Mesopotamian journal of Cybersecurity
Vol.4,No.3, **pp**. 59–74
DOI: https://doi.org/10.58496/MJCS/2024/016; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Hybrid Classifier for Detecting Zero-Day Attacks on IoT Networks

Rana M. Zaki [1,*], Inam S. Naser [1]

[1] *Department of Computer Science, University of Technology, Baghdad, Iraq*

ARTICLE INFO

Article history

Received 13 Jul 2024
Accepted 12 Oct 2024
Published 02 Nov 2024

Keywords

Hybrid classifier

Zero-day

Ensemble machine learning

XGBoost Classifier

IoT

ABSTRACT

Recently, Internet of Things (IoT) networks have been exposed to many electronic attacks, giving rise to concerns about the security of these networks, where their weaknesses and gaps can be exploited to access or steal data. These networks are threatened by several cyberattacks, one of which is the zero-day distributed denial-of-service (DDoS) attack, which is considered one of the dangerous attacks targeting network security. As such, it is necessary to find smart solutions to address such attacks swiftly. To address these attacks, this research proposed a hybrid IDS to detect cyber-attacks on IoT networks via machine learning (ML) algorithms, namely, XGBoost, K-nearest neighbors, and stochastic gradient descent (SGD), while classifiers are combined via an ML ensemble. Grid search CV was used to find the best hyperparameters for each classifier at each classification stage. Random projection was used to select the relevant features for training the model. In the evaluation and performance testing phase of the model, two cybersecurity datasets (CIC-IDS2017 and CIC-DDoS2019) were used to test the efficiency of the model in detecting zero-day threats. The best results were obtained for the CIC-DDoS2019 dataset, where 20 features out of the total selection were used. The model was able to achieve an accuracy of 99.91% and an intrusion detection time of 0.22 seconds. The confusion matrix results also revealed a reduction in false alarms. The results and their comparison with those of recent relevant studies demonstrated the effectiveness of the hybrid model in securing IoT networks from zero-day attacks as well as its superiority in terms of accuracy and intrusion detection time. This study is an important step in enhancing security in the IoT environment by presenting a new hybrid model that is capable of dealing with zero-day attacks that are difficult to detect with traditional models.

1. INTRODUCTION

Many intrusion detection systems (IDSs) have been proposed in recent years. With the progress achieved by attackers in finding weak points for exploitation, zero-day distributed denial-of-service (DDoS) attacks are often hidden from IDSs, which has prompted researchers to delve into the field of IDSs and intrusion treatments via machine learning (ML) techniques and artificial intelligence to control such attacks [1, 2]. A DDoS attack is currently one of the most common attacks, as many requests are made to targeted networks by exploiting existing vulnerabilities, thus blocking services from such networks and making them unavailable to real users. Attackers can create many fake networks to attack victims or networks, leading to reflections or amplification and the cutting-off of services [3]. Zero-day threats are vulnerabilities or flaws found in systems, internet networks, or Internet of Things (IOT) networks that are exploited by attackers [4]. They differ from viruses or other hacks because the programmer does not know about them until after the hack. Hence, the role of an IDS is to defend networks from such threats before they occur [5-7]. Intrusion detection systems (IDSs) rely on ML and deep learning algorithms [8]. Their function is to monitor traffic for any abnormal or harmful activities within the network [9, 10]. They are expected to examine the packets and data entering the network and determine whether they contain malicious traffic or normal traffic[11]. They are trained viaML algorithms to detect hacking attempts [12]. ML is a modern technique that is used to train systems to improve their performance via real data from attacks that have already occurred. The most important techniques are classification and clustering[13]. The process of implementing ML algorithms consumes considerable energy in training and intrusion detection; hence, the reduction and selection of features are taken into consideration to help reduce energy consumption and increase the speed of training and detection [14]. Feature selection is a technique that analyses features and selects those features that are relevant for the selected topic. The selection and reduction of features help to create a good classifier in terms of training and contribute to lowering the training speed by reducing the overload, thus contributing to a reduction in energy consumption and training time for the

