NETWORK TRAFFIC CLASSIFICATION METHODS: A SURVEY

[1]Abhishek Kumar Dubey, [2]VK Singh, [3]Sadaf Hussaini, [4]G. Sowjanya, [5]Kiran Dehariya and [6]Anuradha Mangal

[1]M.Tech Scholar, Department of Electronics & Communication Engineering, SR Group of Institutions, Jhansi, (U.P.) India

[2]Professor and Dean, Research & Development, SR Group of Institutions, Jhansi, (U.P.) India

[3-6]Department of Computer Science & Engineering, Sagar Institute of Science, Technology & Research, Bhopal, (M.P.) India

information.dubey.abhishek@gmail.com, singhvinod34@gmail.com

ABSTRACT

The primary goal of the network traffic classification is to distinguish between different types of applications or traffic data. Received data packet analysis is carried out because modern communication networks require it. The process of classifying network traffic involves several stages, including pre-processing the data, extracting attributes, and performing the classification. Input for the classification stage is obtained from the dataset. The classification of network traffic is studied using several machine learning approaches in this article.

Keywords: *Network Traffic, Machine learning, Feature Extraction*

1. INTRODUCTION

The swift growth of the Internet of Things (IoT) has revolutionized various industries like healthcare, agriculture, and smart homes. By 2025, it is projected that over 4.1 billion IoT devices will be in use globally, playing a crucial role in people's everyday lives. However, their widespread internet connectivity poses significant security risks, leaving them vulnerable to various network threats. In the first half of 2020 [1], Nozomi Networks reported a substantial increase in new IoT botnet attacks, with 57% of IoT devices potentially being targeted, highlighting the pressing need for enhanced security measures. Denial-of-service (DoS) attacks serve as yet another means for attackers to deplete both device and network resources. Consequently, enhancing the security of IoT devices has become an imperative area of exploration [2]. To mitigate the potential damage stemming from various attack vectors, researchers are developing intrusion detection systems capable of identifying malicious behaviour within networks. These systems bolster communication security by monitoring systems in real-time and issuing alerts upon detecting anomalies. Machine learning has seen broad applications in the field of intrusion detection because to its recent quick advancements.

When contrasting machine learning algorithms with traditional detection methods, several advantages become evident [3]. Machine learning algorithms excel in intrusion detection within complex systems due to their ability to handle high-dimensional and nonlinear data, as well as their capacity to learn intricate patterns and rules from vast datasets. Furthermore, with the evolution of networks, a significant amount of network data has been accumulated, encompassing samples of various intrusions and anomalous behaviors. The wealth of training data provided by these extensive datasets ensures exceptional detection performance by machine learning algorithms [4]. These algorithms work by building an explicit or implicit model that makes it easier to classify patterns that have been noticed. This process is essential to both machine learning and data mining techniques. Machine learning techniques commonly address three main problems: clustering, regression, and classification. It allows for the treatment of network intrusion detection as a typical classification task. Consequently, building a system model often necessitates a labelled training dataset [5].

