Journal of Harbin Engineering University
ISSN: 1006-7043
Vol 45 No. 5
May 2024

Analysis of Hybrid Deep Learning Algorithms for Distributed Denial of Service Attack Detection in the Internet of Things

Manjusha V. Khond Research Scholar, Dr. M.R.Sanghavi ,
MET's Institute of Engineering BKC Nashik, Affiliated to SPPU Pune
Prof. SNJB COE Chandwad , Affiliated to SPPU Pune

Abstract
The Internet of Things (IoT) plays a pivotal role in shaping smart city environments by enabling the interconnectivity of various devices over the internet backbone. However, ensuring the security of IoT systems is of paramount importance, given their vulnerability to diverse cyber threats, including Distributed Denial of Service (DDoS) attacks. This survey focuses on the classification and detection of DDoS attacks within IoT ecosystems, employing a hybrid approach incorporating Deep Learning (DL) algorithms. The analysis reveals that hybrid classifiers outperform other methods, showcasing superior performance across essential performance metrics. These optimized hybrid classifiers, primarily evaluated on accuracy, demonstrate heightened efficiency in detecting attacks within IoT environments. Notably, the most frequently employed classifiers for attack detection are the Hybrid Convolutional Neural Network (Hybrid CNN) and Long Short-Term Memory (LSTM) models. In summary, our survey examines the landscape of hybrid DL algorithms used for IoT attack detection, emphasizing performance metrics, publication timelines, methodology diversity, and notable achievements in this critical field of IoT security.

Keywords: Hybrid DL classifiers, DDoS, IoT

1. Introduction

Any device can be connected to the Internet, which is the basis of the IoT [51]. Smart cities have been developed as a result of this technology, in which essential infrastructure elements like energy, water resources, and traffic are tracked and handled online [52] [53] [1]. The IoT, which is defined as a global network of all the networked devices with dispensed unique addresses, has experienced a tremendous expansion in recent years. Different communication protocols and sensor capabilities are used by IoT devices and where these gadgets are computationally capable of data analysis and service provision [3]. Researchers have been concentrating on finding network disturbances due to a rise in cybercrime. Cyberattacks are used to target individual computers and traditional computer networks and individual computers, but as communication organization has expanded to include the medical, electric vehicles, the IoT, and 5G [54-57], these have increasingly come under the cyberattacks [9]. The lack of intelligent intrusion detection algorithms and insufficient security measures for IoT networks reduce their vulnerability to a variety spoofing, data outflow, etc. [58] [12].

A malicious method known as a DDoS attack uses large amounts of data to overcome a target's bandwidth or other resources to reduce the accessibility of services in the networks of computers [5]. A DDoS attack takes place when attackers overcome the victim's system with requests, rendering their system and the unavailable network resources [59] [6]. Machine learning algorithms (ML) have been used in several ways to detect intrusions into the IoT [10]. Intrusion Detection Systems (IDS) based on ML and DL algorithms have more benefits than conventional techniques, but as the number of attacks rises, overfitting issues also arise [60]. As a result, to create an intelligent IDS that can be measured for more attacks, the right DL algorithms must be used [12]. K-Nearest Neighbor (KNN), Neural Networks (NN), Support Vector Machine (SVM), and DL are some of the popular supervised ML techniques for IoT attack detection [14]. DL has recently been demonstrated to be particularly efficient at identifying cyberattacks in smart cities [61] [62]. As a result, the effectiveness of the hybrid DL models is examined, and the results

indicated that they are capable of offering high accuracy rates [1].

In this research, hybridized DL methods is analyzed concerning numerous research papers. This survey reveals that various existing research expertise majorly focused on the detection of attackers in the IoT by utilizing DL methods. The performance measures, year of publication, different DL methods, and achievements are the significant terms considered for this analysis, in addition to the challenges.

The rest of the paper is structured as follows: Section 2 reveals the review of the existing works based on the DL methods for attack detection. Section 3 reveals the analysis of the DDoS attack detection in IoT using the hybrid DL methods. Section 4 reveals the challenges as well as the research gaps that arise during the research. Finally, concludes the paper in section 5.

2. Related works

The review of the existing works using the hybrid DL methods is revealed in this section. Asmaa A. Elsaeidy *et al*. [1] developed a hybridized DL model for detecting the DDoS attack and the replay by combining the Boltzmann machine and the deep CNN. Here, the efficacy of the hybridized model is determined by generating the data related to the DDoS as well as the replay attacks. This hybridized model overcomes the issues of a lesser number of features as well as the distribution of complicated probability involved in the data. Amiya Kumar Sahu *et al*. [2] introduced a mechanism using hybrid CNN and the LSTM classifiers. These hybridized classifiers accurately extract the data suitable for the representation of features and also for the classification of attacks. The classification of malicious attacks is accurately classified by the hybrid DL models and the security modeling is easily accessible in addition to the computational overhead. Danish Javeed *et al*. [3] developed the combination of Cuda-bidirectional LSTM (Cu-BiLSTM) and the Cuda-deep NN, gated recurrent unit (Cu-DNNGRU) for efficient attack detection. The efficiency of the hybridized model is high in accuracy and speed, in addition, the testing time of the developed hybridized classifiers is only a few seconds. Ihtisham Ullah *et al*. [4] introduced a hybridized method using the CNN and the LSTM for identifying the threats and various attacks in the fog to the IoT network, in which the profociency of the introduced method is analyzed by the response time as well as the accuracy. For the multiclass classification, the developed method is more effective in terms of the detection of of threats. Mohammad Najafmehr *et al*. [5] presented a technique that is the combination of both the density-based clustering with noise algorithm and the principal component analysis. These combined models are raised from the unsupervised as well as the supervised algorithms, initially, the clustering algorithms are utilized to split the normal data from the anomalous traffic. Yuanyuan Wei *et al*. [6] combine the autoencoder (AE) and the multi-layer perceptron (MLP) network for the efficient classification of attack. The autoencoder plays a major role in the extraction of relevant features from the data, these selected features are utilized by the MLP as inputs for the effective classification of attacks. Thus, the hybridized model overcomes the issue of computational overhead and eliminates the irrelevant feature values. Safi Ullah *et al*. [7] utilized the hybrid model of LSTM and GRU algorithms for identifying malicious attacks than the existing DL as well as machine learning algorithms. The malicious attacks are well detected by the developed hybrid LSTM and the GRU algorithms with high accuracy. The performance of the developed method is low, which is further enhanced by integrating the additional layers. Daniyal Alghazzawi *et al*. [8] presented the combined model of CNN and the BiLSTM classifiers for effective attack detection in the IoT network with enhanced feature selection. The recent, as well as the most relevant categories, are considered. The utilization of single data and single statistical methods to determine the significant features are the major limitations of this model. Mohammed Y. Alzahrani and Alwi M Bamhdi [9] presented an innovative combined model of CNN with the LSTM network to determine the various attacks present in IoT devices. This method majorly focuses on the two serious and common attacks, which are recorded in the security system. The optimal performance is attained by the combined model of the DL networks. Cristiano Antonio de Souza *et al*. [10]