*Corresponding author. Email: Rana.M.Zaki@uotechnology.edu.iq

model, which are important factors[15]. This technique has become indispensable in data preprocessing. Owing to the increase in real data, many algorithms are available for feature selection, and the algorithm is selected on the basis of its need and strength in influencing the model [16]. Intrusion detection systems (IDSs) face many challenges in the field of the IoT [17], including the choice of appropriate algorithms and avoidance of computational complexity due to the lack of resources in IoT devices and the speed of detection in real time due to the sensitivity of IoT data. Another challenge is the selection of data to train the model, as it represents a pivotal stage[18]. Since training the model depends on the nature of the data used, data with real traffic must be chosen to help train the model well [19]. Another factor that helps in the effectiveness of the model is the selection of only relevant features, which directly affects the speed of training the model and avoids overtraining, which can have a negative impact on the results of the model [20]. Zero-day attacks are among the greatest challenges facing IoT networks, where unintended security vulnerabilities in programs are used to access and harm devices and data [4]. As such, attacks are difficult to detect in traditional models; therefore, hybrid and multi technical models must be used to protect IoT networks from them [21].

The main problems addressed in this paper were how to design an IDS and protect IoT networks from zero-day attacks, hence overcoming the challenges and limitations found in previous works. The goal of this study was to design an advanced model to detect zero-day threats on IoT networks via datasets with real traffic to train the model and make a comparison with existing studies to prove the effectiveness of the model.

The sparse random projection algorithm was used to select the relevant features with the fewest possible numbers. At the training level of the model, the ML classifiers XGBoost, K-nearest neighbors, and stochastic gradient descent (SGD) were used. To improve the performance of the algorithms, GridSearchCV is used to find the best parameters for each stage of the work. The performance of the model was evaluated on the CIC-IDS2017 and CIC-DDoS2019 datasets to prove the accuracy of the proposed IDS for zero-day attacks, as well as the time spent on training and intrusion detection. This methodology helps improve the ability of intrusion detection systems to detect threats on IoT devices and networks.

The contributions of this paper are presented below:

1. A hybrid model for monitoring network traffic and detecting zero-day threats on IoT networks is proposed.

2. The features used in training the model are reduced, and only the relevant features are selected via the sparse random projection technique.

3. The ensemble classifier comprising the ML algorithms, XGBoost K-nearest neighbors, and SGD was used, and the best hyperparameters were used for each algorithm and level.

The performance of the model was evaluated on the CIC-IDS2017 and CIC-DDoS2019 datasets, and the accuracy, training time, detection time, and false and true alarm rates of the model were calculated. This hybrid methodology can be used in IoT applications, including in smart homes and in the field of medical devices.

The rest of this paper is organized as follows:

Section 2 provides an explanation of previous works related to IDSs, while Section 3 provides a detailed explanation of the techniques used in IDSs. In Section 4, a detailed presentation of the hybrid methodology employed to create the hybrid model is provided. The performance evaluation results of the hybrid model are presented in Section 5 together with a comparison with previous works and challenges. Finally, Section 6 presents the conclusion and recommendations for future work.

2. LITERATURE REVIEW

[22] proposed a deep learning system for detecting DDoS attacks and used an additive tree classification algorithm to identify features, of which 20 features were selected. The models were designed with the RNN, LSTM, and GRU algorithms, and a careful comparison was made by testing them with the CIC-IDS2017 and CIC-DDoS2019 datasets. The accuracy and detection times were not at the desired levels, and these were to be overcome in the current study.

[23] proposed a DL-2p-DDoS deep learning model to detect DoS threats. First, an autoencoder was used, and then, the results were compared with those obtained by the DNN, LSTM, and GRU algorithms. The model had accuracies of 97% and 96% when applied to the CIC-DDoS2019 and DDoS-AT-2022 datasets, respectively. Its computational complexity has a negative effect on its generalizability to other environments. This would be overcome in the current study.

