2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC) | 979-8-3503-0009-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICESC57686.2023.10193232

An Artificial Intelligence Network based-Host Intrusion Detection System for Internet of Things Devices

1. Mr Ashish Jain, Assistant Professor,
Department of Computer Applications,
BSSS College, Bhopal, Madhya
Pradesh, India.
ashish.jain14@yahoo.com

4. Aniruddh Kumar, Lecturer,
Electronics, Government Polytechnic,
Aurai, Bhadohi, Uttar Pradesh, India.
aniruddhknmiet@gmail.com

2. Dr B. Srinivasa Rao, Professor,
Department of Computer Science and
Engineering, Gokaraju Rangaraju
Institute of Engineering and
Technology, Bachupally, Hyderabad,
Telangana, India.
bsrgriet2015@gmail.com

5. Dr M. S. Muthuraman, Professor,
Department of Mathematics, PSNA
College of Engineering and
Technology, Dindigul, Tamilnadu,
India. msmraman@psnacet.edu.in

3. Saumitra Chattopadhyay, Assistant
Professor, Department of Computer
Science and Engineering, Graphic Era
Hill University, Dehradun, India,
schattopadhyay@gehu.ac.in

6. Dr A. Manjula, Associate Professor,
Jyothishmathi Institute of Technology
and Science, Karimnagar, India,
manjula3030@gmail.com

***Abstract*— Internet of Things (IoT) is currently employed in almost all the areas, including applications in smart cities, smart homes, e-Wellbeing, and others. Due to its wider utilization, IoT security has become a serious concern. A secure Intrusion Detection System (IDS) for the Internet of Things is often built using artificial intelligence (AI) and its subsets, deep learning (DL), and machine learning (ML). Industrial IoT devices, which are readily available, are regularly used by researchers and industry experts. This research study investigates the possibility of deploying a DL-Based Host-IDS (DL-HIDS) on specific commercial IoT devices. In this study, an optimized Convolutional Neural Network (O-CNN) based on DL is used. The proposed model's efficiency is evaluated by utilizing performance metrics like recall, precision, accuracy, and f1score. The proposed model's effectiveness is verified by analyzing the promising results obtained from the implementation of the proposed DL-HIDS on various existing models.**

Keywords*— Deep Learning, Internet of Things, Intrusion Detection System, Artificial Intelligence, Convolutional Neural Network.

I. INTRODUCTION

Applications in Smart Cities, smart homes, as well as e-Health are just a few examples of where the IoT can be found. Security of the IoT is a real concern due to its widespread utilization. When creating a safe IoT Intrusion Detection System (IDS), methods based on AI along with its subsets ML as well as DL are frequently utilized [1]. In contrast to network-based IDSs, which are solely intended to monitor network traffic, host-based IDSs are made to keep an eye on both PCs and the network. These networks are the two common IDS implementations. The four types of IDPS technologies covered in this article are network-based, Network Behaviour Analysis (NBA), wireless, and host-based. Security is of incredible concern these days as a huge measure of information is being sent consistently in each space. A survey on the use of a neural network to protect data in the prevention and detection of intrusions is provided here [2].

Using the generative adversarial network (GAN), a unsupervised AD Host-IDS is given for the IoT. This architecture is based on adversarial training. Due to their limited functionality, this IDS, dubbed "EdgeIDS," primarily targets IoT devices; in contrast to traditional devices like computers or servers, which exchange data, IoT devices only send along with receive specific data [3]. Due to their limited processing power and energy, IDSs typically require an excessive amount of resources to manage. For IoMT device-generated attacks, ML and DL approaches are the best detection and control methods [4].

Applications related to cyber security have made use of DL algorithms. Numerous areas, Android-based malware, IDS, including PC-based malware, cyber intelligence, phishing attacks, along with spam detection, have been the subject of DL application studies in the literature [5]. The various AI-based detection and/or prevention systems used in IoTs are the subject of this investigation, and to focus on their significance. In particular, ML and DL methods are checked for prevention systems as well as intrusion detection ,focusing on their difficulties, viability, compatibility, along with real-time issues. The ML or DL methods can help industry as well as academia classify the challenges along with issues in existing security models as well as generate new dimensions of security framework development [6].