developed the hybrid DL classifiers of DNN and K-NN for intrusion detection in IoT devices. The processing time of the hybrid DNN, as well as the KNN classifiers, are very much reduced which even though enhances the performance of the classifier. Arvind Prasad and Shalini Chandra [11] presented a voting-based framework to conflict attacks with three different modes of high accuracy mode (HAM), defensive fast detection mode (DFDM), and fast detection mode (FDM). The network traffics are classified by the FDM, the malicious-based network traffics are identified by the DFDM, and the HAM is also responsible for the attack detection with high accuracy, which is activated when the server is stable. B. Jothi and M. Pushpalatha [12] presented an innovative technique for determining the presence of malicious devices using the whale-integrated LSTM (WILS). This innovative method detects the type of attacks involved in the IoT network with the enhanced response time, and minimum predicting time. Prabhat Kumar *et al*. [13] utilized the three different ML-based algorithms for further classification of attacks by considering the input as the set of features. The three different algorithms are XG Boost, KNN, and the random forest (RF), which analyze the IoT networks for detecting the data traffic. The performance of the developed hybridized reduced feature analyzing system is better by considering the limited features. Subramonian Krishna Sarma [14] optimally tuned the developed deep belief network (DBN) by introducing the hybridized algorithm of firefly and grey wolf. The classification of attacks takes place through the optimal tuning of the activation function in the DBN classifier. The major limitation of this type of classifier is time-consuming and is more complex, which is required to be further improvement. Amritanshu Pandey *et al*. [15] integrated various machine learning-related algorithms, which include RF-KNN-LR, RF-NB-KNN, and RF-SVM for the effective classification of attacks. The testing data is analyzed by the RF-SVM classifier; depending on attaining high accuracy, the RF-NB-KNN classifier is utilized, and the RF-KNN-LR classifier determines whether the network is normal or looks malicious. Jabed Al Faysal *et al*. [16] developed hybridized machine learning technique for the different intrusion detection systems using the eXtreme gradient boosting-RF (XGB-RF) classifier. The performance of the developed hybrid classifiers is better by combining the benefits of both the classifiers in detecting the intrusion detection technique. The detection time of the developed method is high when attaining the accuracy maximum. Ozgur Tonkal *et al*. [17] utilized the hybridized classifiers for classifying the DDoS attack as a result of the pre-processing and the feature selection. The utilized classifiers for selecting the required features and also to classify the attacks are KNN, ANN, DT, and SVM. The performance of the developed methods is better and there is the requirement of diversity of attacks. Li Xinlong1 and Chen Zhibin [18] presented a hybridized DL method using the hierarchical memory with the LSTM for detecting the various malicious web attack on the data signals. The labels involved in the data are not required in the utilized unsupervised learning algorithms, and where the training data is required for identifying the threshold value. M. Ganesh Karthik and M. B. Mukesh Krishnan [19] introduced the IoT attack detection method by integrating the techniques of RF and synthetic minority over-sampling technique (RF-SMOTE). The hybridized model eliminates the latency in the nodes of IoT, which further minimizes the false prediction of the attackers in terms of the various security measures in the network. Tong Liu *et al*. [20] introduced the hybridized DL-based methods using the autoencoder and the multi-layer perceptron for the detection of DDoS among the provided stakeholders in the network. The average detection of attackers in the network is much enhanced by utilizing DL-based hybridized classifiers. To ensure the security of the smart intelligent transportation system from cyber-attacks, these hybridized classifiers are applicable. Abdullah Emir Cil *et al*. [21] presented the DNN for identifying and classifying the attackers in the network signals. The utilized DNN attains high precision in detecting DDoS attacks and is also provided as the intrusion detection system along with the various security layers. The DDoS attacks on real-time data using hybridized DL methods are more effective. Pheeha Machaka *et al*. [22] utilized the KNN models for detecting the intrusions that

evolved in the IoT during the communication of interconnected devices. The performance of the utilized KNN is enhanced by integrating the communication of data framing as well as the measure as standard deviation. The IP addresses, source, destination, and ports are not considered for evaluating the performance of the KNN classifier in the classification of DDoS attacks. Muhammad Ashfaq Khan [23] developed the hybrid convolutional recurrent NN based on the IDS, in which the local features are selected by the CRNN, and the temporal features are selected by the RNN to enhance the prediction as well as the performance of the system. The attached traffic data may be modified depending on the application of various datasets, here only a single dataset is utilized. Reddy SaiSindhuTheja and Gopal K. Shyam [24] presented the DBN for the classification of attacks, which is optimized by the median fitness-oriented sea lion optimization (MFSLoN) algorithm. The hyperparameters of the DBN classifier are well tuned for the classification process by the developed optimization. This method does not focus on the attacks involved in the cloud infrastructure, which further reduces the significance of utilizing the developed optimization. Rami J. Alzahrani and Ahmed Alzahrani [25] utilized six various kinds of ML algorithms, which include KNN, SVM, NB, DT, RF, and LR for the intrusion detection. The detection of anomalies in the IoT network using the intrusion detection system outcomes various challenges, and there is the absence of traffic datasets belonging to the publicly available IoT network. Auther Makuvaza *et al*. [26] developed the DNN in software-defined network (SDN) by splitting the data as testing and training. The DNN classifier is tested and trained for the classification process with the four different layers. The SDN network has the tendency to regulate the network from the common central point, in which the SDN is get affected by the various types of attacks. Segun I. Popoola *et al*. [27] hybridized the SMOTE with the DRNN for balancing the class imbalance as well as the representation of hierarchical features from the balanced data for the classification. The performance measures of the hybridized method are affected by the presence of imbalanced data in the training samples. K.S. Niraja and Sabbineni Srinivasa Rao [28] implemented the deep autoencoder for detecting malicious attacks for ensuring security. The process of encoding and decoding is considered for the accurate classification as well as the detection of attacks by the deep autoencoder. The performance of the deep autoencoder is significantly improved than the ensembled autoencoder in terms of detecting malicious behaviors. Haomin Wang and Wei Li [29] hybridize the CNN with the transformers in SDN. The transformer structure is integrated individually for the normalization layer to speed up the convergence and enhance the space of optimization. This developed model is not suitable for multilabel classification even though there is the existence of high evaluation ability. Prahlad Kumar *et al*. [30] utilized both DL and ML algorithms for the identification of DoS and DDoS attacks in the network. The DL methods play a major role in transferring the data with high-security resources. Thus, the ML models are applicable only for the data with less traffic, and also the utilization of resources is minimal. Umar Islam *et al*. [31] utilized the most effective machine learning techniques, such as SVM, KNN, and RF for classifying the DDoS attacks. The SVM plays a significant role in identifying the attacks and is more robust, this utilized model does not apply to the offline datasets depending on the supervised learning algorithms. Ruba Abu Khurma *et al*. [32] selected the features by integrating the optimization of the Salp swarm and the ant lion as the wrapper feature selection model. The issue of high dimensionality space in addition to the IoT attack detection is regulated in the intrusion detection system. The performance sis better even in the presence of imbalanced datasets. E. S. Phalguna Krishna and Arunkumar Thangavelu [33] presented the hybridized algorithms of the lion and the firefly algorithm for detecting the various attacks by analyzing the ranking. As a result of the feature selection process, the presence or the absence of attacks is classified by the RF classifier. The performance of classifying the attacks is enhanced by the integrated optimization for the various kinds of attacks in the IoT network. K. Lakshmi Narayanan *et al*. [34] prevented the DDoS attacks by introducing the ML-dependent NB classifier to determine and round-trip time. With