[24] proposed a model for detecting DDoS attacks in cloud environments by using ML algorithms such as NB, LR, RF, andXGBoost. The CIC-IDS2017 dataset was used to evaluate the performance of the model. The best precision was obtained with the XGBoost algorithm (99.11%). As the model was trained and tested on only one dataset, it could not be generalized. In the present study, more than one dataset was used.

[25] proposed a model to detect attacks on IoT networks by using ResNet, transformer, and BiLSTM (Res-TranBiLSTM) as well as SMOTE to identify features. The performance of the model was based on the NSL-KDD, CIC-IDS2017, and MQTT datasets, where accuracies of 90.99%, 99.15%, and 99.56%, respectively, were obtained. The results of the model obtained with the old datasets were lower than the results obtained with the recent dataset. It is assumed that only a modern dataset with real traffic was used, and there was also some complexity in the work. In the present study, modern datasets with real traffic data were used.

[12] proposed a supervised zero-day threat detection system. To identify the landmarks, they used the Gaussian random projection technique and K-means, SVM, and Gaussian mixed model algorithms to design the model. An accuracy of 94.55% was achieved when the model was applied to the CIC-DDoS2019 dataset. The challenges related to the use of more than one dataset were not overcome. To prove the efficiency of the model in generalization and adaptation, these challenges were overcome in the current study. In [26], the authors propose a model to secure IoT networks from zero-day attacks on the basis of the ensemble mean weighted probability. The results were 99.54% and 99.33% after using the IoTID2020 and CICIoT2023 datasets, respectively. Although the results of the study are good, relevant feature selection techniques were not used. This can lead to overtraining and increased training time. This has been overcome in our work by selecting and reducing the number of features used.

[27] proposed a model to secure IoT networks from zero-day attacks on the basis of the ensemble mean weighted probability. Accuracies of 99.54% and 99.33% were attained after using the IoTID2020 and CICIoT2023 datasets, respectively. Although the results of the study were good, relevant feature selection techniques were not used, which can lead to overtraining and increased training time. In the present study, the number of features used was selected and reduced.

In Table I, a comparison of existing studies, which included creating and improving intrusion detection systems in IoT environments via several machine learning and deep learning algorithms, is presented. Each study is explained, which depends on several criteria, namely, the type of algorithm used, the feature selection technique, the dataset used in training, and finally, the limitations presented in each study. This facilitates comparisons between current methods.

TABLE I. COMPARISON OF RELATED STUDIES

Ref	Year	Algorithm	Feature selection	Dataset	limitation
[22]	2023	RNN, LSTM, and GRU	classifier decision tree	CIC-DDoS2019 CICIDS2017	The proposed model is good in terms of results and feature selection, but the time taken is significant for intrusion detection systems. This is considered a weak point.
[23]	2023	Auto Encoder	-	CICDDoS2019 DDoS-AT-2022	The results were unsatisfactory, and, in our opinion, the reason is due to the way the features were selected.
[24]	2023	NB, LR, RF, XGBoost	Extra Tree classifier	CICIDS2017	The results of the proposed model are not satisfactory, and the reason is up to our knowledge to be in the method of selecting features and in the use of only one classifier.
[25]	2023	ResNet, Transformer, and BiLSTM (Res-TranBiLSTM)	reshape the 1D features into 2D features	NSL-KDD ,CIC-IDS2017 and MQTT	The results show that the accuracy of the model is not considered high, and the reason is believed to be the complex feature selection process.
[12]	2024	K-means, GMM, and one-class SVM	random projection	CIC-DDoS2019	For feature selection, they used Gaussian random projection algorithm and selected 25 features, but the model accuracy results were unsatisfactory.
[26]	2024	weighted probability averaging ensemble	Information gain	IoTID20 and CICIoT2023	The way to select features is not clear, and all features are used after filtering.
[27]	2024	Logistic Regression, Random Forest, Decision Tree, and XGBoost	-	CIC-DDoS2019	The results were not sufficientcompared to other work, despite the use of machine learning algorithms. The reason, in our opinion, is the feature selection process, as all features were worked on.