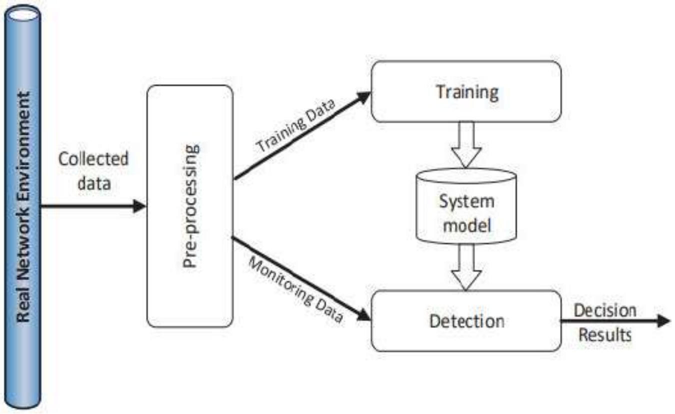

Figure 1: ML-NIDS architecture

Figure 1 illustrates the three basic phases that are commonly followed by all machine learning algorithms used for detecting intrusion in networks. Firstly, in the pre-processing stage, data instances gathered from the network environment are arranged and readied for input into the machine learning algorithm, involving tasks such as feature extraction and selection [6]. Then, in the training stage, a machine learning algorithm is applied to identify patterns in various kinds of data and create an appropriate system design. The observed traffic data is used as inputs to be evaluated against the system's representation once it has been built. An alarm will sound if the detected pattern matches a known threat. Both machine learning methods, both supervised and unsupervised, have been used to address issues in detection of intrusions. Many supervised learning classifiers have been successfully used to identify illegal access, including k-nearest neighbour (k-NN), support vector machines (SVM), decision trees, naïve Bayes networks, random forests, and artificial neural networks (ANN) [7]. Furthermore, network intrusion detection problems have been effectively solved by applying unsupervised learning approaches like self-organized map (SOM) and k-means clustering. Creating one ML mechanism that surpasses existent ones is currently highly challenging, primarily due to factors such as imbalanced training datasets and high computational demands. Consequently, hybrid machine learning techniques have garnered significant interest recently, including hierarchical classifiers and clustering with classifiers [8].

1.1 Machine learning (ML) algorithms for NID

Under the general heading of artificial intelligence (AI), machine learning (ML) refers to methods and strategies that enable computers to learn on their own by utilizing mathematical representations to extract insightful information from large datasets. Deep learning (DL) represents a subset of ML, characterized by its utilization of multiple hidden layers to extract intricate features from data. These techniques are renowned for their efficiency [9], owing to their deep architecture and capability to independently extract crucial features from datasets to produce outputs. The subsequent section will cover the most commonly employed ML algorithms for Intrusion Detection Systems (IDS).

i. Decision tree: Decision tree (DT), a fundamental supervised machine learning approach, employs a series of decision rules to perform tasks like as regression and classification on a specified dataset. The framework is arranged in a hierarchy, with nodes, branches, and leaves much as in a conventional tree. A characteristic or attribute is represented by each node, a possible result or class name is indicated by each leaf, and choices or rules are indicated by the branches [10]. The DT algorithm autonomously selects optimal features to construct a tree, mitigating the risk of overfitting, and subsequently prunes the tree to eliminate unnecessary branches. DT frameworks that are often used are CART, C4.5, and ID3. XGBoost and Random Forest (RF), two more sophisticated algorithms, are made up of several decision trees.

ii. K-Nearest Neighbour: Recognized as one of the most straightforward supervised ML techniques, KNN predicts the class of a given data sample by leveraging the concept of "feature similarity." It accomplishes this by assessing how closely the sample resembles its neighbours. The performance of the model hinges on the parameter ‘k’ of the KNN algorithm. When ‘k’ is exceedingly small, there's a risk of overfitting [11]. Conversely, employing a ‘k’ value that is excessively large may lead to misclassification of the sample instance.

iii. Support vector machine: Supervised Vector Machines (SVM) are supervised in nature that operate on the idea of a max-margin separation hyper-plane in n-dimensional feature space. It can be used to tackle both linear and nonlinear problems. For nonlinear problems, kernel functions are used. First, a low dimension input vector must be mapped into a feature space with a high dimension using the kernel function. The optimal maximal marginal hyper-plane is then created using the support vectors, acting as a decision boundary. By precisely dividing threats into categories that are dangerous and normal, the SVM approach can be utilized to increase the effectiveness and accuracy of NIDS [12].

iv. K-mean clustering: Clustering, a technique that groups highly similar data points together, enables the segmentation of data into meaningful clusters or groups. One popular unsupervised machine learning algorithm that employs centroid-based iterative learning is K-Means clustering. The number of centroids, or cluster centers, in the dataset is indicated by the parameter “K”. Typically, distance metrics are utilized to assign data points to their respective clusters, with the primary objective being the minimization of total gap across each cluster's centroids and data points [13].

v. Artificial neural network: ANN is a supervised approach that takes its cues from how the human nervous system works. It is made up of the connections between the nodes, or neurons, which are the processing units. These nodes are organized into an input layer, multiple hidden levels, and an output layer. As a learning technique, the ANN employs the backpropagation algorithm. The main advantage of an artificial neural network (ANN) is its ability to perform nonlinear modeling by learning from larger information. However, the main issue with training the ANN framework is that it is time-consuming due to its complexity, which inhibits learning and produces less-than-ideal outcomes.