the utilization of the authorized code, the black hole attack that evolved in the wireless network is analyzed, in addition to the wormhole attack. To satisfy both the authentication and the integrity, the developed method is required to be enhanced by an effective encryption algorithm. R. Doriguzzi-Corin *et al*. [35] presented a lightweight DL-based DDoS detection system (LUCID) that attains the features of a CNN for the classification of traffic flows. In terms of the resource-confined operational environments, the presented method is more relevant for the detection of DDoS. The stability of the developed model is high in the attack detection of DDoS traffic. Segun I. Popoola *et al*. [36] classify the network traffics by employing the optimal DNN with the federated DL (FDL) model in the IoT edge devices. The network traffic is classified by the DNN and the aggregation of the DNN is renovated by integrating the FDL algorithm. The communication round of the developed method is high, which is need to be improved, and the training time of the model is required to be reduced. Rajaputhri Maharaja *et al*. [37] provided security against the various malicious attacks in the IoT systems by introducing the fog computing-based security (FOCUS) system. The selection of a threshold for ensuring security in communication is applied by the FOCUS, which classifies the traffic as suspicious, trusted, and untrusted. The computational complexity may arise the computational delay, which is avoided by the developed FOCUS model. Raja Majid Ali Ujjan *et al*. [38] identify the irrelevant nodes present in the network by utilizing the polling-based traffic sampling and the sFlow with the DNN. The detection of attacks by the DNN is enhanced by analyzing each sample implementation of the data as well as the SDN controller. The sampling methods offer flexible and effective handling of data, which enhances the classification of the attacks. Najla Al-Taleb and Nazar Abbas Saqib [39] hybridized the CNN and quasi-RNN (QRNN) not only for enhancing the classification performance but also improves the accuracy of the classifiers. The false prediction of the attacks is minimized by improving the process of feature extraction, and the classification accuracy. The evaluation of the developed model using real-time data is challenging because of the security and privacy concerns of residents in smart cities with a centralized system. Jiushuang Wang *et al*. [40] introduced the DL algorithm in the network database using the CNN in the software defined-IoT (SD-IoT). The flow entry collection model gathers the statistical information via the protocol and if the gathering is processed infrequently, there is an occurrence of delay in the detection as well as the classification of attacks. Majda Wazzan *et al*. [41] identify the botnet attacks in the IoT by fusing the DL classifiers as CNN with the LSTM. The accuracy of the method is high in classifying the attacks in the early stage. The output is not subsampled by the hybridized DL methods, which results in the issue of overfitting when the model is trained. Nisha Ahuja *et al*. [42] introduced the hybrid model of SVM with the RF classifier for detecting the DDoS attacks, and also for the classification process. The traffic involved in the network is classified by the hybridized classifiers and attains the minimum false prediction with high accuracy. The computationally intensive of the hybridized classifiers is high for the developed methods. Francisco Sales de Lima Filho *et al*. [43] classify the traffic in the network by the RF classifier utilizing the various sampling rates. The requirement of the RF classifier is high in terms of the efficiency of computation and hit rates. The most significant attacks are not considered for the detection mechanism using the developed classifier and require enhancement in the multiple-class classification. Ismail *et al*. [44] utilized a ML-based technique for the prediction and classification of the DDoS attacks. The RF and the eXtreme gradient boosting (XG Boost) are the hybridized classifiers for the attack detection as well as the classification process. The non-labeled datasets are not considered along with the developed hybrid classifiers to reveal better performance. Hasan Alkahtani and Theyazn H. H. Aldhyani [45] hybridized both the CNN and the LSTM classifiers to predict botnet attacks, which eliminates the risk of other DDoS attacks. The developed model further enhances the security issues as well as the detection of attackers in the IoT network. The several undetermined patterns involved in the IoT networks are identified by the IoT networks for improving attack detection more efficiently. Satish Pokhrel *et al*. [46] presented the

K-Nearest Neighbour (KNN) classifier for ensuring security in the IoT network. Security is considered the major concern in the distributed communication system by eliminating the various types of botnet attacks. In the detection of a botnet, the developed KNN classifier with the SMOTE algorithm plays a significant role in the reliable performance. Ihtisham Ullah *et al*. [47] presented an adaptive ML-based SDN-enabled DDoS detection and mitigation (AMLSDM). The identification and mitigation of DDoS attacks are successful by enabling security in the SDN. In order to detect phishing attacks, there is the requirement of enhancing the implementation in the network. Gonzalo De La Torre Parra *et al*. [48] ensembles the DL method based on the cloud infrastructure, in which the CNN and the LSTM classifiers are hybridized to mitigate and detect phishing as well as botnet attacks. The developed hybridized method can identify the attacks in a distributed manner both at the back-end level and the device. Salva Daneshgadeh *et al*. [49] developed the hybridized online detection techniques for the attacks in the IoT network, the kernel-based algorithm, and the mahala Nobis distance (KOAD-MD) are utilized. The general behavior of data traffic is modeled to design the normal as well as the abnormal data resulting from the KOAD, in which the distance between the normal as well as the abnormal data is identified by the mahala Nobis distance. Murk Marvi *et al*. [50] utilized the light gradient boosting machine (LGBM) for enhancing the classification and detection of attacks by training the machine learning model. The achievements of the developed LGBM classifier are analyzed by the generalized behavior and the satisfactory performance in the unknown attacks. The developed LGBM model performance is further enhanced by reducing the dimension of the feature space. The developed model is not utilized in the attack detection of software-defined networks or the IoT network.