In addition, the IoT cannot function without confidentiality, integrity, and availability. An adaptive prevention system as well as intrusion detection and prevention system for the IoT (IDPIoT) keep up with the growing number of connected devices and improve security. By examining the existing IDS, the IDPIoT improves network-based functionality, security, along with including host-based. The IDP IoT examines the behavior after receiving the packet, suspects the packet, and either blocks or drops it [7].

The rest of this work organization is stated. section 2 presents related work on IoT devices using various ML and DL algorithms. Section 3 discusses the proposed AI based technique. Section 4 presents the results achieved and dataset used for simulation, as well as finally, section 5 concludes the work followed by the references.

II. Background Work

Table 1 lists and discusses a few of the currently used methods, along with their benefits and drawbacks.

TABLE I. Comparison Study of Some Existing Approaches

Paper	Methodology	Advantages	Disadvantages
Atefinia, Ramin, and Mahmood Ahmadi [8]	ML technique	Computer Security	No Efficient Feature Extraction
Kaushik et al.[9]	A Hybrid Feature-Selection Method	Protect From Attacks	_
Baniasadi et al. [10]	Neighborhood Search-Based Particle Swarm Optimization (NSBPSO) Algorithm	Security	_
Azzaoui, Hanane [11]	The detection method and the deployment strategy	Defend Against Network Attacks	No Optimization is done
Albulayhi et al. [12]	Feature selection and extraction approach	Protect various attacks	Does not check more parametes
Tabassum et al.[13]	A framework with robust access control, robust authentication, lightweight cryptography along with IDS	Secure the data and communication between devices	Not better performane

Atefinia, Ramin, and Mahmood Ahmadi [8] gave a model for a modular deep neural network with multiple architectural elements to lower the rate of false positives in anomaly-based intrusion detection systems. This model is of a stack of controlled Boltzmann machine modules, a feedforward module, along with two recurrent modules make up our model. The model's answer is generated by feeding the output weights to an aggregator module.

Kaushik et al. [9] described an IoT ecosystem which is made vulnerable to cyberattacks. This work is challenging to implement accurate IDSs in IoT devices owing to these limitations. This paper presents a feature selection algorithm and a new lightweight IDS to address the issues of accuracy and cost of computation. The Information Theory models serve as the foundation for the proposed algorithm, which selects the dataset feature with the highest statistical dependence and the lowest entropy.

Baniasadi et al. [10] to implement accurate IDSs in IoT devices foster an original preparation calculation to more readily tune the boundaries of the utilized profound design. In order to accomplish this, this work present a NSBPSO algorithm to enhance the PSO algorithm's exploitation and exploration. Then, we utilize the upside of NSBPSO to ideally prepare the profound design as our organization interruption finder to get better precision and execution.

Azzaoui, Hanane [11] looks into and suggests new IDS strategies for IoT-based networks, as well as a better way to deploy the proposed IDS by making use of an existing routing protocol like RPL (Routing Protocol for Low-Power as well as Lossy Networks). The temporal and spatial complexity of the proposed methods is superior, as shown by our experiments. High detection rates in real-world scenarios are revealed by these findings, which mark a significant advancement in IDS for the IoT.

Albulayhi et al. [12] gave a method for anomaly-based IDS features selection and extraction in this paper. The method commences by choosing as well as extracting relevant features in numerous ratios using two entropy-grounded approaches, information gain (IG) along with gain ratio (GR). The best features are then extracted using union and intersection mathematical set theory. Using four ML algorithms, the training and testing of the model framework is done. This was done on two datasets such as the NSL-KDD dataset: Sacking, Multi-facet Discernment, J48, and IBk as well as the IoT intrusion dataset 2020 (IoTID20).

Tabassum et al. [13] Zero-day attacks are constantly emerging, so conventional IDS strategies are ineffective. A possible solution seems to be intelligent mechanisms that can identify unfamiliar intrusions. This article investigates well known assaults against IoT engineering and its important safeguard instruments to recognize a proper defensive measure for various systems administration rehearses and assault classes. Also, several security enhancement systems and a IoT architecture security framework for list are also given.

