэл синхрончлолгүйгээр нэгэн зэрэг ажиллуулж байвал үйлдлийн үр дүн буруу гарах магадлалтай. Доорх үйлдлийн дараалал нь энэ хувилбарыг харуулж байна.

thread 1	thread 2		integer value
			0
read value		<-	0
	read value	<-	0
increase value			0
	increase value		0
write back		->	1
	write back	->	1

Хүснэгт 2. Хугацааны агшинг ашиглан уралдааны нөхцөл үүсгэж өөрчилж буй үйлдлийн дараалал.

Limit overrun race condition :

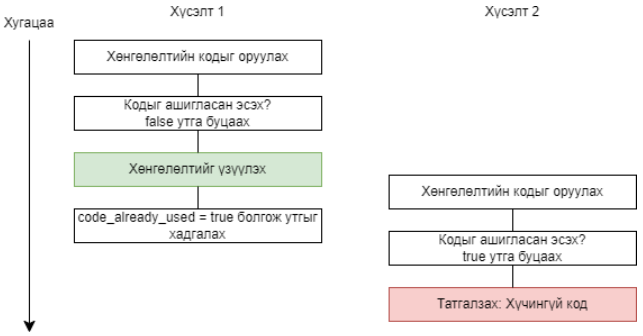
Race condition ашигласан веб exploit нь ихэвчлэн limit overrun race condition байдаг бөгөөд энэ нь ямар нэгэн хязгаарлалтыг давж, олон хүсэлтүүдийг илгээх аргаар race condition-ийг хэрэгжүүлдэг, Жишээлбэл:

- Бэлгийн картыг давтамжтай ашиглах
- Нэг хөнгөлөлтийн кодыг дахин дахин хэрэглэх
- Дансны үлдэгдэлээс илүү бэлэн мөнгө авах, шилжүүлэх
- Нэг CAPTCHA шийдлийг дахин ашиглах гэх мэт

Жишээлбэл, захиалгын үнийн дүнгээс хямдруулахын тулд төлбөрийн явцад хөнгөлөлтийн код оруулах боломжтой онлайн дэлгүүрийг авч үзье. Хөнгөлөлтийг хэрэгжүүлэхийн тулд програм нь дараах логик дараалалтай байж болно.

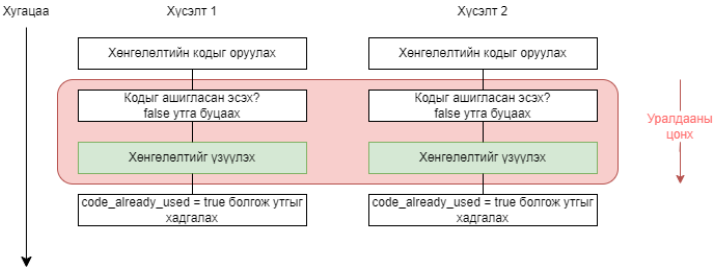
1. Хөнгөлөлтийн кодыг ашигласан эсэхийг шалгах.
2. Нийт захиалгын үнийн дүнгээс хөнгөлөлтийг хасах.
3. Хөнгөлөлтийн кодыг ашигласан эсэхийг мэдээллийн санд бүртгэн, шинэчилэх

Хэрэв ашигласан хөнгөлөлтийн кодыг дахин ашиглахыг оролдвол процессын эхэнд хийсэн анхны шалгалтууд дараах байдлаар сэргийлнэ:



Зураг 1. Хугацааны хувьд дараалласан 2 хүсэлт илгээх үед веб хүсэлтийг биелүүлэх дараалал

Харин өмнө нь хөнгөлөлтийн кодоо ашиглаж байгаагүй хэрэглэгч бараг ижил хугацаанд хоёр удаа хүсэлт явуулж хэрэглэхийг оролдвол дараах байдлаар эмзэг байдал үүсэх магадлалтай.



Зураг 2.Хугацааны хувьд нэгэн зэрэг 2 хүсэлт илгээх үед веб хүсэлтийг биелүүлэх дараалал

Уралдааны цонх (race window) : 2 болон хэд хэдэн хүсэлтүүд мөргөлдөх буюу collision үүсэх боломжтой хугацаа. Энэ цонх нь ихэвчлэн миллисекунд, түүнээс ч богино байж болно.