3. Analysis and Discussion

In this section, we undertake an analysis of DDoS attack detection within the IoT context. The examination encompasses factors such as publication dates, performance metrics, a spectrum of DL techniques, and notable accomplishments in the field.

3.1 Analysis relying on the year of publication

Table 1 presents an examination of DDoS attack detection within the IoT domain, utilizing DL techniques, categorized by publication years. The research papers under scrutiny span from 2018 to 2022, with a notable concentration of publications in the year 2021, primarily focusing on DDoS attack detection within IoT. The graphical representation of this paper analysis is visually depicted in Figure 1.

Table 1. Year of publication

Year of publication	Reviewed papers
2018	[49]
2019	[15] [43]
2020	[10] [24] [35] [37] [38] [40] [48]
2021	[1] [2] [3] [4] [6] [8] [12] [13] [14] [17] [19] [20] [21] [22] [23] [25] [26] [27] [28] [29] [32] [33] [34] [36] [42] [45] [46] [50]
2022	[5] [7] [9] [11] [16] [18] [30] [31] [39] [41] [44] [47]

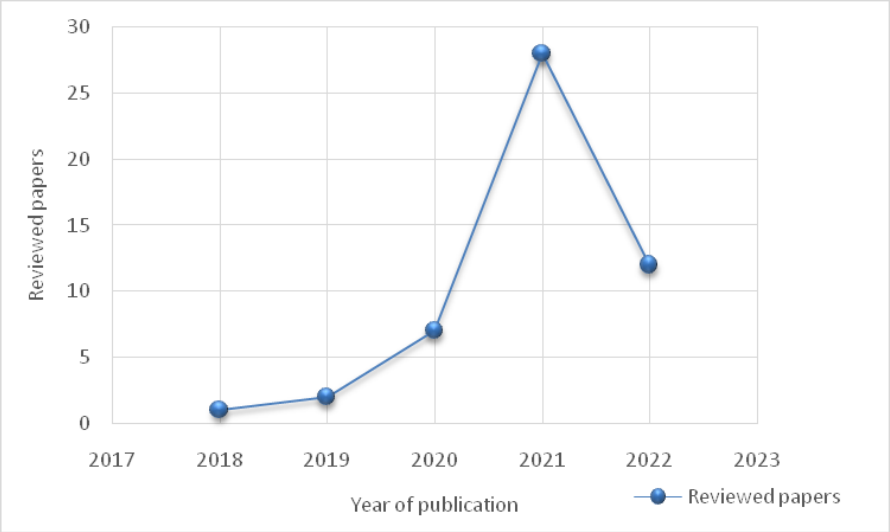


Figure 1. Chart analysis relying on the year of publication

3.2 Analysis relying on the various DDoS attack detection methods

Table 2 provides an overview of the analysis concerning specifically focusing on hybridized DL classifiers. The findings from the review demonstrate a prevailing trend where a majority of recent papers leverage a hybrid approach involving CNN and LSTM. Additionally, DNN, Autoencoder-Multilayer Perceptron (AE-MLP), and RF-SVM are also noteworthy methods frequently employed for IoT network attack detection. For a visual representation of this analysis, Figure 2 illustrates a chart showcasing the various methods examined.

Table 2. Various DDoS attack detection methods

Method	Reviewed papers
Deep RBM + deep CNN	[1]
CNN + LSTM	[2] [4] [9] [41] [45] [48]
Cu-DNNGRU + Cu-BiLSTM	[3]
DBSCAN and PCA	[5]
AE+MLP	[6] [20]
LSTM+GRU	[7]
CNN + BiLSTM	[8]
DNN+KNN	[10]
VMFCVD (FDM+DFDM+HAM)	[11]
WILS-TRS	[12]
RF+KNN+ XG Boost	[13]
FAE-GWO-DBN	[14]
RF-SVM	[15] [42]
RF-Naive Bayes-KNN	[15]
RF-KNN-LR	[15]
XGB-RF	[16]
KNN, DT, SVM, ANN	[17]
HTM+LSTM	[18]
RF-SMOTE	[19]
DNN	[21] [26] [36] [38]
ANN + Data framing + SD	[22]
HCRNNIDS	[23]
MFSLnO	[24]

SVM+KNN+DT+NB+RF+LR	[25]
SMOTE-DRNN	[27]
Deep Autoencoder	[28]
DDoSTC	[29]
DT+ RF+ KNN+ NB+ Stacking+ ANN	[30]
SVM+RF+KNN	[31]
SSA-ALO	[32]
ML-F	[33]
NB-EC BRTT	[34]
LUCID	[35]
FOCUS	[37]
CNN+QRNN	[39]
CNN	[40]
RF	[43]
RF+XG Boost	[44]
KNN	[46]
AMLSDM	[47]
KOAD+MD	[49]
LGBM	[50]

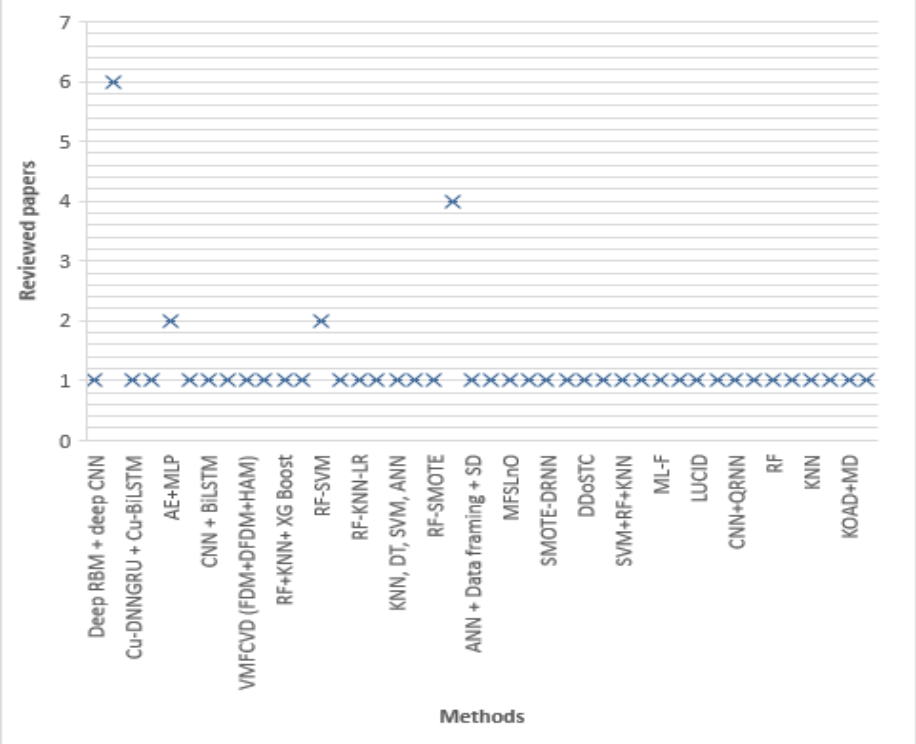


Figure 2. Chart analysis relying on the various methods

3.3 Analysis relying on the performance measures

Table 3 presents an examination of the diverse performance metrics assessed in various research studies. Accuracy, precision, recall, and the F1 score emerge as the foremost parameters essential for evaluating the effectiveness of DDoS attack detection within IoT communication networks. Among these metrics, accuracy takes precedence and is predominantly employed in 41 out of the 50 reviewed papers. Figure 3 provides a visual representation illustrating the analysis of the

reviewed papers with respect to the use of these performance measures.