3. BACKGROUND

This section explains zero-day attacks and the requirements for the hybrid threat detection model.

3.1 Zero-Day Attacks

A zero-day attack is one of the most common cyberattacks and threats to data security today. It exploits unintended and undetected loopholes or weak points in internet networks, systems, or IoT networks [28]. Notably, such attacks are difficult to detect with firewalls and difficult to predict and discover, as they are unknown or are identified only after the infiltration and repair of weak points [29].

3.2 Intrusion Detection System (IDSs) for Zero-Day Attacks

Intrusion detection systems (IDSs) are systems that use ML and prior learning to predict and evaluate normal or abnormal traffic within a network [30]. One of the challenges facing IDSs is identifying developments that occur in attacks. Therefore, the systems are trained on up-to-date data on an ongoing basis to enable them to identify threats [31]. An intrusion detection system (IDS) is considered an important part of network security because it provides complete protection to a network and devices connected to the network and protects existing weak points. Many systems have been designed using ML and deep learning techniques [32, 33].

3.3 Machine Learning Algorithms

These algorithms learn on their own and adapt according to the available data. They can provide outputs on the basis of what they learn from the data, which allows the device to perform certain tasks when abnormal traffic is discovered. They can also automatically analyse threats and efficiently evaluate traffic [34]. One of the main things involved in ML is data mining, which is the discovery of knowledge, where the data are analysed well, thus helping to increase the accuracy of predictions [35-38].

The XGBoost classifier is a supervised ML algorithm. Its work, which is mostly based on decision tree algorithms, involves creating a forecast model that combines the individual decisions of the models. It is considered to be one of the most accurate prediction algorithms. One of the strengths of this algorithm is its ability to handle data composed of noise and outliers [39]. The algorithm balances and optimizes memory buffers. One of the techniques used in this algorithm is lasso and ridge regression, which handle complexity well [40], where it learns from the results of previous trees and produces results (Figure 1).

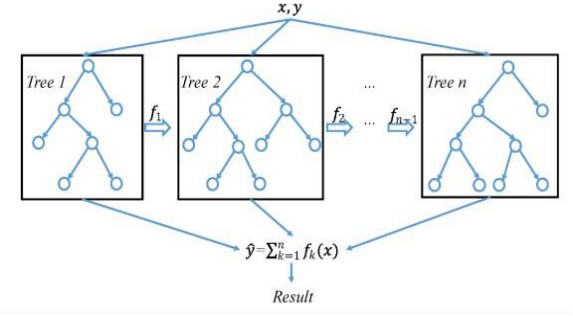

Fig. 1. XGBoost classifier[41]

$$Yi = n\sum k = 1 \int k(xi), \quad \int k \in F, \tag{1}$$

F represents the regression trees, ∫ k represents the fit between the decision trees, and ∫ k(xi), represents the result of the k-tree.

yi is the prediction result of xi.

The K-nearest neighbor classifier is a supervised learning algorithm that is widely used because of its ease of handling. It uses points close to a collection of individual data, obtains predictions, uses classification and regression techniques, and performs parallel operations [42].

$$D = \sqrt{(x_a - x_b)^2 + (y_a - y_b)^2} \quad (2)$$

$(x_a - x_b)$ is the horizontal distance a.

$(y_a - y_b)$ is the horizontal distance a.