In existing several approaches has been proposed including ML, ML along with feature selection, some optimization approaches like NSBPSO along with some lightweight cryptography methods. These methods have some advantages like computer security, protection from attacks, defend the attacks and secure communication between devices. Although it has some disadvantages like inefficiency with feature extraction methods, does not check and optimize the parameters and less performance. Hence to rectify these limitations this work proposes an efficient DL based optimized CNN (O-CNN) algorithm. Since the prediction issues will be solved by deep learning algorithms efficiently. The contributions of the proposed O-CNN are summarized below:

- The proposed approach, utilizes the first design and train it as needs be to the IoT-IDS dataset. This implies that the model can be retrained without any preparation.
- To avoid over fitting, this method trains the CNN layers and optimizes some hyperparameters.

- Along with this the weight of the CNN model is optimized to build an efficient model.
- The BoT-IoT dataset is a cyber security dataset is used in this work.

III. Research Methodology

The purpose of the work is to categorize the intrusions. For this the BoT-IoT dataset [15] is used where initially preprocessing is done. This BoT-IoT dataset is generated in the year 2018. Pre-processing thus converts the raw dataset and normalize its values. To redescribe an image's characteristics, the image normalisation process is used. Along with pre-processing feature selection is also done by which only the specific needed features are selected. The feature selection is done with aid of chi-square test. Then the recognition is done with the proposed O-CNN model. The proposed O-CNN model stacks 15 layers from scratch. Moreover, in this model the weights hyperparameter is optimized to provide better accuracy and less loss. After evaluation the efficiency of the proposed model is checked by using some performance metrics parameters such as the accuracy, loss, precision, recall and f1score. This performance measure is compared with some existing approaches. The proposed model flow is illustrated in fig 1.

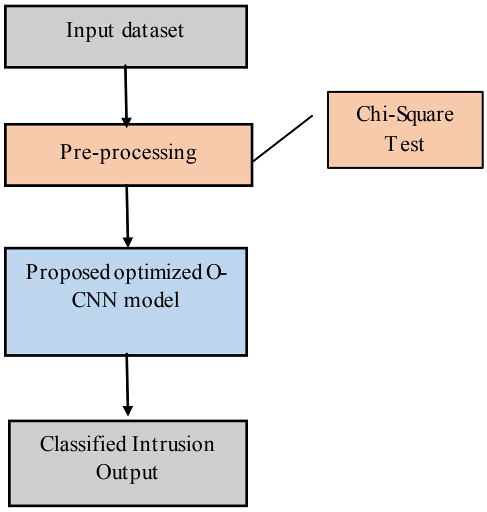

Fig. 1. Proposed Flow

A. Pre-Processing

Encoding the dataset's raw data and normalizing its values must be done as the initial step. This means changing the normalized output data into the shape of image data along with extending the vectors individually into unit form. After that, the data is randomly divided into 60 % for training subset, 20 % for testing subset as well as another 20% for validation subset. After that, in a pre-optimization context, a feature collection is made to reduce the count of features, even though DL does not require this process; however, in order to produce a lightweight model, the number of features is reduced from 16 to just 7. The statistical test, a chi-square test, for determining the features relationship, is employed to choose the finest features for the model. A Chi-Square estimate determines whether a feature is independent of the class label. According to the formulas (1) and (2), the chi-square score with the "c" class along with "v" values [14]:

$$C^2 = -\sum_{(i=1)}^{v}\sum_{(j=1)}^{c}\frac{\left(n_{ij}-\mu_{ij}\right)}{\mu_{ij}} \tag{1}$$

Where $\mu_{ij} = \frac{(n_{*j}\, n_{i*})}{n}$ (2)

By the i th feature value, here n_{ij} is the value for the count of samples; n_{i*} is the quantity of tests with the i th include esteem; n_{*j} is the count of models in class j, and n is the sample count.

B. Proposed Optimized CNN Model

The O-CNN model that has been proposed has multiple layers and is trained in 32 batches over 10 epochs. An input layer, a Convolution1D layer, a MaxPooling1D layer, a Flatten layer, a Convolution1D layer, a ReLU layer, a MaxPooling1D layer, a dropout layer, a Dense layer, along with an output layer were the components of the IDS O-CNN model. The neural network has four intermediate (hidden) layers, 16 input neurons, 16 Convolution1D neurons, 8 MaxPooling1D neurons, 256 Flatten neurons, 44 Dense neurons, 4 output neurons, as well as 256 ReLU neurons for the multiclass classification.