vi. Recurrent neural networks: Recurrent neural networks (RNNs) are designed to extend feed-forward neural networks' capabilities to model sequence data [14]. An RNN's input, hidden, and output units are referred to as its memory elements. For every decision it makes, an RNN unit takes into account the outcome of its previous input as well as its current input. Semantic understanding, handwriting prediction, audio processing, and human activity recognition are just a few of the numerous fields in which RNN is widely used. Using RNN in an IDS can help with supervised classification and extraction of features. RNNs often have trouble with short-term memory when dealing with long sequences and have little ability to handle length sequences. A number of RNN modifications, such the gated recurrent unit (GRU) and long short-term memory (LSTM), are proposed to deal with these issues.

vii. Deep belief network (DBN): The DBN DL system is composed of multiple Restricted Boltzmann Machines (RBM) overlaid with a softmax classification layer. An RBM is a two-layer (input and hidden layer) model with bidirectional data flow. Each node in a DBN layer is linked to all other nodes in the layers before and succeeding it, however nodes have no connection within a single layer. DBN is pretrained using the greedy layer-wise learning technique in an unsupervised way [15]. A process of supervised fine-tuning is then employed to achieve the learning of helpful characteristics. In IDS, DBN is used for feature extraction and classification tasks.

viii. Convolutional neural network (CNN): CNNs are one kind of DL structure that performs well when processing data that is stored in arrays (CNN). It consists of three layers: an input layer, a fully connected layer, a feature extraction stack consisting of convolutional and pooling layers, and a classification layer that makes use of a softmax classifier [16]. CNN has made significant strides in the field of computer vision. They are used by the IDS for the supervised extraction and classification of features processes.

2. LITERATURE REVIEW

M. Baich, et.al (2022) suggested an approach on the basis of machine learning (ML) methods to detect intrusion in Internet of Things (IoT) [17]. The major emphasis was on detecting effectual ML methods. The suggested approach was quantified by conducting experiments. A dataset was utilized to analyze the results against the traditional methods. Two methods of selecting features and a method of extracting features were employed and their execution time was computed while detecting and classifying intrusions into five kinds, namely normal, DOS, probe, U2R, and R2L. The experiments demonstrated the supremacy of Decision Tree (DT) over other methods. The accuracy of this method was calculated 99.26% and its prediction time was counted 0.4 seconds.

X. Zhou, et.al (2022) presented a new hierarchical adversarial attack (HAA) strategy that used the level-aware black-box adversarial attack (LBAA) methodology to detect intrusions in IoT platforms using graph neural networks (GNNs) at a lower price point [18]. A shadow GNN framework known as an intelligent system depending upon a saliency map method was developed for creating adversarial examples. For this, the vital feature components having minimal perturbations were recognized and modified. In a network made up of IoT devices, a hierarchical method utilizing random walk with restart (RWR) was used to choose a group of nodes that were more susceptible to attacks and had a higher assault priority based on structural characteristics and total loss variations. The UNSW-SOSR2019 dataset was applied to simulate the introduced technique. The results depicted that the introduced technique led to enhance precision up to 30% in IoT scenarios.

P. Sanju, (2023) projected a hybrid metaheuristics-deep learning (MDL) technique to detect intrusion effectively in internet of things (IoT) systems [19]. An ensemble of recurrent neural networks (RNNs) was used in conjunction with an advanced metaheuristic algorithm to identify intrusions in the Internet of Things. By creating RNNs, the Long-Short Term Memory (LSTM) and Gated Recurrent Unit (GRU) were utilized to identify certain IoT attacks. For feature selection, the fractional derivative mutation (FDM) and Harris Hawk Optimization (HHO) techniques were used. On the IoT-23 and UNSW-NB15 datasets, the proposed approach was assessed for accuracy and effectiveness. Furthermore, a strong solution was developed that effectively identified infiltration in Internet of Things systems. The experimental findings showed that, compared to alternative approaches, the projected strategy was more effective. In IoT networks, this method proved to be reliable in identifying known as well as undiscovered assaults.

