International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

A Deep CNN Framework for UAV Intrusion Detection in Intelligent Systems

Dr. V. Arulalan[1], Dr. G. Balamurugan[2], Dr. V. Premanand[3]
[1]Assistant Professor, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology ,Kattankulathur 603203,Tamil Nadu, India
arulalav@srmist.edu.in
[2]Assistant Professor, Department of Computing Technologies, Faculty of Engineering and Technology, SRM Institute of Science and Technology ,Kattankulathur 603203,Tamil Nadu, India
balamurg1@srmist.edu.in
[3]Assistant Professor,School of Computer Science and Engineering,Vellore Institute of Technology,Chennai Tamil Nadu, India
premanand.v@vit.ac.in

Abstract— Unmanned Ariel Vehicle (UAV) s are dealing with several safety and protection issues including internal hardware/software and potential attacks. In addition, detecting UAV anomalies will be a crucial responsibility to defend against hostile enemies and prevent accidents. In this research, we present a UAV and an Automatic Dependent (AD) system using surveillance and Machine Learning (ML) algorithms to analyze data from their detectors in real-time. Proposed Improved Region based Convolutional Neural Network (IRCNN) model used to generate and acquire the characteristics of untreated sensor information and characteristics to facilitate AD. The proposed model creating an Inertial Measurement Unit (IMU) & UAV sensors dataset using cyber security simulation system and Active Learning (AL) identifies aggressions based on the least probable interrogation method. This proposed model enables the identification to efficiently improve the occurrences of unexplained aggressions discovered of IRCNN at reduced labeling cost. A thorough trial showed that IRCNN-AL is effective at detecting unknown threats with frequency improvements of between 9% and 30% on comparison approaches. The AL methodology presented with as few as 1% of a labeled unexpected aggressions.
Keywords-component; formatting; style; styling; insert.

I. INTRODUCTION

Some problems arise from the rapidly expanding use of UAVs; Cyber security is the biggest issue. In addition to commercial usage, UAVs have a safety problem. Cyber-attacks are detected too late have catastrophic repercussions [1]. The captured UAV submitted to Inversion Engineering and a replica created for use of UAVs very common in commercial, public safety, and private environments [2]. Unfortunately, an increasing number of unintended and deliberate drone-related incidents have been documented, including mid-air crashes at airports, the smuggling of illegal products, or unauthorized ecosystems. As a result, methods for locating and recognizing UAVs have been thoroughly researched in the literature [3-4]. A system that combined the use of multivariate signal computing and ML methods was proposed the first major contribution to precise localizing and detecting trespassing UAVs within regulated airspace. The calculations demonstrate that the proposed strategy consistently surpasses its rival methods in terms of various performance metrics. UAVs are often the object of many cyber-attacks such as Jamming, Denial of Service (DoS), Malware insertion in the center, and Global Positioning System (GPS) spoofing. The GPS spoofing assault is the most prevalent of these cyber-attacks. Any vehicle that uses a GPS receiver and UAVs could be targeted for GPS spoofing attacks [5]. This proposed article uses the technique for detecting GPS spoofing aggressions based on ML and Deep Learning (DL). The majority of approaches use CNN, RNN, MLP and LSTM. In addition, the training method uses information from flight logs, various signal features, and spectrograms.

II. RELATED WORK

There is various examples of Intrusion Detection (ID) based on DL and theYOLOv2 single object detection method are used in the literature. This study proposes rapid R-CNN with two separate backbones, VGG16 and ZFNet. It is also proposed to use RFCN and ResNet101 for the detection portion of the drone detection and monitoring system. R-CNN faster with ResNet101 used to build a collection of simulated images to process scattered datasets [6–8]. Critical infrastructure operator safety procedures are enhanced by accurate identification of intrusive objects by the computer vision-based detector.

The program used advanced driver assistance, GPS, the smart Internet of Vehicles (IoV) offer dependable and essential automotive connectivity. It is one of the most important methods for utilizing ITS to create smart cities. To provide

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

users with more bandwidth, several networking solutions, including the 5G communication network recently implemented in connected vehicles [9]. Accordingly, privacy-sensitive data from users are sent through IoVs and it was the network to the customer as the individual could be a potential assault. IoV was increasingly endangered by various malware as a result of its opening [10]. The distributed DoS assault also called brute force attack is a major threat to automobiles in the meantime overwhelming their memory and computational power. To protect the safety and privacy of users, identification methods have attracted increasing interest in IoVs [11].

Data taxonomy should focus on identification techniques based on signatures and abnormalities. To perform identification signature-based methods use a database in an identification system [12], reporting irregular pattern signatures from known intrusions. In this case, the IDS compares the characteristics with the assault characteristics are collected to determine if an intrusion occurred. The major disadvantage of signature-based techniques was the susceptibility to incursions through new and unidentified attackers [13]. Network data are analyzed by anomalous-based algorithms, which identify aggressions based on the particular characteristics of the network data [14]. Anomalous-based algorithms could identify unidentified aggressions of new malware, but they have a high rate of false warnings.

IDS performance has been ensured to actual-time ID & IoV due to considerable advances in signature-based IDS techniques [15]. The authors use a quantitative approach to examining IoV traffic flows to identify networks and more attacks. This technical method is the challenge of IDS as a hypothesis test for gathering network traffic streams. The IDS developed can decide whether to accept or reject the information based on an informed traffic flow assessment [16]. Rogue nodes and threats have been successfully identified through the proposed intrusion detection system [17]. However, performance is drastically reduced to multiple strikes. The author is created at the light IDS DDoS attack, reliability target, and creating false alarms in mind [18]. The IDS should be relevant detection rules to recognize the associated attacks and separately identify each assault.