The stochastic gradient descent (SGD) classifier is a supervised ML algorithm that is considered one of the most effective techniques for making the right decisions. It calculates the decision boundaries or the best decision to differentiate the distance of points from each other in the data with different categories of features by using the loss function [43, 44].

$$(\circledcirc) = \frac{1}{n} \sum_{i=1}^{n} L(yi, \int(x)) + \alpha R(w) \quad (3)$$

L: This measures the fit of the model.

R: The penalty is the complexity of the model

α: It is a nonnegative parameter

Ensemble ML is an ML technique that combines or stacks classification models, where more than one model or algorithm can be used for classification, and it collects or takes advantage of the decisions resulting from these models and produces a final decision. One of its advantages is that it provides highly accurate classifications or predictions [45].

3.4 Feature Selection, Sparse Random Projection

Feature selection is essential in designing a good model and occurs after the data have been pre-processed to obtain high-quality data. Relevant features are selected to help increase the accuracy of the model [46]. Random projection is a feature selection technique that is effective and easy to use, reduces linear dimensions and helps maintain a high level of probability, thus speeding up operations [47]. Sparse random projection, which is a random matrix, helps increase quality and memory power and contributes to increasing the speed of computational operations. It also speeds up data projection [48, 49]. The elements of the matrix are as follows:

Our definition is s = 1/density

$$\begin{cases} -\sqrt{\frac{s}{n_{components}}} & 1/2s \\ 0 \quad \text{with probability} & 1 - 1/s \\ +\sqrt{\frac{s}{n_{components}}} & 1/2s \end{cases} \quad (4)$$

s is the square of the original dimension of n.

$n_{components}$ The amount of subspace expected

where the density was set to the default value, which is the minimum recommended density.

3.5 Dataset

CIC_DDoS2019 is a recent dataset provided by the Canadian Cyber Security Institute. This dataset is a powerful addition to cybersecurity, which makes it good for designing IDSs. It is composed of real data and simulations of real attacks. It is divided into seven categories and contains 88 features of normal data traffic and DDoS attack scenarios [50]. The data focus on DDoS attacks, one of the most common attacks currently in IoT networks, whereby the networks are overwhelmed with a very large number of requests. This dataset helps train models to evaluate traffic within a network and protect it from threats [51]. The CIC-IDS2017 dataset is one of the most famous collections of data in the cyber field [52]. It contains real traffic and includes a group of attacks: DDoS, brute force, DoS, and infiltration [53]. It consists of 84 features and covers many statistics related to protocols in communication networks [54-56].

4. METHODOLOGY

The hybrid model for detecting zero-day DDoS threats was presented with a data preprocessing method using several data analysis techniques. The relevant and appropriate features were selected via the sparse random projection technique.

The hybrid model, consisting of three ML algorithms, namely, XGBoost, K-nearest neighbors, and SGD, was subsequently created. The results of the two classifiers were combined with the results of the third classifier via the ensemble stacking technique to produce the hybrid classifier. Figure 2 provides a detailed explanation of the hybrid model.