P. Mahadevappa, et.al (2024) developed a LDA-LR framework which detected intrusions at lower training time and higher accuracy [20]. Firstly, the data was pre-processed in order to mitigate the training time. The Linear Discriminant Analysis (LDA) method was employed for classifying data so that the data features were alleviated after simulating variables from a normal distribution. Moreover, a Logistic Regression (LR) was assisted in classifying the covariates based on their association with the feature-reduced variable. The developed framework was capable of detecting intrusions robustly and accurately. This framework was employed for isolating the classified data and devices from the other edge nodes and devices quickly and diminishing the chances of the intruder. In comparison to previous methods, the trial findings confirmed that the proposed framework performed well, offering 96.56% accuracy, 95.78% precision, and 0.04 seconds of training time. The resiliency of this framework was proved against diverse attacks which secured IoT applications more effectively.

Y. K. Saheed, et.al (2022) created an intrusion detection system (ML-IDS) that uses machine learning to find attacks on Internet of Things networks [21]. Implementing ML-supervised algorithm-based IDS for IoT was the main goal. Initially, the UNSW-NB15 dataset's characteristics were scaled using the Minimum-Maximum (min–max) concept of normalization in order to limit disclosure of information on the testing data. This dataset had a number of attacks as well as typical network traffic activities with nine different attack types. At second, Principal Component Analysis (PCA) was implemented to lessen the dimensionality. Finally, an assessment was carried out on six machine learning algorithms using the following metrics: precision, kappa, accuracy, recall, area under the curve, F1, and Mathew correlation coefficient (MCC). The simulation results exhibited that the designed system was more resistible against attacks and yielded 99.9% accuracy and 99.97% MCC.

R. Y. Aburasain, et.al (2021) formulated an Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection (EBWO-HDLID) method to detect attacks in the IoT-based Smart Farming scenario [22]. First of all, this method was deployed for capturing complex patterns and detecting considerable intrusions which ensured to make the network secure and reliable. After that, the bald eagle search (BES) algorithm was assisted in selecting features. Moreover, HDL method was utilized for detecting and classifying intrusions. In the end, the parameters were fine-tuned using EBWO algorithm. The ToN-IoT and Edge-IIoTset datasets were applied to quantify the formulated method against conventional methods. The experiments revealed the superiority of formulated method over others at accuracy of 98.35%, precision of 84.85%, recall of 80.95%, and F1-Score of 82.79%. Besides, this method was proved applicable for automated ID and securing the smart farming scenarios.

S. A. Bakhsh, et.al (2023) presented a DL-based IDS in which FFNN,LSTM, and RandNN algorithms were implemented for protecting IoT networks from cyberattacks [23]. The initial algorithm was deployed for handling complicated IoT network traffic patterns, and the second algorithm was utilized to capture long-term dependencies available in the network traffic. The potential to learn data of last algorithm was considered for adapting and learning from network data. The defense systems were adopted for enhancing the cyber security against complex cyber threats and ensured that the sensitive data was secured. The results on CIC-IoT22 dataset exhibited that the presented approach outperformed other techniques. Furthermore, the initial algorithm yielded an accuracy of 99.93%, second one offered 99.85% and last one offered 96.42% accuracy to detect intrusions. The swift responses were developed for tackling security problems in IoT networks so that intrusions were effectively more accurately.

S. Latif, et.al (2022) recommended a lightweight dense random neural network (DnRaNN) to detect intrusion in IoT [24]. This algorithm was suitable in resource-constrained IoT networks as it had inherent generalized potentials and distributed nature. The ToN_IoT dataset was exploited for simulating the recommended algorithm under dissimilar hyperparameters. Diverse parameters were considered to analyze the results of this algorithm under binary class and multiclass scenarios. The results proved that the recommended algorithm provided an accuracy of 99.14% in primary scenario and 99.05% in latter one. Additionally, this algorithm was feasible for classifying 9 dissimilar assaults on the IoT at higher accuracy.