The convolutional layer is considered as a fundamental component in CNN. Most of the computation burden of the network is done by it. A dot product is done by the convolutional layer between two matrices. One matrix is the receptive field's restricted portion. Then the other matrix is the set of learnable parameters, or kernel. While the kernel is deeper than an image, it occupies a smaller spatial area. This specifies that while the kernel width as well as height will be spatially small for an image with three (RGB) channels, the depth will encompass every three channels. The image depiction of that receptive region is formed as the kernel. It moves across the width as well as height of the image throughout the forward pass. An activation map is a two-dimensional depiction of the image. This activation map displays the kernel's reply at all spatial position, is the consequence of this. The kernel's decreasing size is considered as a stride. Convolution use three significant thoughts that propelled the researchers are parameter sharing, sparse interaction, and equivariant representation.

By deriving a measurement of the nearby outputs, the pooling layer substitutes the network output at exact locations. The representation's spatial size is reduced as a result, the computation and weighting required is reduced. The representation of each slice is preserved independently during the pooling operation. The L2 norm of the rectangular neighborhood, the average of the rectangular neighborhood, and a weighted average rooted on the distance from the central pixel are among the pooling functions. However, max pooling process is the most utilized process. This process reports the maximum output from the neighborhood. As can be seen in a typical O-CNN, neurons in the fully connected layer are fully connected to every neuron that come before and after it in the layers. Because of this, it can be calculated as usual by means of a bias effect and a matrix multiplication. The representation is mapped between the input and output with the assistance of the FC layer.

Recently, there the Rectified Linear Unit (ReLU) is considered more popular than the other activation functions. The function f(h)=max (0, h) is derived from ReLU. To put it extra way, the activation is merely threshold zero. ReLU is more reliable and accelerates convergence six times faster than sigmoid and tanh. The fact that ReLU can be fragile during training is unfortunately a disadvantage. It can be efficient by a significant gradient so that the neuron will never be updated again. Nevertheless, it can be dealt by establishing an appropriate learning rate.

The proposed model is trained and tested on the Bot-IoT dataset. In like manner, a misfortune capability including a softmax and Relu is remembered for the last thick layer. With these preoptimizations; like diminishing the quantity of elements the quantity of model's boundaries is decreased. By utilizing this the proposed O-CNN model is prepared and the interruption is recognized. The proficiency of the proposed work is finished by examination with existing methodologies.

IV. Results and Discussions

Keras is used for the experimental evaluation (2.4.0) which is an Python DL library that makes use of Tensor Flow-GPU (2.3.0) as a backend engine and runs on Google's open-source data flow software top.

A. Dataset

The BoT-IoT dataset is a cyber security dataset is used in this work. shaped by a real network milieu specifically for IoT systems. There are four types of attacks and ten subcategories in the environment, which includes both typical normal traffic and bad traffic. DoS (UDP, TCP, as well as HTTP), theft (key logging along with data exfiltration), along with DDoS (TCP, UDP, and HTTP) are examples of reconnaissance.

B. Discussions

For a variety of road anomalies, the proposed ICNN-VGG model is contrasted with previous methods. The confusion matrix is used in performance analysis. The positive class that was found to be positive and the true positive rate are both represented by the term "true positive" (TP). False positive (FP) is the pace of a negative class not entirely settled to be positive; The rate of a positive class that was found to be negative is called false negative (FN); The rate of a true negative class that was found to be negative is known as true negative (TN). The proposed O-CNN model's performance is evaluated using the F1-score, precision, recall, and accuracy metrics. Precision, also known as a positive predicted value, can be estimated by the equation (3):

$$Precision = \frac{TP}{FP+TP} \tag{3}$$

The count of positive class predictions done from all of the positive examples in the dataset is counted by the recall. The mathematical appearance for the recall can be seen in the equation (4) below.

$$Recall = \frac{TP}{TP+FN} \tag{4}$$

The term "accuracy" refers to the total count of correct expectations in a chaotic network for a specific class and can be measured using the accompanying condition(5).