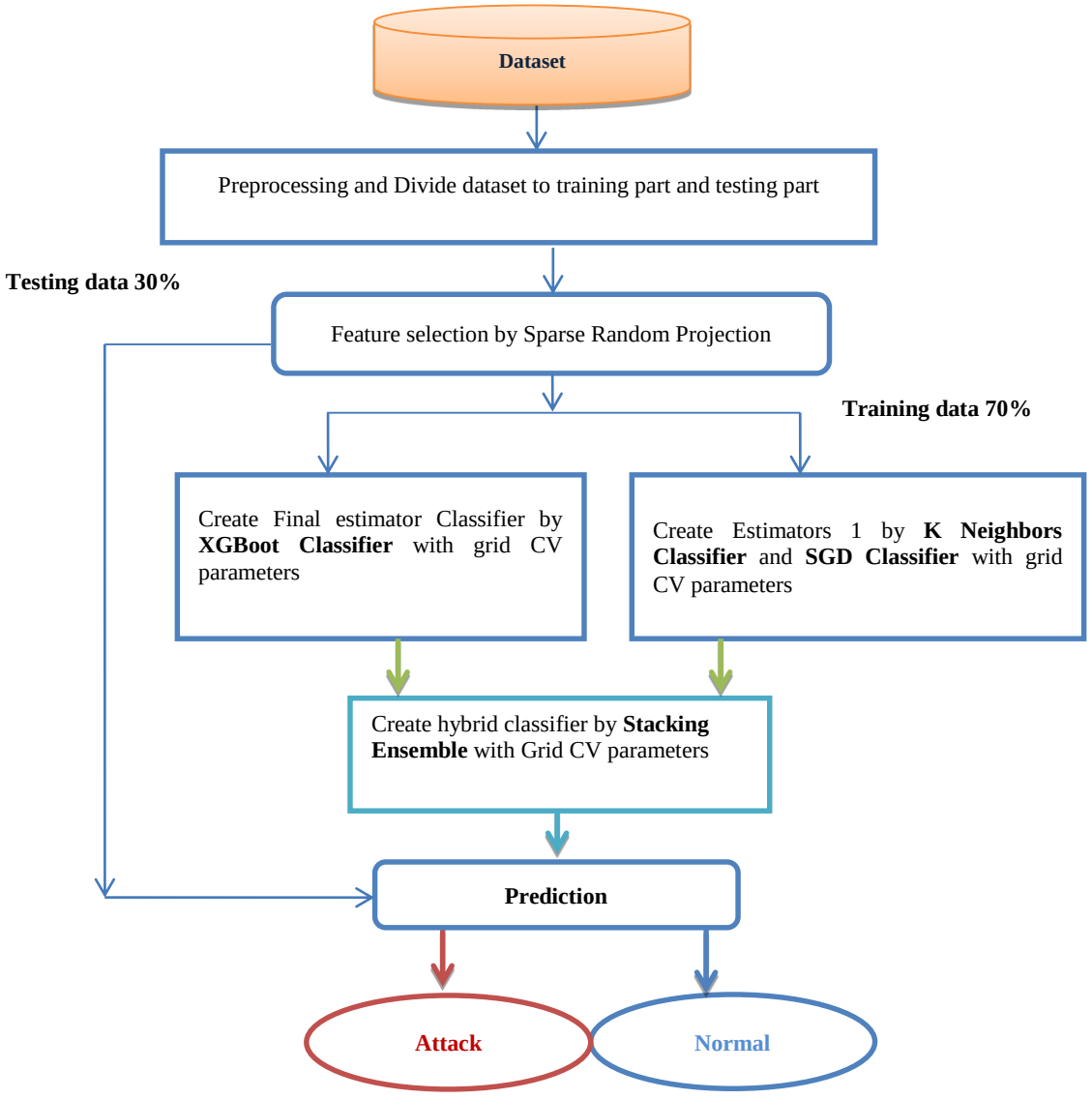

Fig. 2. Proposed hybrid classifier

In this work, two datasets were used, namely, CIC-IDS2017 and CIC_DDoS2019. They simulate data traffic within a network that contains DDoS attacks and normal data. The goal of applying these datasets was to test and evaluate the performance of the hybrid model and to determine the accuracy of the model in detecting attacks and reducing false alarms. Two datasets were used, namely, CIC-IDS2017 and CIC_DDoS2019. They simulate data traffic within a network that contains DDoS attacks and normal data. The goal of applying these datasets was to test and evaluate the performance of the hybrid model and to determine the accuracy of the model in detecting attacks and reducing false alarms.

The preprocessing process was carried out as shown in Figure 2 and as follows:

First, the data were inserted to begin preprocessing. Second, outliers were detected and processed [np.inf, -np.inf], and null data were deleted. Third, the data were randomly divided into training data and test data (70%–30%). Fourth, standard scaling was used to make the data more consistent. In the fifth stage, the standard deviation was calculated to ensure the variance and regularity of the data. Finally, one of the very important stages was feature selection, where relevant features were identified and reduced via the sparse random projection technique to help speed up model training.

$$\text{Scale} = (x - m) \setminus s \tag{5}$$

s= the standard deviation, m = the mean.