ML based identification achieved a level of development appropriate to the rapidly developing area of Artificial Intelligence (AI). Authors [19] surveyed on the question of ID and its associated overhead. They developed a mechanism for identifying the Bayesian game model, on the compromise between false positive rates and overheads. In addition, researchers [20] built distributed IDS depending on calculating fog to IoTs using extreme sequential ML online. In contrast to conventional IDS is centralized from a recognized intrusion and deciphered the attacker using fog nodes. A traffic-based, botnet-based IDS has been proposed, and decision-making on botnet detection has been implemented using a set of network features and a feature selection method [21]. To minimize false alarms, in-DL techniques are used for identification. An example is the deep hierarchical structure, which combines a multi-layered perceptron and a Recurrent Neural Network (RNN). In addition, a network of simple feed forward neurons with three hidden layers has been constructed from ID & IDS in software-defined networks.

To cross-check their status during run-time, redundant systems often use redundant hardware and software components [22]. Duplicates are only required for the operation of the critical system, ultimately increasing the complexity and cost of the system. For instance, to support certain redundancy-based techniques, many versions of the same controllers would need to be created. Moreover, it is physically impossible to duplicate UAV parts, redundant techniques are not able to address the abnormal status of component failures [23]. The behavior-based methods use a description to define typical system functions. Restrictions were generally programmed based on the description of the program status or the performance duration of a particular operation [24]. Behavioral techniques focus mainly on program-level abnormalities, where system activities are considered abnormal if predetermined limits are respected. However, several program-level reasons can contribute to the aberrant state of a UAV system.

The rule-based & signature-based IDS were used in previous works of drone networks. The management was difficult and involved manual signature updates & regulation setup making them to identify unidentified assaults [25]. An anomaly was the ID method extensively used in the UAVs network correlating new information with characteristics of the typical normal category and designating a dramatic divergence of normal category anomaly. In contrast to the signature and regulation methods, it protect UAVs threats of the DoS [26] introduced an anomaly-based identification method. The proposed ID system was tested using traffic data gathered from UAV networks, and it was found to be effective in detecting DDoS attacks on a flying ad hoc network [27]. Test results have shown acceptable performance in identifying different attacks; however, tests are required to ensure efficacy. Rapidly growing ML or DL lately, it facilitate many UAV platforms have included Jetson AI components from Nvidia [28]. DL and ML method based on training allows us to follow the state of health of a system. The basic difficulty of training techniques should be too great quality data collection with enough normal and unusual supporting documents, in particular abnormal data [29].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

III. UAV CONSTRUCTION

As shown in Figure 1, there are three major steps to the construction of our detecting system: (1) gathering data to IMU sensors during normal and unusual UAV operations; (2) selecting, learning, & optimizing the most effective DNN techniques for UAV anomaly detection; and (3) developing the detecting system using the DNN method. Consumers describe each phase of our property in detail in the following sections. When DL models are formed, collecting high-quality data is a crucial element that allows for the required method. As a result, the first stage of our construction entails gathering an equitable dataset that comprises enough IMU sensor information on both normal and unusual UAV functions [30]. Regularly flying UAVs can easily gather common data; however, the following two factors make it difficult to get enough aberrant data: Data of aberrant status under various conditions, including the change of unusual condition in terms of UAV type, power, length, regularity, patterns, and IMU parameters included in a great-quality data points. The failure of UAVs owing to aberrant function conditions in field trials could result in high research expenses due to the need to repair equipment. To facilitate data collection and training on DNN models, researchers could create UAV flight plans that capture the normal and abnormal conditions of UAVs. An illustration of the associated IMU detector dataset about the acceleration x to the unstable state of the UAV is shown in Figure 2. The researchers have reproduced several flight plans with 7 flight hours, including standard flight plans with various anomalies inserted to collect training information.

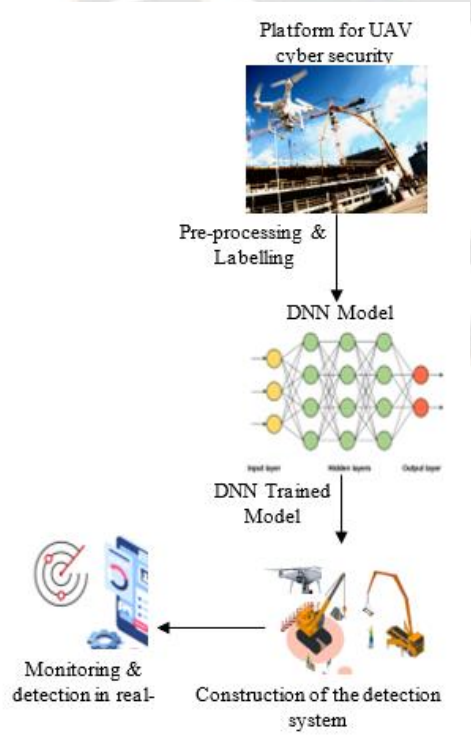

Figure 1: Overview of Construction

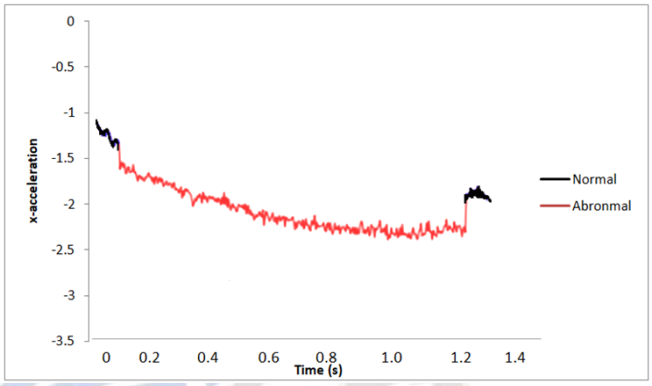

Figure 2: Abnormal Status in a Flying

The researchers implemented several time frames for the time series data they collected during the simulation to be ready for training. On the data that the researchers have collected, they modify the window duration from 0.5 seconds to 5 seconds, and they express the timeframe as a data matrix. However, a period would also require more information about the UAV to complete real-time surveillance and identification [31]. The researchers categorize a time timeframe as unusual T% of the dataset were unusual labeling the collected time windows. To maximize the detection rate, the value of T can be used as a limit and modified. A tiny number of anomalous datasets could be generated by external forces of UAV movement brought on by wind, the value of T is limited; it could result in a large error-positive value. Big T can also fail to recognize short, abnormal statuses that have enough abnormal data points. Researchers constructed a time frame of 0.5 seconds and a T% of 40% by the findings of our assessment.