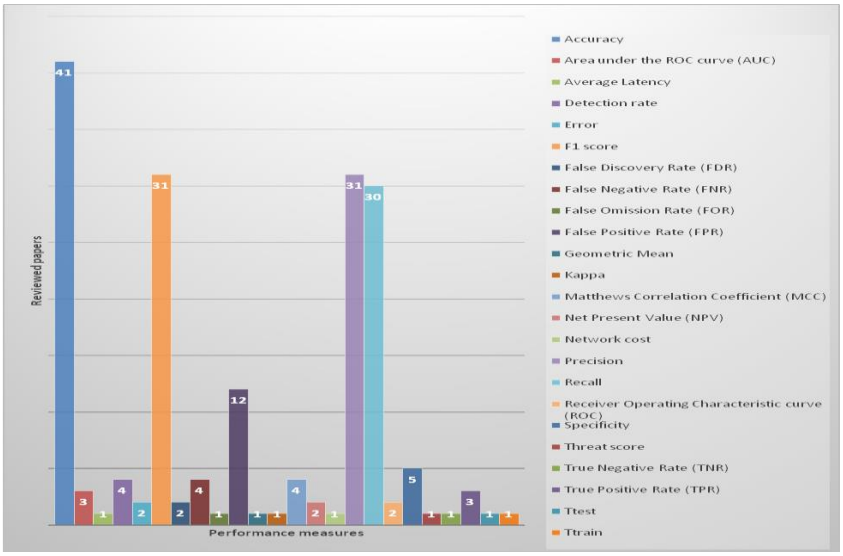


Figure 3. Chart analysis relying on the performance measures

Table 3. Performance measures

Measures	Reviewed papers
Accuracy	[1] [2] [3] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [21] [22] [23] [24] [25] [26] [27] [29] [30] [31] [33] [35] [36] [38] [39] [40] [41] [42] [44][45] [46] [47] [48] [49]
Recall	[3] [4] [6] [7] [8] [9] [10] [11] [12] [14] [16] [17] [18] [19] [20] [21] [24] [27] [28] [29] [31] [33] [35] [36] [38] [40] [41] [45] [47] [50]
Precision	[3] [4] [5] [6] [7] [8] [9] [10] [11] [14] [15] [17] [18] [19] [20] [21] [24] [27] [28] [29] [31] [33] [36] [38] [40] [41] [42] [43] [45] [47] [50]
F1 score	[3] [4] [6] [7] [8] [9] [10] [11] [13] [14] [15] [16] [17] [18] [19] [20] [21] [27] [28] [29] [31] [33] [35] [36] [38] [40] [41] [42] [45] [47] [50]
Error	[10] [15]
True Negative Rate (TNR)	[10]
Matthews Correlation Coefficient (MCC)	[10] [14] [16] [27]
Specificity	[12] [16] [17] [24] [42]
Detection rate	[13] [34] [42] [43]
False Positive Rate (FPR)	[14] [19] [22] [23] [24] [27] [32] [35] [39] [42] [43] [49]
False Negative Rate (FNR)	[14] [22] [24] [49]
Net Present Value (NPV)	[14] [27]
False Discovery Rate (FDR)	[14] [24]

Kappa	[16]
Threat score	[16]
Receiver Operating Characteristic curve (ROC)	[18] [46]
Area under the ROC curve (AUC)	[19] [27] [46]
False Omission Rate (FOR)	[24]
Geometric Mean	[27]
T_{train}	[27]
T_{test}	[27]
True Positive Rate (TPR)	[32] [35] [39]
Average Latency	[37]
Network cost	[37]

3.4 Analysis based on the achievements of the various methods in attack detection

Table 4 provides insights into the accomplishments showcased in the examined papers utilizing hybrid classifiers for DDoS attack detection within IoT. The achieved accuracy across these papers consistently exceeds the 85% threshold, while the precision of the hybrid classifiers remains consistently above 80%. Furthermore, the recall rates in the reviewed papers surpass 75%, and notably, the F1 score across all 50 reviewed papers consistently registers above 90%.

Table 4. Achievements of the various methods based on the measures

Hybrid classifiers	**Reviewed paper**	**Achievements (%)**			
		Accuracy	Precision	Recall	F1 score
Deep RBM + deep CNN	[1]	99.51	-	-	-
CNN + LSTM	[2]	96	-	-	-
Cu-DNNGRU + Cu-BiLSTM	[3]	99.87	99.87	99.96	99.96
CNN + LSTM	[4]	99.92	99.85	99.85	99.91
DBSCAN and PCA	[5]	-	99.9	-	-
AE+MLP	[6]	98.34	97.91	98.48	98.18
LSTM+GRU	[7]	99.98	99.97	99.98	99.97
CNN + BiLSTM	[8]	99.98	99.97	99.98	99.97
CNN + LSTM	[9]	90	94	91	88
DNN+KNN	[10]	99.77	99.74	99.76	99.75
VMFCVD (FDM+DFDM+HAM)	[11]	99.99	99.99	99.99	99.99
WILS-TRS	[12]	99.5	98.7	98.45	-
RF+KNN+ XG Boost	[13]	95.3	-	-	96.89
FAE-GWO-DBN	[14]	100	100	100	100
RF-SVM, RF-Naive Bayes-KNN, RF-KNN-LR	[15]	85.3	82.7	-	76.67
XGB-RF	[16]	99.94	99.94	99.94	99.94
KNN, DT, SVM, ANN	[17]	99.38	99.44	99.44	99.47
HTM+LSTM	[18]	97.74	97.20	97.92	97.72
RF-SMOTE	[19]	98.31	98.61	98.41	98.56
AE-MLP	[20]	-	100	100	100
DNN	[21]	99.97	99.99	99.98	99.98
ANN + Data framing + SD	[22]	99.405	-	-	-