In the fifth stage, the standard deviation is calculated to ensure the variance and regularity of the data.

$$SD = \sqrt{\frac{\sum(X-U)^2}{N}} \tag{6}$$

X= the value, U = the mean value, N= the number of points.

Finally, one of the very important stages is feature selection, where relevant features are identified and reduced to help speed up model training, and the sparse random projection technique is used.

4.1 Training the Hybrid Classifier

After completing the data processing and preparing and selecting only the relevant features, the hybrid model was created from the three classifiers, namely, XGBoost, K-nearest neighbors, and SGD. Through the use of ensemble stacking and adoption of the best hyperparameters for each stage, Grid Search CV was employed to produce the hybrid classifier.

The first estimator was created through the K-nearest neighbors and SGD classifiers, and the best Grid Search CV parameters were chosen for each algorithm. The outputs of this stage were used as the inputs for the hybrid classifier (Algorithm 1).

Algorithm 1. The first Estimator Classification
Input: K-neighbors , SGD ***Output: The first estimators trainer***
Begin - Training the first classifier (K-neighbors) on data. With best parameter (‘algorithm: kd_tree’, ‘n_jobs: -1’, ‘n_neighbors: 4’, ‘weights: distance’). - Training the second classifier (SGD) on data. With best parameter (‘loss=hinge’, ‘alpha=0.0001’,’ max_iter=1000’, ‘shuffle=True’, ‘verbose=0’,’ class_weight=None’). - Enter the outputs of the first classifier and the second classifier into the first estimator. - Return first estimators trainer - End.

Next, the original XGBoost classifier was trained on the training data using the best parameters. The outputs of this classifier were the inputs for the hybrid classifier (Algorithm 2).

Algorithm 2. Training XGBoot Classifier
Input: XGBoot classifier ***Output: XGBoot classifier trainer***
- Begin

- Training the XGBoot classifer on data. With best parameter (‘n_estimators:80’,’random_state:42’).
- Return XGBoot classifier trainer
- End.

Finally, the hybrid classifier was created via ensemble stacking of the classifiers. This was dependent on the outputs of the first trained estimator and the outputs of the trained XGBoost classifier, as well as the choice of the best Grid Search CV pair, and the hybrid classifier trained to detect attacks (Algorithm 3).

Algorithm 3. Created Hybrid Classifier

Input: ***The first estimators trainer, Training XGBoot classifier***
Output: ***the hybrid classifier***

Begin

1- input the first estimators into ensemble stacking
2- Input the XGBoot classifier into ensemble stacking.
3- Building the hybrid classifier by ensemble stacking.
4- Training the hybrid classifier on data. With best parameter (‘bootstrap: True’,’class_weight: balance’, ‘riterion: gini, ‘max_depth: None’, ‘max_features: sqrt’, ‘max_leaf_nodes: 10’, ‘min_samples_leaf: 1’, ‘min_samples_split: 2’,’n_estimators: 80’).
5- Return hybrid classifier trainer

4.2 Testing the Hybrid Classifier

In the testing phase, the hybrid model was tested on the previously processed datasets and on the same features that were identified. The aim was to determine the ability of the model to make appropriate decisions and its accuracy in detecting attacks. A confusion matrix was constructed, and through it, the accuracy, error rate, recall, and detection rate were calculated. The time taken by the model to train and detect attacks was also calculated.