IV. ACTIVE LEARNING

The researchers proposed IRCNN-AL method, which has been used in biomedical applications. For labeling and initial learning, these existing AL approaches selecting a limited number of cases that can accurately represent the entire unprocessed database [32]. Our method concentrates on learning through actual unidentified attacks that should appear in the training dataset and aims to choose a limited subset of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

cases that more accurately represent the most recent unidentified threats.

V. IRCNN-AL METHODOLOGY

In this article, they develop the IRCNN-AL framework, a CNN that combines open identification and identification of unknown attacks. The proposed IRCNN-AL model is an approach for classifying (N +1) categories, where N represents the total number of training courses that are known to exist and 1 stand for the lone unknown class. Figure 3 depicts the structure of the neural network system, which consists of two convolution methods & maximum cumulating levels, and connected layers. The RCNN model employs the softmax layer to moderate the initiation parameters of the fully linked final stage and compel the total of the outcome variable to equal 1. When unknown samples are present, the RCNN method to the softmax level would be overconfident since the softmax layer should continue to output a high likelihood to the closest established learning category to 1. DNN uses the OpenMax15 level, the SoftMax level, high-value theory, and meta appreciation to accomplish recognition.

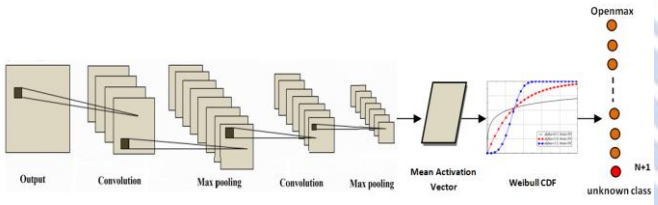

Figure 3: IRCNN- AL pattern to detect unknown attacks.

To create the preformation structure, they use the learning traffic information of well-known categories. From there, researchers can extract the activator variables from the completely connected final layer, V(x). Enablers may reveal information about the association of categories. According to the available research, it is also possible to use the meta-recognition technique on the penultimate level of the statistical method could be studied using the high-value concept and primarily represents the Weibull distribution. The possibility of OpenMAX normalization about unknown attacks could be obtained by applying a high quantity meta-recognition to the initiation matrices of the densely integrated final level.

Using the accurately categorized traffic examples in the testing dataset, they construct the Mean Activation Vector (MAV) for each class M = [m1,..., mN] to prevent the introduction of misclassified information. The example of the separation of the properly categorized traffic examples and the corresponding MAV was chosen to match the Weibull distribution. LibMR WeibullFitHigh feature can be used to create the Weibull fit framework for each category.

$$P_y = (t_y, \lambda_y, k_y) = Weibull(|u_y - m_y|, \eta) \quad (1)$$

Researchers recalibrate the activity matrix of the final completely connected layer to determine the likelihood of the unidentified assaults using the Weibull CDF likelihood of the traffic example separation is used. Firstly, they assess Weibull's CDF probability using weights from the most active categories.

$$W_{r(y)}(i) = 1 - \frac{\alpha - y}{\alpha} - \left(\frac{|u(i) - t_{i(y)}|}{\lambda_{i(y)}}\right)^{k_{i(y)}} \quad (2)$$

The OpenMAX layer was linked to the completion connected level, and the OpenMAX likelihood of category could be calculated utilizing the newly validated matrices, which are the following,

$$P^*(j = y|i) = \frac{e^{u_{y(i)^*}}}{\sum_{y=1}^{N+1} e^{u_{y(i)^*}}} \quad (3)$$

Algorithm 1: Unknown Attack Detection using IRCNN-AL Algorithm

Input: Known class of traffic data; Unknown class of attack data; a represents modify classes

Output: Known class of probability predictive value as $prob_{1...N+1}$

Step1: Enable MAV for known data of Weibull of each class
Step 2: Preprocessing: RCNN with known classes trained datasets
Step 3: Extract the penultimate layer of activation vector u (i)
Step 4: for known class **do**
{
Step 5: Compute MAV with trained dataset correctly.
}

Step 6: fit Weibull model, $P_y = (t_y, \lambda_y, k_y), y = 1, \ldots, N$
}
Step 7: Unknown network attack detected
Step 8: **for** y = 1, 2...., α **do**
{
Step 9: Recomputed the weights of each class probability
}
Step 10: Recomputed the AV of the traffic samples u(i)*
Step 11: Compute the AV of network attacks $u_{N+1}(i)$*
Step 12: **Get** the probability of output values of both attacks $prob_{1...N+1}$

It was discovered that it is possible to compute OpenMAX likelihood for N available training program and unidentified attack category. A proposed open-set recognition model may identify unknown threats by using the OpenMAX likelihood for the network threats, in contrast to the nearest set classification method, which could outcomes the forecast likelihood of the N category. Algorithm 1 shows the precise steps of the overall algorithm to detect unknown attacks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

VI. SECURITY-RELATED ISSUES

Labeling and expert labeling are two crucial processes in the AL methodology. An inquiry was another word for choosing an observation for labeling. The in formativeness criterion is typically the foundation of query tactics. The model could be trained properly from a limited amount of tagged data after selecting the most informative observations for tagging. In this article, categorization uncertainty is assessed using the least reliable The AL query criterion was OpenMax likelihood. This is a beneficial system to learn with uncertain observation because the greatest OpenMax likelihood of detection was limited, the variability should be significant. Since then, detection of aggression assessment of IRCNN-AL must be classified into fine-grain aggression classes; the researchers examine the OpenMax probability at the lowest level of certainty. The least confidence was indicated by the observation of unidentified aggressions which IRCNN-AL identified as follows:

$$cl_x = \max_y P^*(j_x = y|i_x) = P^*(j_x = N + 1|i_x) \quad (4)$$

where P (yi = j|xi) is the diagnosis likelihood of the observation xi belonging to the jth category, whereas the maximum forecast likelihood of the observation of an unknown assault corresponds to the (N +1) class. Consumers order every observation of the unidentified assaults discovered by the IRCNN-AL model in increasing order based on the score, and then designers choose the observations of the highest rankings for labeling. The intrusion detection system is updated to account for novel assaults while retaining knowledge of previously learned categories using the differently labeled data to network threats and initial learning material. Figure 4 illustrates the entire AL process for unidentified assaults.