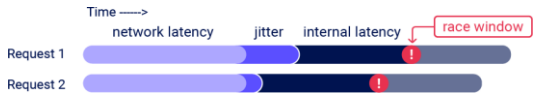
Дээр харуулж буй жишээ (зураг1,2) програм нь дэд төлөвөөр (sub-state) дамждаг; өөрөөр хэлбэл хүсэлтийг боловсруулж дуусахаас өмнө орж ирээд

гардаг төлөв юм. Энэ тохиолдолд дэд төлөв нь серверт эхний хүсэлтийг боловсруулж эхлэх үед эхэлж, оруулсан хөнгөлөлтийн кодыг ашигласан болгож, мэдээллийн баазад шинэчлэх үед дуусна. Энэ нь уралдааны жижиг цонхыг үүсгэж байгаа бөгөөд энэ үеэр хөнгөлөлтийг хэдэн ч удаа давтан авах боломжтой болж эмзэг байдал үүсэж байна.

III. СУДАЛГААНЫ ХЭСЭГ

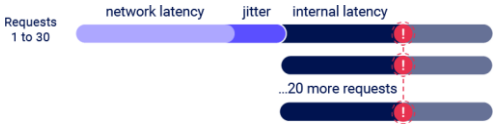
Race condition эмзэг байдлыг илрүүлэхийн тулд доорх бүтцийн схемийн дагуу туршилт хийхийг зорьсон. Судалгааны обьект нь сонголтот динамик вебсайт байна.

Өмнө нь дурьдсанчлан уралдааны цонх нь миллисекундээр хэмжигдэх богино хугацаанд үүсдэг тул хүсэлтүүдийг гар аргаар яг нэгэн зэрэг илгээсэн ч практик дээр хэзээ, ямар дарааллаар боловсруулахад нөлөөлдөг янз бүрийн хяналтгүй, урьдчилан таамаглах боломжгүй гадны хүчин зүйлүүдээс шалтгаалан хугацааны хувьд хоцрогдолтойгоор буюу ялгаатайгаар серверт очдог.



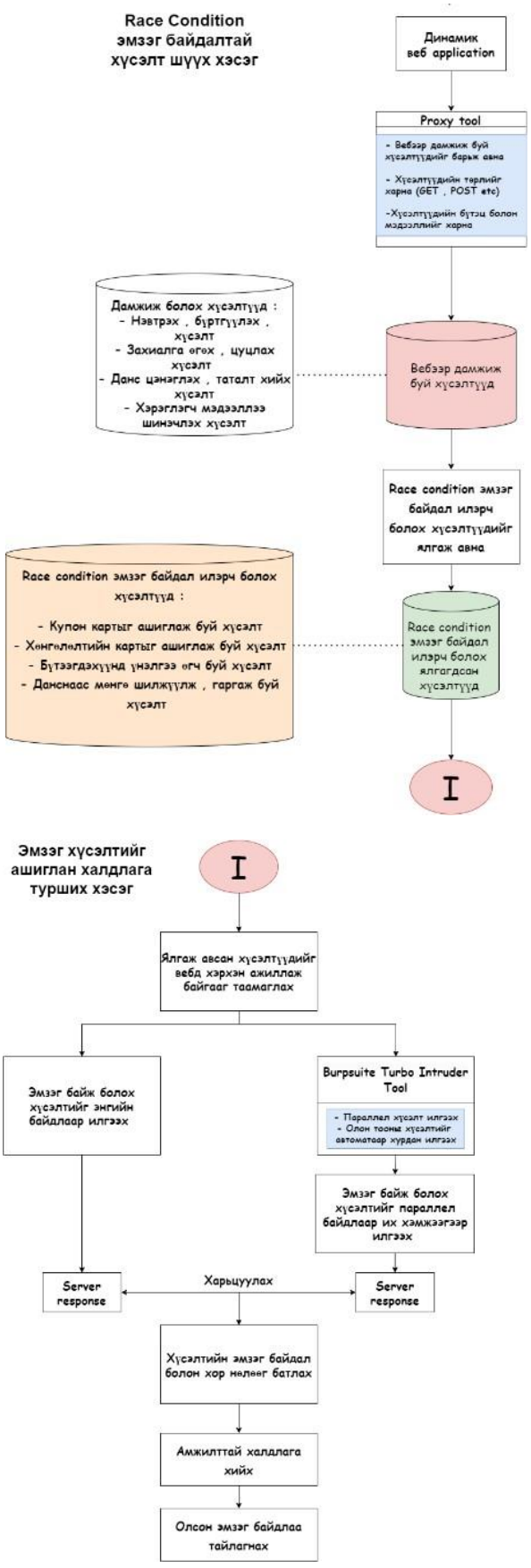
Зураг 3. Үүсэж болох сүлжээний хоцрогдол