$$accuracy = \frac{TP+TN}{FP+FN+TP+TN} \tag{5}$$

The F1-score offers a single score that associates precision along with recall in a single number. The equation (6) that follows shows the mathematical formula for the F1-score:

$$F1-score = 2 * \frac{Precision*Recall}{Precision+Recall} \tag{5}$$

The differentiation between the actual value along with the value that was predicted is called the Loss (*Ls*). Cross-entropy is the greatest frequently utilized loss function in the proposed O-CNN model, and the formula for its calculation is as follows:

$$Loss = -\sum_{c=1}^{N} y_{o,c} log(p_{o,c}) \tag{6}$$

Where y is the binary indicator (true indicates 1 or false indicates 0) indicating whether N the class label c is the appropriate classification for observation o . p is the anticipated likelihood perception of class. The experimental outcomes of the proposed O-CNN model are depicted. Fig 2 depicts the confusion matrix plot of the proposed O-CNN model obtained by display the confusion matrix plot.

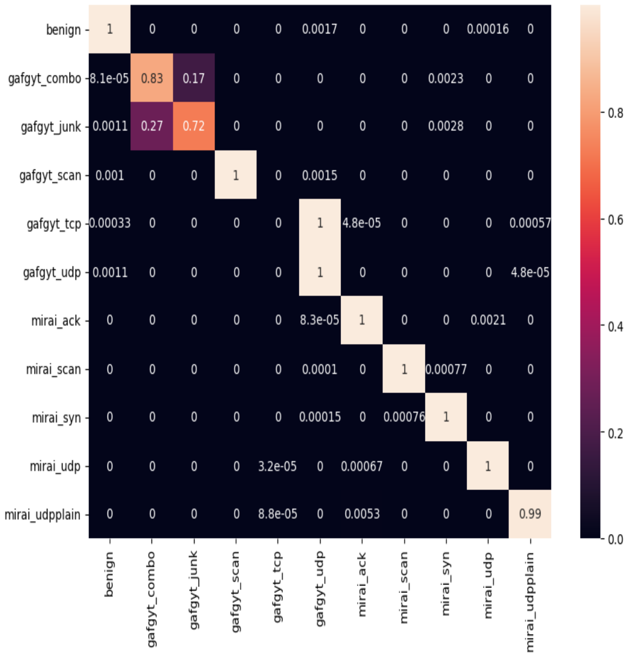

Fig. 2. Proposed O-CNN Model Confusion Matrix

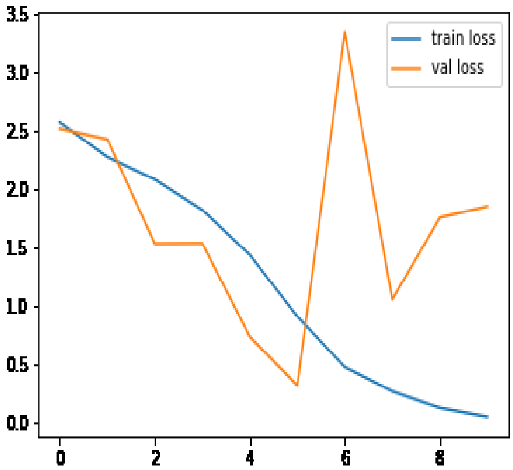

Fig. 3. Proposed O-CNN Loss Graph

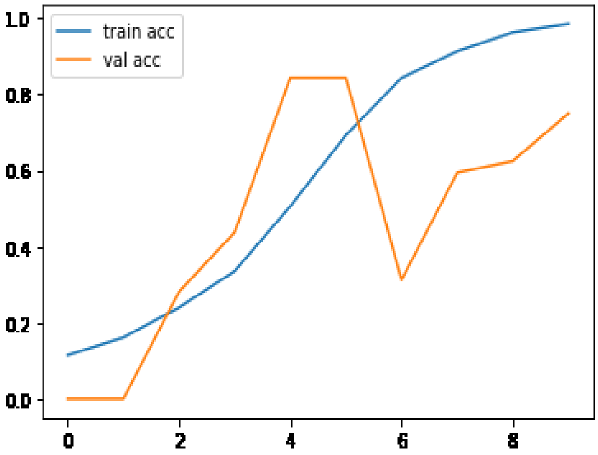

Fig. 4. Proposed O-CNN Accuracy Graph

Fig 3 depicts the train loss and validation loss of the proposed O-CNN model. From this figure it is clear that the loss decreases with increase in epochs. The loss of the proposed O-CNN model is as low as 0.23. This proves the good of the proposed model. Also, as the loss decreases automatically the accuracy increases. The accuracy of the proposed O-CNN model is 0.99. The increase in accuracy is depicted in fig 4.