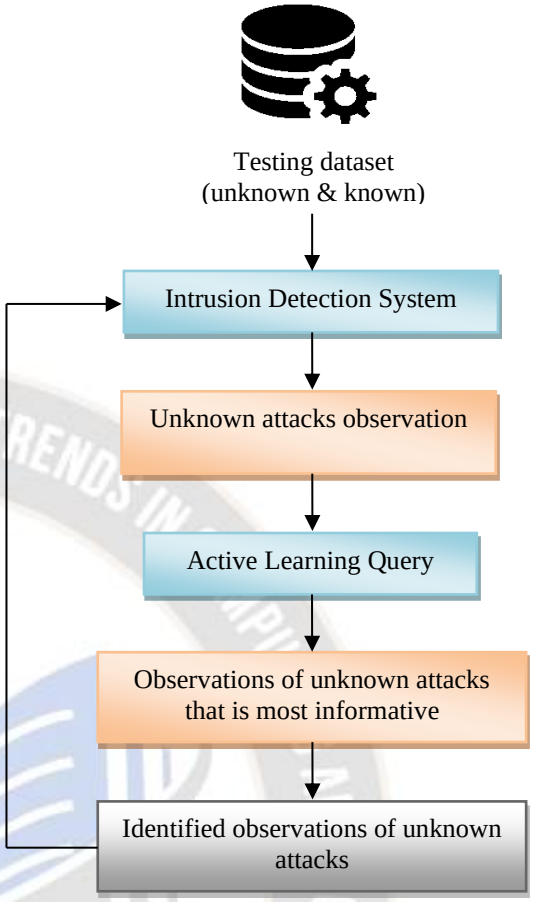

Figure 4: Hypothetical Active Learning Methodology.

Consumers are building the AD system as depicted in Fig. 5 using the CNN methodology. The pre-packaged RCNN method has been installed in the UAV system. The UAV continuously monitors and analyzes the IMU detector data of the schedule selected to the performed RCNN method to detect anomalies in real time. It produces if the data is abnormal or supplies the RCNN model with the processed IMU sensor information. Our method considers a two-level abnormal assessment throughout the detection phase, i.e., a great-level alert to the likelihood of the examined data being unusual was above 65%, and a less-level alert in other cases. Our technology would alert the UAV system immediately to start its safety tactics should a high-level alert be found. When a low-level alert was identified, the system would run secondary evaluations, and if the low-level alert was found within the following time frames, the low-level alert would be upgraded to a high-level alert.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

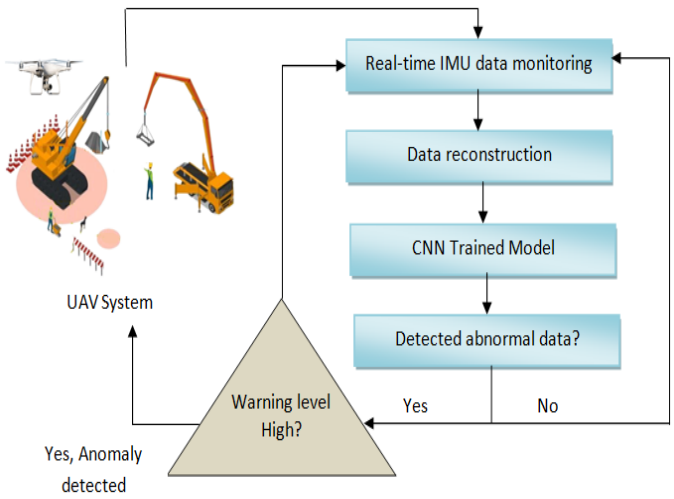

Figure 5: System for Detecting UAV Anomalies

VII. EXPERIMENTATION AND DISCUSSIONS

This article proposed strategies to test; they use the CTU 1 data set and the CICIDS2017 2 data set. Both data sets collect unprocessed traffic information to the actual network ecosystem t and record it to pcap files. The BotNet traffic information gathered from CTU University is known as the CTU database. It includes a sizable volume of BotNet traffic along with background and regular traffic. It should be various kinds of BotNet transformed to various contexts. CICIDS2017 database that was compiled to the CNSI in 2017 and is open source covers a variety of network attack types as well as a vast amount of actual file data. Researchers randomly select the typical form and nine varieties of threats as recognized categories of IRCNN-AL system formation because the CTU database consists of a variety of types of attacks. The types of aggressions are considered unknown in the experiments. In addition, four types of unidentified attacks are randomly chosen from the CICIDS2017 database. Information on known and unidentified aggressions used in the studies is presented in Table 1.

Table 1 the specifics of common threats.

Dataset	*Known Atta*	*Number*	*Dataset*	*Unknown A*	*Number*
CTU Dat	*Benign*	65923	*CTU Datase*	*Simda*	36548
	*CoinMiner_*	17648		*TrickBot*	31284
	Sathurbot	15948		*HTBot*	15313
	Trickster	14741		*Artemins*	10941
	WebCompar	12364		*Ursnif*	10629
	Oh_None	10241	*CICIDS2021*	*Ddos*	16020
	Dridex	6802		*Dos_hulk*	15123
	CoinMiner	1052		*Botnet*	1444
	Viaxmr	1033		*Webattack*	1356
	Trojan	1024			

In addition, they choose 30% of the different classifier databases for the available test data and 70% of the known training database. Regarding the unidentified assaults, they choose 70% of the database for these categories to test the IRCNN-AL framework, and the remaining 30% are utilized to test the proposed ed AL strategy. To ensure the objectivity of the assessment findings for the IRCNN-AL model, they randomly down sample the unknown assaults with more than 10,000 samples, keeping just 3500 samples for each of them.