Тиймээс туршилтандаа Burp suite хэрэгслийн өргөтгөл хэрэгсэл болох Turbo intruder-г ашигласан. Хэрэгсэл ашигласнаар гадны хүчин зүйлсийн нэг болох сүлжээний нөлөөллийг эрс багасгаж, параллель хүсэлтийн бүлгийг өөрсдийн нэгэн зэрэг илгээх боломжтой болгодог.



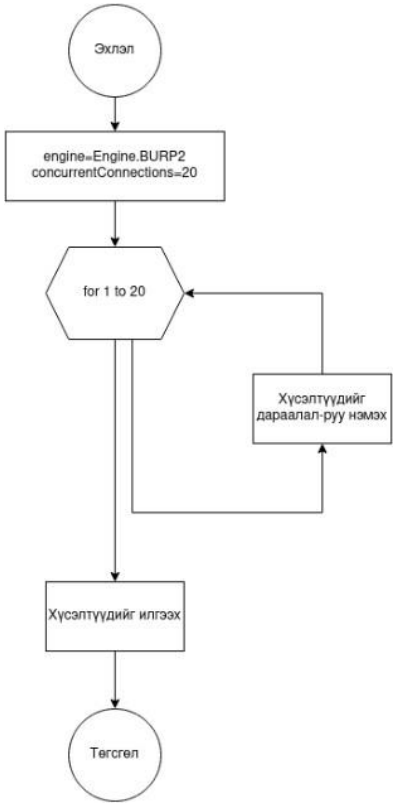
Зураг 4. Proxy хэрэгсэлл ашиглан сүлжээний хоцрогдоллийг арилгасан байдал

1. Вебээр дамжиж буй хүсэлтүүдийг барьж авах хэрэгтэй. Ингэхдээ proxy хэрэглсэл ашигласан.
2. Барьж авсан хүсэлтүүд дотроос эмзэг байдал илэрч болох хүсэлтүүдийг ялган барьж авсан.
3. Бүтцийн схемд үзүүлсэний дагуу барьж авсан эмзэг байдалтай байж магадгүй хүсэлтээ Turbo Intruder нэртэй proxy хэрэгсэл ашиглан параллель байдлаар их хэмжээгээр хугацааны нэг интервалаар веб рүү илгээх мөн эмзэг байж болох хүсэлтийг энгийн байдлаар илгээж үзсэн.
4. Илгээсэн 2 төрлийн хүсэлтийн серверээс өгсөн response утгуудыг харьцуулан харсан.
5. Үр дүн дээр дүн шинжилгээ хийн эмзэг байдлыг тодорхойлсон.



Зураг 5. Race condition эмзэг байдлыг илрүүлэх бүтцийн схем

Дараах алгоритмоор халдлагыг гүйцэтгэхэд ашиглах буюу Turbu Intruder-т хэрэглэж буй кодын алгоритмыг зурсан.



Зураг 6 . Хугацааны тодорхой интервалд олон тооны параллель хүсэлт илгээх алгоритмын бүтэц

```
# Хүсэлтүүдийн дараалал үүсгэх,BURP ENGINE 2 ашиглаж илүү
хурдан болгох
# 2 удаагийн параллель хүсэлт илгээх concurrentConnections=20
тохиргоо
def queueRequesta(target, wordlists)
   engine RequestEngine(endpoint target.endpoint,
   concurrentConnections 20,
   engine Engine.BURP2

# Зэрэг явуулах 20 хүсэлтүүдийг дараалал руу оруулах
   for 1 in range(20):
engine.queue(target.req, gate race1'))

#engine-ий дараалалд оруулсан хүсэлтүүдийг race үүсгэх
параллелаар илгээх
   engine.openGate('races')


def handleItesponse[rea, interesting);
# Серверээс ирсэн хариуг UI хүснэгт рүү нэмэх
   table.add(req)
```