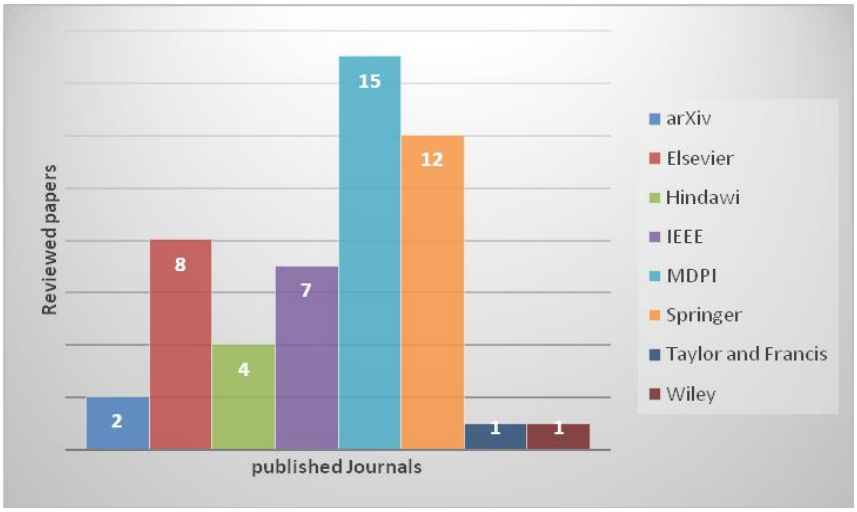
HCRNNIDS	[23]	97.75	-	-	--
MFSLnO	[24]	99	98	99	99
SVM, K-NN, DT, NB, RF and LR	[25]	99	-	-	-
DNN	[26]	97.25	-	-	-
SMOTE-DRNN	[27]	100	99.50	99.75	99.62
Deep Autoencoder	[28]	-	100	100	100
DDoSTC	[29]	99.82	99.88	99.92	99.96
DT+ RF+ KNN+ NB+ Stacking+ ANN	[30]	95.04	-	-	-
SVM+RF+KNN	[31]	98.68	98.28	97.38	98.01
ML-F	[33]	99.98	99.87	100	99.73
LUCID	[35]	99.67	-	99.39	89.59
DNN	[36]	99.93	99.08	96.97	97.96
DNN	[38]	91	95	83	88.10
CNN+QRNN	[39]	99.99	-	-	-
CNN	[40]	98	98	99	97
CNN+LSTM	[41]	99.7	99.67	99.68	99.67
RF-SVM	[42]	98.8	98.27	-	97.65
RF	[43]	-	99.90	-	-
RF+XG Boost	[44]	89.5	-	-	-
CNN+LSTM	[45]	100	100	100	100
KNN	[46]	99.6	-	-	-
AMLSDM	[47]	98.7	98.2	98	96
CNN+LSTM	[48]	94.80	-	-	-
KOAD+MD	[49]	82.2	-	-	-
LGBM	[50]	-	99.99	99.99	99.99

Analysis relying on the published journals

Table 5 presents an examination by the journals in which they were published. The analyzed papers find their homes in reputable journals, including IEEE, Springer, Elsevier, MDPI, Hindawi, arXiv, Wiley, Taylor and Francis. Our analysis highlights that Springer, IEEE, and MDPI are the most prolific publishers among the reviewed papers focused on DDoS attack detection within IoT, utilizing hybrid DL classifiers. For a visual representation of this analysis, Figure 5 depicts a chart showcasing the distribution of reviewed papers across these journals.

Table 5. Published journals

Published journals	Reviewed papers
IEEE	[1] [6] [35] [36] [40] [44] [49]
Springer	[5] [9] [11] [12] [13] [15] [19] [26] [30] [33] [34] [37]
Elsevier	[2] [10] [21] [24] [28] [38] [42] [48]
MDPI	[3] [7] [8] [16] [17] [20] [23] [25] [27] [29] [31] [32] [39] [41] [47]
Hindawi	[4] [18] [43] [45]
Taylor and Francis	[14]
arXiv	[22] [46]
Wiley	[50]



3.6 Research gaps in the detection of DDoS attack

The various challenges that evolved using the DL classifiers are analyzed as follows,

- The lengthy training timeframes, high computation cost, an enhanced requirement in size for testing and training, and increased complexity of the SVM model be the contributing factors to its poor performance [8]. The utilization of an appropriate kernel function in SVM to separate data is difficult and cannot be separated linearly [25].
- The RF model performs poorly for the following reasons, which consumes more time to make valid predictions, which is undependable for the attribute's categorization, and smaller, related groupings of comparable attributes are preferred over larger ones in the data [8].
- Since LR only produces brief forecasts and is susceptible to overfitting, which is rated as poor. LR may be eliminated, when there are fewer observations than the available features, otherwise, an overfitting issue may arise. A significant drawback of LR is the assumption of linearity between the independent as well as the dependent variables [8] [25].
- KNN is a low-ranking method because that takes a long time to process massive data sets and is susceptible to erroneous and noisy input [8].
- In the NB, the assumption class's conditional independence could lead to a loss of accuracy in which the premise of independence might not hold for a few attributes and the variables are practically dependent on one another [25].
- The multiple linear regression classifiers attain the worse outcomes and the performance is poor due to the presence of several factors [8].
- XG Boost attains poor performance since, which is tricky to adjust, requires a longer training period, and is prone to overfitting in the face of noisy data [8].

Conclusion

This comprehensive survey has delved into the realm of DDoS attack detection within IoT networks, with a particular focus on the utilization of various hybrid DL-based classifiers. In a landscape replete with diverse DL algorithms, the emergence of novel hybrid DL classifiers has drawn the attention of researchers. This analysis, encompassing research papers published from 2018 to 2022, sheds light on the efficacy of these hybrid classifiers in combatting DDoS attacks. One prominent finding of this analysis is the superior performance achieved by optimized classifiers when compared to their general hybrid counterparts, as evident in key performance metrics. This observation underscores the value of tailored, hybrid DL solutions in addressing the unique challenges posed by DDoS attacks within IoT networks. Furthermore, our examination has considered factors such as the publication journals, publication years, and the array of hybrid DL classifiers deployed, offering a holistic perspective on the landscape of DDoS attack detection research. These insights can guide future endeavors in refining and advancing DDoS detection methods. In closing, while the deployment of DL algorithms presents promise in enhancing IoT security, it is imperative to acknowledge the existing challenges associated with DDoS attack detection. As technology evolves, so too do the strategies employed by malicious actors. Therefore, ongoing research and innovation are essential to fortify IoT networks against the ever-evolving threat landscape.

References

[1] Elsaeidy, A.A., Jamalipour, A., and Munasinghe, K.S., "A Hybrid DL Approach for Replay and DDoS Attack Detection in a Smart City," IEEE Access, vol.9, pp.154864-154875, 2021.

[2] Sahu, A.K., Sharma, S., Tanveer, M., and Raja, R., "Internet of Things attack detection using hybrid DL Model," Computer Communications, vol.176, pp.146-154, 2021.