Since the suggested IRCNN-AL system was a class classification model (N 1), researchers use categorization performance and measure F as indices to assess Open efficiency. IRCNN is to discuss the proposed AD system rate, since the diagnosis method could be represented as a categorization problem with 2 groups, i.e. Normal and abnormal, the True Positive Rate (TPR) and False Positive Rate (FPR) were designed to quantify the performance of our detection system using the curve of the operating characteristics of the receiver. F P R = F P/ F P +T N evaluates the error made by the diagnosis technique to categorize normal data as abnormal, where F N and T N signify false negative and true negative, accordingly. T P R = T P/ T P F N assesses the capabilities of the diagnosis method to precisely detect unusual data. Since the F P R of our suggested detection system was determined to the Area of ROC Curve, our goal is to lower F P R & raising T P R.

VIII.EVALUATION RESULTS

Researchers conducted in-depth experiments as part of our assessment to examine the effects of several elements on the choice of DNN methods, the size of the identification timeframes, and the limited value T, on the effectiveness of our suggested detection system. In addition, to confirm the effectiveness of our detection system evaluation considers many types of abnormal conditions. First, they assess various DNN models performed on the detection system. Six distinct DNN designs based on CNN and LSTM were developed and evaluated. 200 periods are used to form all classifiers. The CNN-based detection method, as illustrated in Figure 6, has an AUC of 0.82. It should also be noted that systems that incorporate IRCNN-AL levels are LSTM compliant only. CNN is therefore used to develop our detection methodology.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

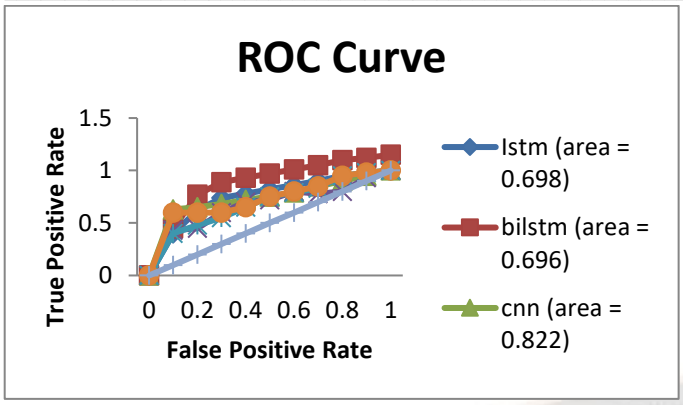

Figure 6: Assessment findings for several systems

The CNN-based detector system shown in Figure 7, they modify the time range used to detect the aberrant state from 0.5 seconds to 5 seconds. Although the 5-second timeframe to AUC = 0.921 provides the best detection rate, it greatly extended the amount of time needed to collect actual-time information of diagnosis. Early diagnosis of anomalies is critical to safeguard the UAV from safety concerns risks & hardware problems, as fault diagnosis are a time-sensitive activity of UAVs. For example, to get an AUC of 0.826, our identification algorithm uses a 0.5-second time window. Since T% = 20% gets the best performance with AUC = 0.871 and a significantly lower criterion would also boost the susceptibility of the classification algorithm to an unstable state of UAVs, T% = 20% is used in our build.

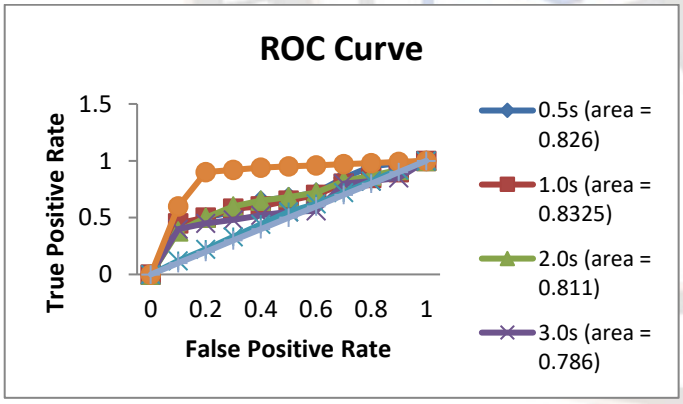

Figure 7: Evaluation results for multiple periods.

Consumers assess the efficiency of the detection system against a variety of anomalies. Researchers start by thinking about anomalies that have an impact on various IMU parts. As shown in Figure 8, our detection system works best for an anomaly affecting the accelerometer, but it also works well for an anomaly affecting more than one IMU component. Additionally, they assess abnormalities that range in time from 1 to 2 seconds to 4 to 5 seconds. Figure 9 shows that our detection system successfully detects anomalies of varying durations and maintains consistent performance with an SSC between 0.841 and 0.881.