TABLE II. PROPOSED O-CNN MODEL RESULTS

Classes	Precision	Recall	F1-score
0	1.00	0.99	1.00
1	0.94	0.96	0.97
2	0.89	0.92	0.90
3	1.00	1.00	1.00
4	0.80	0.76	0.77
5	0.89	0.99	0.98
6	1.00	1.00	1.00
7	0.99	1.00	1.00
8	1.00	1.00	1.00
9	1.00	1.00	1.00
10	1.00	1.00	0.99
accuracy			0.99

Table 2 narrates the precision, recall as well as f1-score value of the proposed O-CNN model. The eleven different classes in the dataset are benign, gafgyt junk, gafgyt scan, gafgyt combo, gafgyt udp, gafgyt tcp, mirai scan, mirai ack, mirai udp mirai syn, and mirai udpplain. Table 3 shows how the proposed O-CNN model compares to other models in the literature. From table 2 it is noticeable that the performance parameters of most classes is equal to 1.00, and 0.99.

TABLE III. PERFORMANCE COMPARISON

Methods	Accuracy	Loss	Precision	Recall	F1-score
Proposed	0.99	0.23	0.98	0.97	0.96
DL-IDS [14]	0.98	0.25	0.96	0.95	0.95
Feature selection and extraction [12]	0.97	0.27	0.96	0.94	0.95
NSBPSO-DCNN [10]	0.96	0.28	0.94	0.93	0.94
MI2G[9]	0.95	0.31	0.93	0.92	0.91

From table 3 it is obvious that the proposed O-CNN model is efficient when comparing to the existing approaches in the literature. The accuracy or detection rate of the proposed O-CNN model is 0.99. Thus, the proposed is 1.02% efficient than DL-IDS, 2.06% efficient than feature selection and extraction method, 3.12% efficient than NSBPSO-DCNN and 4.21% efficient than MI2G. The loss of the proposed O-CNN model is 0.23. Thus, the proposed is 8.69% efficient than DL-IDS, 17.39% efficient than feature selection and extraction method, 21.73% efficient than NSBPSO-DCNN and 34.78% efficient than MI2G. The precision of the proposed O-CNN model is 0.98. Thus, the proposed is 2.08% efficient than DL-IDS and feature selection and extraction method, 4.25% efficient than NSBPSO-DCNN and 5.37% efficient than MI2G.

The recall of the proposed O-CNN model is 0.97. Thus, the proposed is 1.05% efficient than DL-IDS, 2.12% efficient than feature selection and extraction method, 3.22% efficient than NSBPSO-DCNN and 4.34% efficient than MI2G. The f1 score of the proposed O-CNN model is 0.96. Thus, the proposed is 1.05% efficient than DL-IDS and feature selection and extraction method, 2.12% efficient than NSBPSO-DCNN and 5.49% efficient than MI2G. From the training results obtained testing is done. By testing the intrusion is networks is also detected. From these results it is clear that the proposed O-CNN model is efficient.

V. CONCLUSION AND FUTURE WORK

Traditional IDS are being severely hampered by the enormous amounts of network traffic data generated by IoT devices distributed worldwide. Due to its outstanding work in diverse fields and its own shortcomings, such as data dependence or a lack of labeled data, researchers frequently construct IDS using DL. The Bot-IoT dataset served as the initial foundation for the proposed IDS O-CNN for IoT. After a few tests, a sensible recognition rate is obtained on this proposed O-CNN IDS. This work comes to the conclusion that the proposed O-CNN model can be an ideal solution for both compensating for the absence of data in some attack classes and updating the IDS systems with minimal computing power as well as effort by analyzing the obtained results. This work will deploy the IDS in a real IoT environment along with on a lightweight IoT device, optimize it without sacrificing accuracy, and examine the real IoT network traffic data performance in future research works.

REFERENCES

[1] Idrissi, Idriss, Mostafa Mostafa Azizi, and Omar Moussaoui, "A lightweight optimized deep learning-based host-intrusion detection system deployed on the edge for IoT," International Journal of Computing and Digital System, 2021. Doi: 10.12785/ijcds/110117.