[3] Javeed, D., Gao, T., Khan, M.T., and Ahmad, I., "A hybrid DL-driven SDN enabled mechanism for secure communication in Internet of Things (IoT)," Sensors, vol.21, no.14, p.4884. 2021.

[4] Ullah, I., Raza, B., Ali, S., Abbasi, I.A., Baseer, S., and Irshad, A., "Software defined network enabled Fog-to-Things hybrid DL driven cyber threat detection system," Security and Communication Networks, 2021.

[5] Najafimehr, M., Zarifzadeh, S. and Mostafavi, S., "A hybrid machine learning approach for detecting unprecedented DDoS attacks," The Journal of Supercomputing, vol.78, no.6, pp.8106-8136, 2022.

[6] Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W. and Camtepe, S., "Ae-mlp: A hybrid DL approach for ddos detection and classification," IEEE Access, vol.9, pp.146810-146821, 2021.

[7] Ullah, S., Khan, M.A., Ahmad, J., Jamal, S.S., e Huma, Z., Hassan, M.T., Pitropakis, N. and Buchanan, W.J., "HDL-IDS: a hybrid DL architecture for intrusion detection in the Internet of Vehicles," Sensors, vol.22, no.4, pp.1340, 2022.

[8] Alghazzawi, D., Bamasag, O., Ullah, H. and Asghar, M.Z., "Efficient detection of DDoS attacks using a hybrid DL model with improved feature selection," Applied Sciences, vol.11, no.24, pp.11634, 2021.

[9] Alzahrani, M.Y. and Bamhdi, A.M., "Hybrid deep-learning model to detect botnet attacks over internet of things environments," Soft Computing, pp.1-15, 2022.

[10] de Souza, C.A., Westphall, C.B., Machado, R.B., Sobral, J.B.M. and dos Santos Vieira, G., "Hybrid approach to intrusion detection in fog-based IoT environments," Computer Networks, vol.180, pp.107417, 2020.

[11] Prasad, A. and Chandra, S., "VMFCVD: An Optimized Framework to Combat Volumetric DDoS Attacks using Machine Learning. Arabian Journal for Science and Engineering," pp.1-19, 2022.

[12] Jothi, B. and Pushpalatha, M., "WILS-TRS—A novel optimized DL-based intrusion detection framework for IoT networks," Personal and Ubiquitous Computing, pp.1-17, 2021.

[13] Kumar, P., Gupta, G.P. and Tripathi, R., "Toward design of an intelligent cyber-attack detection system using hybrid feature reduced approach for iot networks," Arabian

Journal for Science and Engineering, vol.46, no.4, pp.3749-3778, 2021.

[14] Sarma, S.K., "Hybrid optimised DL-deep belief network for attack detection in the internet of things," Journal of Experimental and Theoretical Artificial Intelligence, pp.1-30, 2021.

[15] Pandey, A., Thaseen, S., Kumar, A. and Li, G., "Identification of botnet attacks using hybrid machine learning models," In International Conference on Hybrid Intelligent Systems, Springer, Cham, pp. 249-257, 2019.

[16] Faysal, J.A., Mostafa, S.T., Tamanna, J.S., Mumenin, K.M., Arifin, M.M., Awal, M.A., Shome, A. and Mostafa, S.S., "XGB-RF: A hybrid machine learning approach for IoT intrusion detection," In Telecom, MDPI, vol.3, no.1, pp. 52-69, 2022.

[17] Tonkal, O., Polat, H., Basaran, E., Comert, Z. and Kocaoglu, R., "Machine learning approach equipped with neighbourhood component analysis for DDoS attack detection in software-defined networking," Electronics, vol.10, no.11, pp.1227, 2021.

[18] Xinlong, L. and Zhibin, C., "DDoS Attack Detection by Hybrid DL Methodologies," Security and Communication Networks, 2022.

[19] Karthik, M.G. and Krishnan, M.B., "Hybrid random forest and synthetic minority over sampling technique for detecting internet of things attacks," Journal of Ambient Intelligence and Humanized Computing, pp.1-11, 2021.

[20] Liu, T., Sabrina, F., Jang-Jaccard, J., Xu, W. and Wei, Y., "Artificial Intelligence-Enabled DDoS Detection for Blockchain-Based Smart Transport Systems," Sensors, vol.22, 1, pp.32, 2021.

[21] Cil, A.E., Yildiz, K. and Buldu, A., "Detection of DDoS attacks with feed forward based deep neural network model," Expert Systems with Applications, vol.169, pp.114520, 2021.

[22] Machaka, P., Ajayi, O., Maluleke, H., Kahenga, F., Bagula, A. and Kyamakya, K., "Modelling DDoS Attacks in IoT Networks using Machine Learning," 2021.

[23] Khan, M.A., "HCRNNIDS: hybrid convolutional recurrent neural network-based network intrusion detection system," Processes, vol.9, no.5, pp.834, 2021.

[24] Reddy, S. and Shyam, G.K., "A machine learning based attack detection and mitigation using a secure SaaS framework," Journal of King Saud University-Computer and Information Sciences, 2020.

[25] Alzahrani, R.J. and Alzahrani, A., "Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. Electronics," vol.10, no.23, pp.2919, 2021.

[26] Makuvaza, A., Jat, D.S. and Gamundani, A.M., "Deep neural network (DNN) solution for real-time detection of distributed denial of service (DDoS) attacks in software defined networks (SDNs)," SN Computer Science, vol.2, no.2, pp.1-10, 2021.

[27] Popoola, S.I., Adebisi, B., Ande, R., Hammoudeh, M., Anoh, K. and Atayero, A.A., "smote-drnn: A DL algorithm for botnet detection in the internet-of-things networks," Sensors, vol.21, no.9, pp.2985, 2021.

[28] Niraja, K.S. and Rao, S.S., "A hybrid algorithm design for near real time detection cyber-attacks from compromised devices to enhance IoT security," Materials Today: Proceedings, 2021.

[29] Wang, H. and Li, W., "DDosTC: A transformer-based network attack detection hybrid mechanism in SDN," Sensors, vol.21, no.15, pp.5047. 2021.

[30] Kumar, P., Bagga, H., Netam, B.S. and Uduthalapally, V., "Sad-iot: Security analysis of ddos attacks in iot networks," Wireless Personal Communications, vol.122, no.1, pp.87-108, 2022.

[31] Islam, U., Muhammad, A., Mansoor, R., Hossain, M.S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U. and Shafiq, M., "Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models," Sustainability, vol.14, no.14, pp.8374, 2022.

[32] Abu Khurma, R., Almomani, I. and Aljarah, I., "Iot botnet detection using salp swarm and ant lion hybrid optimization model," Symmetry, vol.13, no.8, pp.1377, 2021.