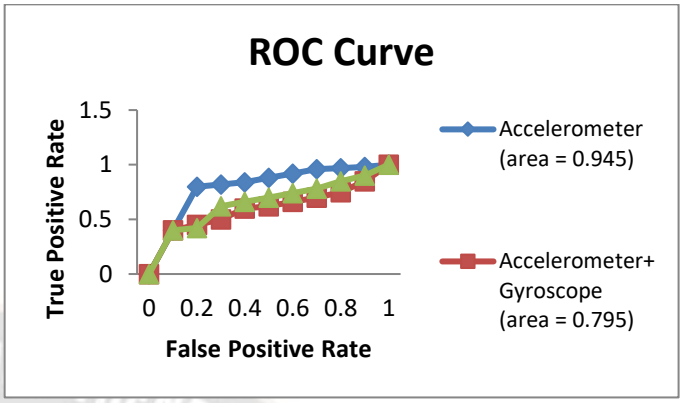

Figure 8: Assessment Results for Various Anomalies

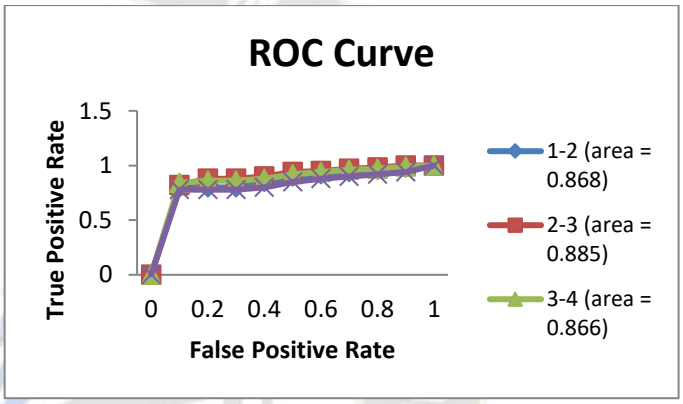

Figure 9: Assessment findings for anomalies of various durations

Table 2 shows that, in terms of efficiency and measure F, the proposed IRCNN-AL model performs better than the approaches considered. The precision results while using IRCNN-AL are above 80% for every unidentified network attack, with a 9% & 30% improvement to CNN LSTM, CNN, and EDFFNN. A presented IRCNN-AL framework to the open-set categorization algorithm could identify the undefined threats by using the high-value concept to recalibrate the parameters of the last completely connected layer and determine the likelihood that an example of the network threats.

This shows the superiority of the IRCNN-AL model suggested in the identification of unknown threats. Furthermore, it is important to note that the plans compared, including CNN LSTM, CNN, and EDFFNN, are nearest-package categorization models based on their criteria. As a result, their softmax classifier incorrectly categorizes any instances of an unknown threat that emerge during the testing phase as a known class, which techniques that should be contrasted are less effective than the recommended IRCNN-AL .

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
Article Received: *14 July 2023* ***Revised:*** *08 September 2023* ***Accepted:*** *20 September 2023*

Table 2 Comparison of the proposed IRCNN-AL model with existing system

Unknown c	*Accuracy (%)*				*F − measure*			
	EDFFN	*CNN*	*CNN_LS*	*IRCN − AL*	*EDFFN*	*CNN*	*CNN_LS*	*IRCN − AL*
Dos Hulk	59.35	65.5	66.92	85.66	0.5584	0.621	0.5925	0.842
Botnet	59.62	68.1	70.12	81.85	0.5627	0.603	0.6514	0.776
Ddos	56.38	62.6	64.98	87.18	0.5625	0.575	0.5828	0.845
Web Attac	61.21	69.6	71.566.9	81.22	0.5641	0.623	0.6442	0.772
TrickBot	59.22	65.5	66.99	85.33	0.5521	0.594	0.6028	0.826
Simda	58.87	65.5	67.33	86.13	0.5547	0.571	0.6354	0.833
Artemis	59.44	65.8	66.99	86.15	0.5562	0.630	0.6551	0.835
HTBot	59.33	65.5	64.05	86.82	0.5201	0.595	0.5945	0.815
Ursnif	56.62	62.7		82.89	0.5421	0.625	0.6571	0.845

Researchers randomly chose varying amounts of HTBot examples and include them in the test data in the operation to evaluate the effects of the added unknown assault examples on the capability of the IRCNN-AL method. Figure 10 shows that suggested IRCNN-AL test accuracy decreases with the number of unknown aggression samples provided. It's important to note that while IRCNN-AL can identify the majority of unknown assault examples, its performance was reduced and its benefit is less clear when the proportion of network threats in the test data is lower. In addition, they evaluate Open-Performance NCCs where fewer known threat samples were provided during the training phase. To create the IRCNN-AL template for the survey, consumers randomly chose 1% of Trickster examples & combine them with the learning algorithm.

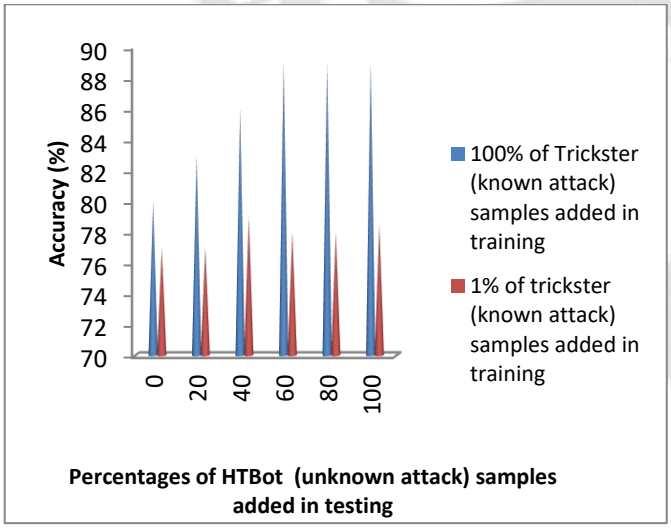

Figure 10: Effects of various additional unidentified aggression samples.

IX. IMPACT OF DIFFERENT CALIBRATION PARAMETERS

Given that the proposed unknown assault detection approach has two calibration parameters— tail size & alpha rank—they examine the effects of the variables by comparing the categorization performance of IRCNN-AL methods to various scores of tail size and alpha. Figure 11 depicts the outcomes of the research. The amount of the most popular choices that algorithm 1 needs to update is displayed. Figure 11 shows that is more accurate when α = 6 compared to when α = 2, but when was increased to 10, the accuracy drops and becomes less accurate than when α = 6. It should be noticed that when the alpha value rises, the open-set classification's accuracy steadily improves before declining. Therefore, the probability of open categorization was not affected by the tiny activation values of the lower classes. In investigations, the alpha value is set at 6. Additionally, they calculate the distance between each successfully categorized traffic sample and the associated MAV using the cosine and euclidean distance, respectively. Figure 12 shows that the suggested IRCNN-AL method works better than the conventional CNN method for various kinds of undefined network assault. The researcher was recommended to use cosine separation to Euclidean distance while analyzing the nine different types of unknown network attacks.