J. Saikam, et.al (2024) suggested a network intrusion detection (NIDS) method in which deep network (DN) was integrated with hybrid sampling [25]. The Difficult Set Sampling Technique (DSSTE) was employed for mitigating the noise samples in the majority category. Afterward, a Deep Convolutional Generative Adversarial Network (DCGAN) was adopted for augmenting the minority sample size. Besides, a deep network (DN) algorithm was employed based on DenseNet169 for extracting spatial features and Self Attention-based Transformer (SAT-Net) model for extracting temporal features. This method was effective for extracting distinctive attributes of data. At last, the attacks were classified through an Enhanced Elman Spike Neural Network (EESNN) algorithm. The suggested method was computed on BOT-IOT, ToN-IoT, and CICIDS2019 datasets. The simulation indicated that the suggested method was more robust against intrusions as compared to other techniques. Moreover, this method yielded higher accuracy, recall, and precision, and lower false alarm rate (FAR).

M. Vishwakarma, et.al (2023) established a two-fold IDS to detect intrusions for internet of things (IoT) [26]. The initial stage was executed for categorizing data into 4 sections in accordance with diverse data kinds. Diverse version of the Naive Bayes (NB) method was employed to classify this data. Thereafter, a majority voting was presented for selecting the final results of classifying attacks. The next phase was emphasized on transmitting those data that appeared normally or benign in initial stage and classifying them based on an unsupervised elliptic envelope (UEE). The NSL-KDD, UNSW_NB15, and CIC-IDS2017 datasets were applied to conduct experiments. The experimental results confirmed the effectiveness of established method over traditional methods to detect intrusions. In addition, this method offered an accuracy of 97%, 86.9% and 98.59% on these datasets respectively at lower false positive rate (FPR) in second stage while detecting intrusions.

2.1 Comparison Table

Author/Year	Technique Used	Dataset	Parameters	Results	Advantages	Limitations
M. Baich, et.al (2022)	An approach on the basis of machine learning (ML) methods	UNSW-NB15, BOT-IOT, and NSL-KDD datasets	Accuracy and prediction time	The experiments demonstrated the supremacy of Decision Tree (DT) over existing methods.	The accuracy of this method was calculated 99.26% and its prediction time was counted 0.4 seconds.	The SVM algorithm had consumed higher execution time.
X. Zhou, et.al (2022)	A new hierarchical adversarial attack (HAA) technique	UNSW-SOSR2019 dataset	Precision	The results depicted that the introduced technique led to enhance precision up to 30% in IoT scenarios.	This technique was resistible against attacks in IoT.	This technique was not applicable to detect all adversarial attacks.
P. Sanju, (2023)	A hybrid metaheuristics-deep learning (MDL) technique	IoT-23 and UNSW-NB15 datasets	Accuracy and efficacy	The experimental results indicated that the projected technique was more effective in contrast to other methods.	This technique was robust for detecting both known and unknown attacks in IoT networks.	This technique was ineffective for handling dynamic and growing IoT network.
P. Mahadevappa, et.al (2024)	LDA-LR framework	NSL-KDD and UNSW-NB15 datasets	Training time, precision and accuracy	The experimental results validated that the developed framework was performed well in contrast to other techniques	The resiliency of this framework was proved against diverse attacks which secured IoT applications more	The efficacy of this framework was restricted to utilized datasets only concerning generalized ability.

				and offered 96.56% accuracy, 95.78% precision, and 0.04s training time.	effectively.	
Y. K. Saheed, et.al (2022)	Machine learning-based intrusion detection system (ML-IDS)	UNSW-NB15 dataset	Accuracy, the area under the curve, recall, F1, precision, kappa, and MCC	The simulation results exhibited that the designed system yielded 99.9% accuracy and 99.97% MCC.	This system was more resistible against attacks.	This system was unsuitable in real-time scenarios.
R. Y. Aburasain, et.al (2021)	Enhanced Black Widow Optimization with Hybrid Deep Learning Enabled Intrusion Detection (EBWO-HDLID) method	ToN-IoT, and Edge-IIoTset datasets	Accuracy, precision, recall and F1-Score	The experiments revealed the superiority of formulated method over others at accuracy of 98.35%, precision of 84.85%, recall of 80.95%, and F1-Score of 82.79%..	This method was proved applicable for automated ID and securing the smart farming scenarios.	This method had computation complexity.
S. A. Bakhsh, et.al (2023)	DL-based IDS approach	CIC-IoT22 dataset	Accuracy	The initial algorithm yielded an accuracy of 99.93%, second one offered 99.85% and last one offered 96.42% accuracy to detect	The swift responses were developed for tackling security problems in IoT networks so that intrusions were effectively more	This approach was ineffective to manage the complexity of IoT data.