[33] Krishna, E.S. and Thangavelu, A., "Attack detection in IoT devices using hybrid metaheuristic lion optimization algorithm and firefly optimization algorithm," International Journal of System Assurance Engineering and Management, pp.1-14, 2021.

[34] Lakshmi Narayanan, K., Santhana Krishnan, R., Golden Julie, E., Harold Robinson, Y. and Shanmuganathan, V., "Machine learning based detection and a novel EC-BRTT algorithm-based prevention of DoS attacks in wireless sensor networks," Wireless Personal Communications, pp.1-25, 2021.

[35] Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J. and Siracusa, D., "LUCID: A practical, lightweight DL solution for DDoS attack detection," IEEE Transactions on Network and Service Management, vol.17, no.2, pp.876-889, 2020.

[36] Popoola, S.I., Ande, R., Adebisi, B., Gui, G., Hammoudeh, M. and Jogunola, O., "Federated DL for zero-day botnet attack detection in IoT-edge devices," IEEE Internet of Things Journal, vol.9, no.5, pp.3930-3944, 2021.

[37] Maharaja, R., Iyer, P. and Ye, Z., "A hybrid fog-cloud approach for securing the Internet of Things," Cluster Computing, vol.23, no.2, pp.451-459, 2020.

[38] Ujjan, R.M.A., Pervez, Z., Dahal, K., Bashir, A.K., Mumtaz, R. and González, J., "Towards sFlow and adaptive polling sampling for DL-based DDoS detection in SDN," Future Generation Computer Systems, vol.111, pp.763-779.

[39] Al-Taleb, N. and Saqib, N.A., "Towards a Hybrid Machine Learning Model for Intelligent Cyber Threat Identification in Smart City Environments," Applied Sciences, vol.12, no.4, pp.1863, 2022.

[40] Wang, J., Liu, Y., Su, W. and Feng, H., "A DDoS attack detection based on DL in software-defined Internet of things," In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), IEEE, pp. 1-5, 2020.

[41] Wazzan, M., Algazzawi, D., Albeshri, A., Hasan, S., Rabie, O. and Asghar, M.Z., "Cross DL Method for Effectively Detecting the Propagation of IoT Botnet," Sensors, vol.22, no.10, pp.3895, 2022.

[42] Ahuja, N., Singal, G., Mukhopadhyay, D. and Kumar, N., "Automated DDOS attack detection in software defined networking," Journal of Network and Computer Applications, vol.187, pp.103108, 2021.

[43] Lima Filho, F.S.D., Silveira, F.A., de Medeiros Brito Junior, A., Vargas-Solar, G. and Silveira, L.F., "Smart detection: an online approach for DoS/DDoS attack detection using machine learning," Security and Communication Networks, 2019.

[44] Mohmand, M.I., Hussain, H., Khan, A.A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I.U. and Haleem, M., "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," IEEE Access, vol.10, pp.21443-21454, 2022.

[45] Alkahtani, H. and Aldhyani, T.H., "Botnet attack detection by using CNN-LSTM model for Internet of Things applications," Security and Communication Networks, 2021.

[46] Pokhrel, S., Abbas, R. and Aryal, B., "IoT security: botnet detection in IoT using machine learning," arXiv preprint, 2021.

[47] Aslam, M., Ye, D., Tariq, A., Asad, M., Hanif, M., Ndzi, D., Chelloug, S.A., Elaziz, M.A., Al-Qaness, M.A. and Jilani, S.F., "Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT," Sensors, vol.22, no.7, pp.2697, 2022.

[48] Parra, G.D.L.T., Rad, P., Choo, K.K.R. and Beebe, N., "Detecting Internet of Things attacks using distributed DL," Journal of Network and Computer Applications, vol.163, pp.102662, 2020.

[49] Daneshgadeh, S., Kemmerich, T., Ahmed, T. and Baykal, N., "A hybrid approach to detect DDoS attacks using KOAD and the Mahalanobis distance," In 2018 IEEE 17th International Symposium on Network

Computing and Applications (NCA), IEEE, pp. 1-5, 2018.

[50] Marvi, M., Arfeen, A. and Uddin, R., "A generalized machine learning-based model for the detection of DDoS attacks," International Journal of Network Management, vol.31, no.6, pp.2152. 2021.

[51] L. Da Xu, W. He, and S. Li, ''Internet of Things in industries: A survey,'' IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[52] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, ''Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare,'' Future Generat. Comput. Syst., vol. 78, pp. 659–676, Jan. 2018.

[53] H. Kumar, M. K. Singh, M. P. Gupta, and J. Madaan, ''Moving towards smart cities: Solutions that lead to the smart city transformation framework,'' Technol. Forecasting Social Change, vol. 153, Apr. 2020, Art. no. 119281.

[54] de Assis, M.V.O.; Carvalho, L.F.; Rodrigues, J.J.P.C.; Lloret, J.; Proença, M.L., Jr. Near real-time security system applied to SDN environments in IoT networks using convolutional neural network. Comput. Electr. Eng. 2020, 86, 106738.

[55] Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access 2020, 8, 77396–77404.

[56] Rehman Javed, A.; Jalil, Z.; Atif Moqurrab, S.; Abbas, S.; Liu, X. Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles. Trans. Emerg. Telecommun. Technol. 2020.

[57] Perez, M.G.; Celdran, A.H.; Ippoliti, F.; Giardina, P.G.; Bernini, G.; Alaez, R.M.; Chirivella Perez, E.; Clemente, F.J.G.; Perez, G.M.; Kraja, E.; *et al*. Dynamic Reconfiguration in 5G Mobile Networks to Proactively Detect and Mitigate Botnets. IEEE Internet Comput. 2017, 21, 28–36.

[58] Anthi E, Javed A, Rana O, Theodorakopoulos G (2017) Secure data sharing and analysis in cloud-based energy management systems. In Cloud Infrastructures, Services, and IoT Systems for Smart Cities, pages 228–242. Springer

[59] J. Mirkovic and P. Reiher, ''A taxonomy of DDoS attack and DDoS defense mechanisms,'' ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, Apr. 2004.

[60] Shukla P (2017) Ml-ids: a machine learning approach to detect wormhole attacks in Internet of things. In Intelligent Systems Conference (IntelliSys), 2017, pages 234–240. IEEE

[61] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, ''Intrusion detection systems for IoT-based smart environments: A survey,'' J. Cloud Comput., vol. 7, no. 1, p. 21, Dec. 2018.

[62] S. Ho, S. A. Jufout, K. Dajani, and M. Mozumdar, ''A novel intrusion detection model for detecting known and innovative cyberattacks using convolutional neural network,'' IEEE Open J. Comput. Soc., vol. 2, pp. 14–25, 2021.