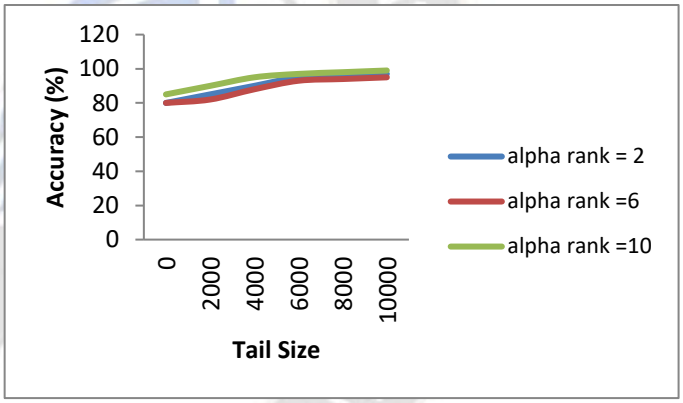

Figure 11 IRCNN performances in open classification across various rank categories

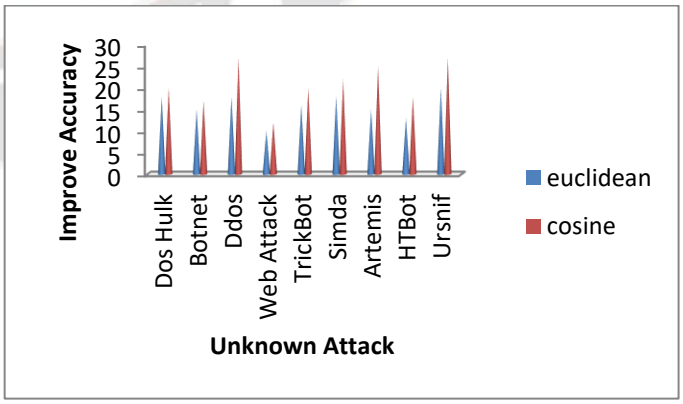

Figure 12: Increased categorization accuracy.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8338
***Article Received:** 14 July 2023 **Revised:** 08 September 2023 **Accepted:** 20 September 2023*

CONCLUSION

In this research, they proposed a system to detect UAV anomalies based on data analysis of IMU sensors. The authors examine and evaluate various DNN methods and detection time frames in our architecture in an attempt to maintain the accuracy and performance of the detection method. A data set of UAV IMU information is collected and designated as a calculation leveraging UAV cybersecurity architecture to facilitate the development of the IRCNN-AL method in our proposal and relevant studies in the ecosystem. The IRCNN-AL model was proposed to enable open reconnaissance for ID and identification of unknown threats. Researchers also suggest an AL strategy based on the least trust query method to unidentified assaults, which enables the ID system to effectively train to discover new network assaults with limited labeling resources. The results show that suggested IRCNN-AL was effective and viable in identifying unknown network threats. The AL method also significantly enhances the performance of the ID method and outperforms an alternative strategy. In the decentralized drone communication system of the future, they intend to focus on IDS more effectively. Further research will examine the question of improving the accuracy of network attacks.

ACKNOWLEDGMENT

We thank the higher officials and faculty members of SRMIST for their wide support towards our research work.

REFERENCES

[1] Wang, Y., Li, S., Teng, F., Lin, Y., Wang, M., & Cai, H. (2022). Improved mask R-CNN for rural building roof type recognition from UAV high-resolution images: a case study in hunan province, China. Remote Sensing, 14(2), 265.

[2] Zhang, Z., Zhang, Y., Niu, J., & Guo, D. (2021). Unknown network attack detection based on open-set recognition and active learning in drone network. Transactions on Emerging Telecommunications Technologies, e4212.

[3] Maranhão, J. P. A. (2021). Tensor based machine learning frameworks for intrusion detection in the physical and network layers of cyber-physical systems.

[4] Rajasekar, R., & Sivakumar, P. (2020). Swarm Based Intelligent Transportation Systems Using Internet of Things in Vehicular Ad-HOC Network. Journal of Computational and Theoretical Nanoscience, 17(12), 5503-5508.

[5] Abdullayeva, F. J., & Valikhanli, O. V. (2022). Development of a method for detecting GPS spoofing attacks on unmanned aerial vehicles. Problems of Information Technology, 3-8.

[6] Yarlagaddaa, J., & Malkapuram, R. (2020). Influence of MWCNTs on the Mechanical Properties of Continuous Carbon Epoxy Composites. Revue des Composites et des Matériaux Avancés, 30(1).

[7] Xiao, Y., Xing, C., Zhang, T., & Zhao, Z. (2019). An intrusion detection model based on feature reduction and convolutional neural networks. IEEE Access, 7, 42210-42219.

[8] Zhang, X., Chandramouli, K., Gabrijelcic, D., Zahariadis, T., & Giunta, G. (2020, July). Physical security detectors for critical infrastructures against new-age threat of drones and human intrusion. In 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW) (pp. 1-4). IEEE.

[9] Alferaidi, A., Yadav, K., Alharbi, Y., Razmjooy, N., Viriyasitavat, W., Gulati, K., ... & Dhiman, G. (2022). Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles. Mathematical Problems in Engineering, 2022.

[10] Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering, 7(4), 2219-2230.

[11] Zhang, R., Condomines, J. P., & Lochin, E. (2022). A Multifractal Analysis and Machine Learning Based Intrusion Detection System with an Application in a UAS/RADAR System. Drones, 6(1), 21.

[12] Abu Al-Haija, Q., & Al Badawi, A. (2022). High-performance intrusion detection system for networked Vs via deep learning. Neural Computing and Applications, 1-16.

[13] Yarlagaddaa, J., & Ramakrishna, M. (2019). Fabrication and characterization of S glass hybrid composites for Tie rods of aircraft. Materials Today: Proceedings, 19, 2622-2626.

[14] Gao, F., Ji, S., Guo, J., Li, Q., Ji, Y., Liu, Y., ... & Yang, B. (2021). ID-Net: an improved mask R-CNN model for intrusion detection under power grid surveillance. Neural Computing and Applications, 33(15), 9241-9257.

[15] Sharma, M., & Kumar, C. R. S. (2022). Machine learning-based smart surveillance and intrusion detection system for national geographic borders. In Artificial Intelligence and Technologies (pp. 165-176). Springer, Singapore.