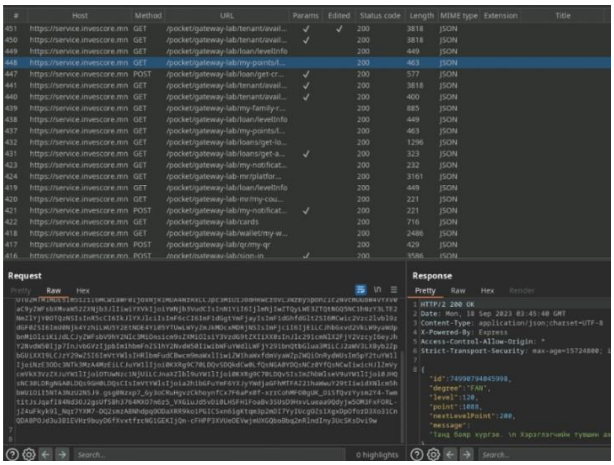
Зураг 7. Алгоритмын бүтцийн дагуу Python хэл дээр бичсэн код

IV. ҮР ДҮН

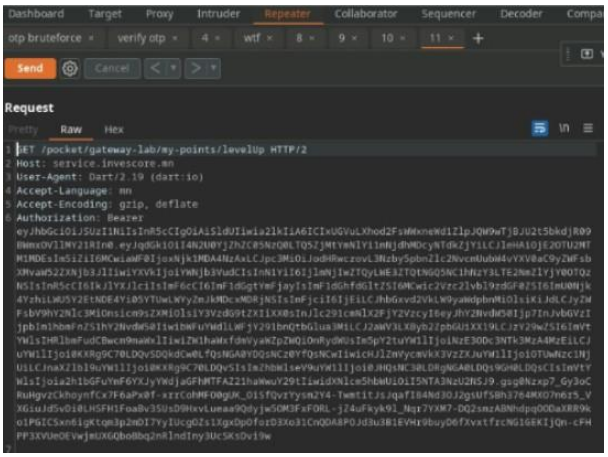
Сонголтот вебсайт дээрээ бүтцийн схемийн дарааллын дагуу алхмуудыг хэрэгжүүлэн туршиж үзсэн ба үр дүнгийн зургуудыг тайлбарын хамт доор хавсаргав.

Бид уг веб аппликейшний хэрэглэгч 200 оноо цуглуулсан тохиолдолд түвшин ахих сонголтыг сонгож өөрийн хэрэглэгчийн эрхээ нэмэгдүүлэх үйлдэл дээр туршилтаа гүйцэтгэсэн.

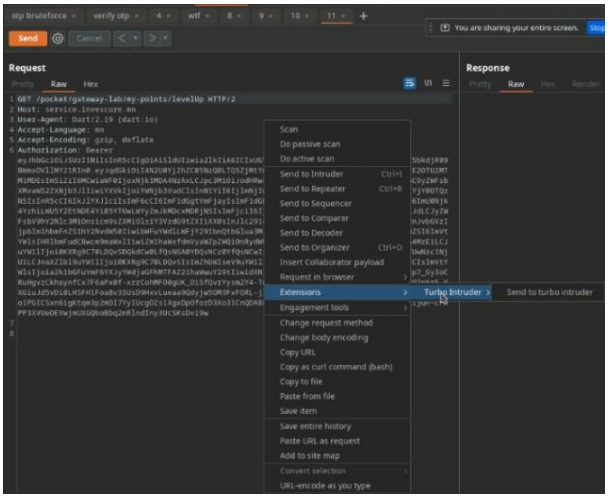
Зураг 8. Хэрэглэгчийн анхны онооны мэдээлэл



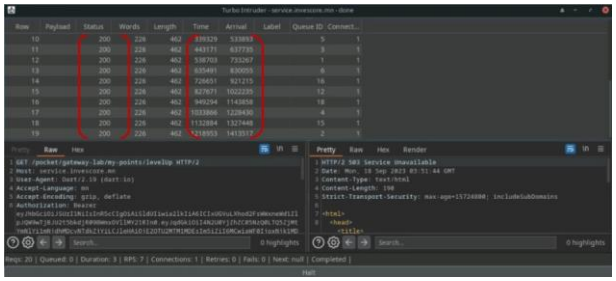
Зураг 9. Бүтцийн схемийн алхам 1 дээрх үйлдэл буюу Burpsuite хэрэгсэл ашиглан вебээр дамжиж буй хүсэлтүүдийг барьж авсан нь



Зураг 10. Бүтцийн схемийн алхам 2 дээрх үйлдэл буюу барьж авсан хүсэлтүүд дотроос эмзэг байдал илэрч болох хүсэлтээ сонгосон. Туршилт хийх levelup хүсэлт



Зураг 11. Бүтцийн схемийн алхам 3 буюу Turbo Intruder хэрэгсэл ашиглан levelup хүсэлтийг сонгон 20 хүсэлт хугацааны тодорхой интервалд илгээх үйлдэл гүйцэтгэсэн.