[2] Bhatia, Vaishali, Shabnam Choudhary, and K. R. Ramkumar, "A comparative study on various intrusion detection techniques using machine learning and neural network," In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), IEEE , 2020, pp. 232-236. Doi: 10.1109/ICRITO48877.2020.9198008.

[3] Idrissi, Idriss, Mostafa Azizi, and Omar Moussaoui, "An unsupervised generative adversarial network based-host intrusion detection system for internet of things devices," Indones. J. Electr. Eng. Comput. Sci, vol. 25, no. 2, pp. 1140-1150, 2022. Doi: 10.11591/ijeecs.v25.i2.pp1140-1150.

[4] Rbah, Yahya, Mohammed Mahfoudi, Younes Balboul, Mohammed Fattah, Said Mazer, Moulhime Elbekkali, and Benaissa Bernoussi, "Machine learning and deep learning methods for intrusion detection systems in iomt: A survey," In 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), IEEE, 2022, pp. 1-9. Doi: 10.1109/IRASET52964.2022.9738218.

[5] Uğurlu, Mesut, and İbrahim Alper Doğru, "A survey on deep learning based intrusion detection system," In 2019 4th International Conference on Computer Science and Engineering (UBMK), IEEE, 2019, pp. 223-228. Doi: 10.1109/UBMK.2019.8907206.

[6] Jayalaxmi, Pls, Rahul Saha, Gulshan Kumar, Mauro Conti, and Tai-Hoon Kim, "Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey," IEEE Access, 2022. Doi: 10.1109/ACCESS.2022.3220622.

[7] Bakhsh, Sheikh Tahir, Saleh Alghamdi, Rayan A. Alsemmeari, and Syed Raheel Hassan, "An adaptive intrusion detection and prevention system for Internet of Things," International Journal of Distributed Sensor Networks, vol. 15, no. 11, pp. 1550147719888109, 2019. Doi: 10.1177/1550147719888109.

[8] Atefinia, Ramin, and Mahmood Ahmadi, "Network intrusion detection using multi-architectural modular deep neural network," The Journal of Supercomputing, vol. 77, pp. 3571-3593, 2021. Doi: 10.1007/s11227-020-03410-y.

[9] Kaushik, Sunil, Akashdeep Bhardwaj, Abdullah Alomari, Salil Bharany, Amjad Alsirhani, and Mohammed Mujib Alshahrani, "Efficient, Lightweight Cyber Intrusion Detection System for IoT Ecosystems Using MI2G Algorithm," Computers, vol. 11, no. 10, pp. 142, 2022. Doi: 10.3390/computers11100142.

[10] Baniasadi, Sahba, Omid Rostami, Diego Martín, and Mehrdad Kaveh, "A novel deep supervised learning-based approach for intrusion detection in IoT systems," Sensors, vol. 22, no. 12, pp. 4459, 2022. Doi: 10.3390/s22124459.

[11] Azzaoui, Hanane, "Application of Intrusion Detection Systems in Internet of Things by surpassing IoT related restrictions," PhD diss., University Kasdi Merbah Ouargla, 2022.

[12] Albulayhi, Khalid, Qasem Abu Al-Haija, Suliman A. Alsuhibany, Ananth A. Jillepalli, Mohammad Ashrafuzzaman, and Frederick T. Sheldon, "IoT intrusion detection using machine learning with a novel high performing feature selection method," Applied Sciences, vol. 12, no. 10, pp. 5015, 2022. Doi: 10.3390/app12105015.

[13] Tabassum, Aliya, and Wadha Lebda, "Security framework for iot devices against cyber-attacks," arXiv preprint arXiv, pp. 1912.01712, 2019. Doi: 10.48550/arXiv.1912.01712.

[14] Idrissi, I., Azizi, M., & Moussaoui, O, “Accelerating the update of a DL-based IDS for IoT using deep transfer learning,” Indones. J. Electr. Eng. Comput. Sci, vol. 23, no. 2, pp. 1059-1067, 2021. Doi: 10.11591/ijeecs.v23.i2.

[15] Koroniotis, Nickolaos, Nour Moustafa, Elena Sitnikova, and Benjamin Turnbull. "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset." Future Generation Computer Systems 100 (2019): 779-796. Doi: 10.1016/j.future.2019.05.041.