[16] Shrestha, R., Omidkar, A., Roudi, S. A., Abbas, R., & Kim, S. (2021). Machine-learning-enabled intrusion detection system for cellular connected UAV networks. Electronics, 10(13), 1549.

[17] Garikapati, P. R., Balamurugan, K., Latchoumi, T. P., & Shankar, G. (2022). A Quantitative Study of Small Dataset Machining by Agglomerative Hierarchical Cluster and K-Medoid. In Emergent Converging Technologies and Biomedical Systems (pp. 717-727). Springer, Singapore. https://doi.org/10.1007/978-981-16-8774-7_59

[18] Guan, L., Li, X., Yang, H., & Jia, L. (2020, August). A visual saliency based railway intrusion detection method by UAV remote sensing image. In 2020 International Conference on Sensing, Diagnostics, Prognostics, and Control (SDPC) (pp. 291-295). IEEE.

[19] Sridharan, K., & Sivakumar, P. (2018). A systematic review on techniques of feature selection and classification for text mining. International Journal of Business Information Systems, 28(4), 504-518

[20] Niu, R., Qu, Y., & Wang, Z. (2021, September). UAV Detection Based on Improved YOLOv4 Object Detection Model. In 2021 2nd International Conference on Big Data & Artificial

Intelligence & Software Engineering (ICBASE) (pp. 25-29). IEEE.

[21] Galvan, J., Raja, A., Li, Y., & Yuan, J. (2021, November). Sensor Data-Driven UAV Anomaly Detection using Deep Learning Approach. In MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM) (pp. 589-594). IEEE.

[22] Mehouachi, F. B., Yang, Q., Galvis, J., Morales, S., Meriac, M., Vega, F., & Kasmi, C. (2021). Detection of UAVs Based on Spectrum Monitoring and Deep Learning in Negative SNR Conditions. URSI Radio Science Letters, 3, 43.

[23] Al-Ansi, A. M. . (2021). Applying Information Technology-Based Knowledge Management (KM) Simulation in the Airline Industry . International Journal of New Practices in Management and Engineering, 10(02), 05–09. https://doi.org/10.17762/ijnpme.v10i02.131

[24] Fraser, B., Al-Rubaye, S., Aslam, S., & Tsourdos, A. (2021, October). Enhancing the security of unmanned aerial systems using digital-twin technology and intrusion detection. In 2021 IEEE/AIAA 40th Digital Avionics Systems Conference (DASC) (pp. 1-10). IEEE.

[25] Huang, H., Liang, L., Zhao, G., Yang, Y., & Ou, K. (2019, June). Railway clearance intrusion detection in aerial video based on convolutional neural network. In 2019 Chinese Control And Decision Conference (CCDC) (pp. 1644-1648). IEEE.

[26] Boukhdir, K., Marzouk, F., Medromi, H., & Benhadou, S. (2015). Secured UAV based on multi-agent systems and embedded intrusion detection and prevention systems. Am. J. Eng. Res.(AJER), 4(8), 186-190.

[27] Alkahtani, H., & Aldhyani, T. H. (2021). Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms. Complexity, 2021.

[28] Yang, B., Cao, X., Yuen, C., & Qian, L. (2020). Offloading optimization in edge computing for deep-learning-enabled target tracking by internet of UAVs. IEEE Internet of Things Journal, 8(12), 9878-9893.

[29] Xu, C., Chen, B., Liu, Y., He, F., & Song, H. (2020, September). RF fingerprint measurement for detecting multiple amateur drones based on STFT and feature reduction. In 2020 Integrated Communications Navigation and Surveillance Conference (ICNS) (pp. 4G1-1). IEEE.

[30] Latchoumi, T. P., Kothandaraman, R., & Balamurugan, K.. (2022). Implementation of Visual Clustering Strategy in Self-Organizing Map for Wear Studies Samples Printed Using FDM. Traitement du Signal, 39(2). DOI: 10.18280/ts.390215

[31] Vanitha, N., & Ganapathi, P. (2020). Traffic analysis of UAV networks using enhanced deep feed forward neural networks (EDFFNN). In Handbook of Research on Machine and Deep Learning Applications for Cyber Security (pp. 219-244). IGI Global.

[32] G.Balamurugan,Dr.J.Jayabharathy, "A Comparative Analysis of Event Detection and Video Summarization". In: Hu, YC., Tiwari, S., Trivedi, M.C., Mishra, K.K. (eds) Ambient Communications and Computer Systems. Lecture Notes in Networks and Systems, vol 356. Springer, Singapore. https://doi.org/10.1007/978-981-16-7952-0_54.

[33] Pérez-Cutino, M. A., Eguíluz, A. G., Martínez-de Dios, J. R., & Ollero, A. (2021, June). Event-based human intrusion detection in UAS using Deep Learning. In 2021 International Conference on Unmanned Aircraft Systems (ICUAS) (pp. 91-100). IEEE.

[34] G.Balamurugan, J. Jayabharathy, "An integrated framework for abnormal event detection and video summarization using deep learning". International Journal of Advanced Technology and Engineering Exploration. 2022; 9(95):1494-1507. DOI:10.19101/IJATEE.2021.875854.

[35] G. Balamurugan, J. Jayabharathy, "Abnormal Event Detection using Additive Summarization Model for Intelligent Transportation Systems" International Journal of Advanced Computer Science and Applications(IJACSA), 13(5), 2022. http://dx.doi.org/10.14569/IJACSA.2022.0130586

[36] G.Balamurugan, J. Jayabharathy, An Efficient CNN and BI-LSTM Model for Abnormal Event Detection in Video Surveillance (May 22, 2021). Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021), Available at SSRN: https://ssrn.com/abstract=3851212 or http://dx.doi.org/10.2139/ssrn.3851212

[37] G. Balamurugan and V. Premanand, "A novel framework for extraction of landscape areas and automatic building detection in satellite images," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2017, pp. 1-4, doi: 10.1109/ICACCS.2017.8014575.

[38] G. Balamurugan and K. Kishore Anthuvan Sahayaraj, "A Blockchain Based Certificate Authentication System," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICCCI56745.2023.10128289.

[39] Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.