				intrusions.	accurately.	
S. Latif, et.al (2022)	Lightweight dense random neural network (DnRaNN)	ToN_IoT dataset	Accuracy	The results proved that the recommended algorithm provided an accuracy of 99.14% in primary scenario and 99.05% in latter one.	This algorithm was feasible for classifying 9 dissimilar assaults on the IoT at higher accuracy.	This algorithm was not performed well with respect to hardware requirements.
J. Saikam, et.al (2024)	Network intrusion detection (NIDS) method	BOT-IOT, ToN-IoT, and CICIDS2019 datasets	Accuracy, recall, and precision, and lower false alarm rate (FAR)	The simulation indicated that the suggested method was more robust against intrusions as compared to other techniques.	Moreover, this method yielded higher accuracy, recall, and precision, and lower false alarm rate (FAR).	This method was lack of storage capacity.
M. Vishwakarma, et.al (2023)	A two-fold IDS	NSL-KDD, UNSW_NB15, and CIC-IDS2017 datasets	Accuracy and false positive rate (FPR)	This method offered an accuracy of 97%, 86.9% and 98.59% on these datasets respectively in second stage while detecting intrusions.	The effectiveness of established method was proved over traditional methods to detect intrusions.	The performance of this method was mitigated in case of multiclass classification

CONCLUSION

Three different approaches named payload-based, port-based, and flow statistics-based are used to categorize network traffic. Classifying the network traffic allows for the recognition of different application kinds or traffic data types. In real-world communication networks, data that is received packets must be recognized. The conventional port-based approach takes standard ports into account. To categorize the network traffic, several stages are carried out, including pre-processing, feature extraction, and classification. This study examines many machine learning techniques for network traffic classification.

REFERENCES

[1] M. S. Korium, M. Saber and P. H. J. Nardelli, “Intrusion detection system for cyberattacks in the Internet of Vehicles environment”, Ad Hoc Networks, vol. 153, pp. 147-158, 3 November 2023

[2] F. J. Mora-Gimeno, H. Mora-Mora, B. Volckaert and A. Atrey, "Intrusion Detection System Based on Integrated System Calls Graph and Neural Networks," in IEEE Access, vol. 9, pp. 9822-9833, 2021

[3] N. O. Aljehane, H. A. Mengash and M. Assiri, “Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security”, Alexandria Engineering Journal, vol. 86, pp. 415-424, 7 December 2023

[4] Z. Jin, J. Zhou and C. Duan, “FL-IIDS: A novel federated learning-based incremental intrusion detection system”, Future Generation Computer Systems, vol. 151, pp. 57-70, 18 September 2023

[5] Z. Sun, G. An and Y. Liu, “Optimized machine learning enabled intrusion detection 2 system for internet of medical things”, Franklin Open, 22 November 2023

[6] P. Sanju, “Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks”, Journal of Engineering Research, vol. 1, pp. 778-789, 19 June 2023

[7] S. Li, Y. Cao and N. Ahmad, “HDA-IDS: A Hybrid DoS Attacks Intrusion Detection System for IoT by using semi-supervised CL-GAN”, Expert Systems with Applications, vol. 128, pp. 47-57, 28 October 2023

[8] T. R. Gadekallu, N. Kumar and P. K. R. Maddikunta, “Moth–Flame Optimization based ensemble classification for intrusion detection in intelligent transport system for smart cities”, Microprocessors and Microsystems, vol. 156, pp. 781-789, 30 September 2023

[9] S. Fraihat, S. Makhadmeh and A. Al-Redhaei, “Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm”, Internet of Things, vol. 22, pp. 12-25, 16 May 2023