Зураг 12. 20 хүсэлт илгээсний дараа серверээс өгсөн response ба үүнээс харвал хүсэлтийн статус код 200, хүсэлт хоорондох хугацаа маш бага, илгээсэн 20 хүсэлт амжилттай биелэснийг харуулж байна.

Зураг 13. Үр дүнд буюу хэрэглэгчийн оноо ахисан байдалтай гарсан ба энэ нь туршилт амжилттай болсныг илэрхийлэв.

Хүсэлтийн статус код	Хүсэлт илгээсэн хугацаа	Хүсэлтийн хариу ирсэн хугацаа	Хугацааны зөрүү [мсек]
200	3393329	533893	-
200	443171	637735	0,103
200	538703	733267	0,095
200	635491	830055	0,096
200	726651	921215	0,091
200	827671	1022235	0,101
200	949294	1143858	0,121
200	1033866	1228430	0,084
200	1132884	1327448	0,099
200	1218953	1413517	0,086

Хүснэгт 3. Хүсэлт хоорондын хугацаа

Дээрх хүснэгтэд хүсэлтүүдийн response өгсөн хугацаануудын хоорондох зай нь маш бага буюу мсек-ээр хэмжигдэж байна. Олон хүсэлт зэрэг явуулахад тухайн хүсэлтүүдээс 200 статустай “хүсэлт амжилттай” гэсэн response өгсөн тул туршилт амжилттай болж байгааг илэрхийлж байна.

ДҮГНЭЛТ

Race condition үүсэж болох нөхцөл байдлыг зөв тодорхойлж, уг эмзэг байдлыг зөв илрүүлэхэд судалгааны ажлын үр дүн оршино.

Уг эмзэг байдал нь программын алдаатай логик ажиллагаа, хугацааны интервалд явуулж буй олон хүсэлтүүдээс шалтгаалж үүснэ. Эмзэг байдалтай байж болохуйц вебсайтын талбарууд хэрэглэгчээс оролт авдаг, хямдралын купон тооцдог, данснаас үлдэгдлээс илүү мөнгө авах зэрэг тохиолдлууд орно.

Race condition халдлага амжилттай болсон буюу сонголтот вебсайт дээр Race Condition халдлага хэрэгжих боломжтойг илэрхийлэх шинж чанарууд:

Олон тооны параллел хүсэлтүүдийг Turbo Intruder хэрэгсэл ашиглаж илгээсний дараа :

- Ямар нэг хэмжүүр утга (Бонус оноо гэх мэт) хэвийн хэмжээнээс гажуудаар өөрчлөгдсөн.
- Нэг хөнгөлөлтийн картыг 2 болон түүнээс дээш тоогоор ашиглагдсан.
- Бүтээгдэхүүн эсвэл үйлчилгээнд 2 болон түүнээс дээш тоогоор үнэлгээ өгсөн.
- Хэрэглэгчийн хэтэвчний тооцоо алдагдсан
- Anti-Brute Force rate limit-ийг bypass хийсэн

бол эмзэг байдалтай байх боломжтой гэж үзэж байна.

НОМ ЗҮЙ

[1] Zhang, Lu, and Chao Wang. "RClassify: classifying race conditions in web applications via deterministic replay." 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE). IEEE, page 281, 2017

[2] Albert, Therese J., Kai Qian, and Xiang Fu. "Race condition in ajax-based web application." Proceedings of the 46th Annual Southeast Regional Conference on XX. 2008.

[3] Alidoosti, Mitra, Alireza Nowroozi, and Ahmad Nickabadi. "Business-layer client-side racer: dynamic security testing of the web application against client-side race condition in the business layer." International Journal of Information Security (2023): 1-26.

[4] James Kettle Director of Research PortSwigger research,Smashing the state machine: the true potential of web race conditions first presented at Black Hat USA 2023.

[5] Zhang, Jianyin, Sen Su, and Fangchun Yang. "Detecting race conditions in web services." Advanced Int'l Conference on Telecommunications and Int'l Conference on Internet and Web Applications and Services (AICT-ICIW'06). IEEE, 2006