[10] L. Yang, J. Li, L. Yin, Z. Sun, Y. Zhao and Z. Li, "Real-Time Intrusion Detection in Wireless Network: A Deep Learning-Based Intelligent Mechanism," in IEEE Access, vol. 8, pp. 170128-170139, 2020

[11] T. Gaber, J. B. Awotunde and W. Li, “Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks”, Internet of Things, vol. 24, pp. 47-57, 29 October 2023

[12] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez and R. A. Abd-Alhameed, "HIDROID: Prototyping a Behavioral Host-Based Intrusion Detection and Prevention System for Android," in IEEE Access, vol. 8, pp. 23154-23168, 2020

[13] X. Yuan, S. Han and F. Zhang, “A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system”, Computers & Security, vol. 137, pp. 45-55, 10 December 2023

[14] S. Layeghy, M. Baktashmotlagh and M. Portmann, “DI-NIDS: Domain invariant network intrusion detection system”, Knowledge-Based Systems, vol. 273, pp. 1-6, 12 May 2023

[15] X. Gao, Q. Wu, J. Cai and Q. Li, "A Fusional Intrusion Detection Method Based on the Hierarchical Filtering and Progressive Detection Model," in IEEE Access, vol. 11, pp. 131409-131417, 2023 [17] M. Baich, T. Hamim and Y. Chemlal, “Machine Learning for IoT based networks intrusion detection: a comparative study”, Procedia Computer Science, vol. 215, pp. 742-751, 2022, doi: 10.1016/j.procs.2022.12.076.

[16] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," in IEEE Access, vol. 9, pp. 138432-138450, 2021

[17] M. Baich, T. Hamim and Y. Chemlal, “Machine Learning for IoT based networks intrusion detection: a comparative study”, Procedia Computer Science, vol. 215, pp. 742-751, 2022, doi: 10.1016/j.procs.2022.12.076.

[18] X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. -K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9310-9319, 15 June15, 2022, doi: 10.1109/JIOT.2021.3130434.

[19] P. Sanju, “Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks”, Journal of Engineering Research, vol. 11, no. 4, pp. 356-361, 19 June 2023, doi: 10.1016/j.jer.2023.100122.

[20] P. Mahadevappa, R. K. Murugesan and G. Alkawsi, “A secure edge computing model using machine learning and IDS to detect and isolate intruders”, MethodsX, vol. 17, pp. 96-105, 13 February 2024, doi: 10.1016/j.mex.2024.102597

[21] Y. K. Saheed, A. I. Abiodun and R. Colomo-Palacios, “A machine learning-based intrusion detection for detecting internet of things network attacks”, Alexandria Engineering Journal, vol. 61, no. 12, pp. 9395-9409, 28 March 2022, doi: 10.1016/j.aej.2022.02.063.

[22] R. Y. Aburasain, "Enhanced Black Widow Optimization With Hybrid Deep Learning Enabled Intrusion Detection in Internet of Things-Based Smart Farming," in IEEE Access, vol. 12, pp. 16621-16631, 2024, doi: 10.1109/ACCESS.2024.3359043.

[23] S. A. Bakhsh, M. A. Khan and J. Ahmad, “Enhancing IoT network security through deep learning-powered Intrusion Detection System”, Internet of Things, vol. 24, 13 September 2023, doi: 10.1016/j.iot.2023.100936.

[24] S. Latif et al., "Intrusion Detection Framework for the Internet of Things Using a Dense Random Neural Network," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6435-6444, Sept. 2022, doi: 10.1109/TII.2021.3130248.

[25] J. Saikam and K. Ch, "EESNN: Hybrid Deep Learning Empowered Spatial–Temporal Features for Network Intrusion Detection System," in IEEE Access, vol. 12, pp. 15930-15945, 2024, doi: 10.1109/ACCESS.2024.3350197.

[26] M. Vishwakarma and N. Kesswani, “A new two-phase intrusion detection system with Naïve Bayes machine learning for data classification and elliptic envelop method for anomaly detection”, Decision Analytics Journal, vol. 7, pp. 456-462, 22 April 2023, doi: 10.1016/j.dajour.2023.100233