5. EXPERIMENT DETAILA AND RESULTS

The performance of the hybrid model in detecting zero-day threats on IoT and internet networks was evaluated. At the beginning of the research, the data were pre-processed, and then important and relevant features were selected via sparse random projection. Then, a hybrid model was designed using XGBoost, K-nearest neighbors and SGD, with separate parameters for each algorithm. A confusion matrix was used to calculate the accuracy and error rate of the model. The following workspace was used to test the model: Windows 11 operating system (64-bit), EVO i7-1185 g processor, frequency 3.0. 16 GB of access memory, and Python 3.10.4.

Two datasets were used to evaluate the performance of the hybrid model, namely, the CIC-IDS2017 Friday Working Hours Afternoon DDoS and CIC-DDoS2019 datasets. They contained samples of traffic from zero-day DDoS attacks. The CIC-IDS2017 dataset had 79 features and a total of 225745 records, of which the top 25 features were selected. The data were divided into 156157 training data records and 66925 test data records. The CIC-DDoS2019 dataset had 88 features and a total of 162590 records, of which the top 20 features were selected. The data were divided into 110729 training data records and 47456 test data records. The confusion matrix was used to compute the accuracy, detection rate, precision, recall, F score, and detection time.

$$\text{Accuracy (Acc)} = \frac{\text{TN+TP}}{\text{All(TP+TN+FP+FN)}} \tag{7}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{8}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \tag{8}$$

$$\text{Recall or DR} = \frac{\text{TP}}{\text{TP+FN}} \tag{9}$$

$$\text{F} = \frac{2*\text{Precision}*\text{Recall}}{\text{Precision+Recall}} \tag{10}$$

5.1 Experiment Results

The evaluation of the performance of the hybrid model on the CIC-IDS2017 and CIC-DDoS2019 datasets yielded the following results:

TABLE II. CONFUSION MATRIX FOR THE CIC-IDS2017 DATASET

Actual Class	**Predicted Class**	
	Normal	***Attack***
Normal	28428	63
Attack	58	38376

Table 2 shows the results of the confusion matrix for the CIC-IDS2017 dataset with 25 selected features, where it was possible to compare the real samples and the expected samples of the hybrid model. Among these samples, 28428 were correctly classified as normal cases, 63 samples were incorrectly classified as attacks, 38376 samples were correctly classified as attacks, and 58 samples were incorrectly classified as normal cases. These results showed that the model was effective on this dataset and was able to reduce false alarms.

TABLE III. CONFUSION MATRIX FOR THE CIC-DDOS2019 DATASET

Actual Class	**Predicted Class**	
	Normal	***Attack***
Normal	4788	8
Attack	14	42648

Table 3 presents the confusion matrix of the hybrid model with the CIC-DDoS2019 dataset with 20 selected features. Notably, 4788 samples were correctly classified as normal, 8 samples were incorrectly classified as attacks, 42648 samples were correctly classified as attacks, and 14 samples were classified as normal but turned out to be attacks. A comparison revealed that the accuracy of the model in this dataset was also effective in detecting attacks and reducing false alarms to a large extent.

The confusion matrix obtained for the two datasets from the hybrid model showed that the hybrid model had a high ability to reduce false alarms and high accuracy in detecting real threats.

TABLE IV. RESULTS OF THE HYBRID MODEL PROPOSED

CIC-IDS2017 dataset			
Acc	***Recall***	***precision***	***D.R***
0.9990	0.9977	0.9979	0.9977
False Alarm Rate	***F_score***	***E.R***	***Time detection***
0.0014	2.0	0.0018	0.27 s
CIC-DDoS2019 dataset			
Acc	***Recall***	***precision***	***D.R***
0.9991	0.9970	0.9983	0.9970
FAR	***F_score***	***E.R***	***Time detection***
0.0003	2.0	0.0004	0.22 s

Table 4 presents the results of the metrics of the hybrid model on all the datasets used in the training, including precision, recall, detection rate, false alarm rate, and detection time. The results of the model with the CIC-IDS2017 dataset were very close to the results of the model with the CIC-DDoS2019 dataset in terms of accuracy and detection time, thus indicating the success of the hybrid model in the tests.

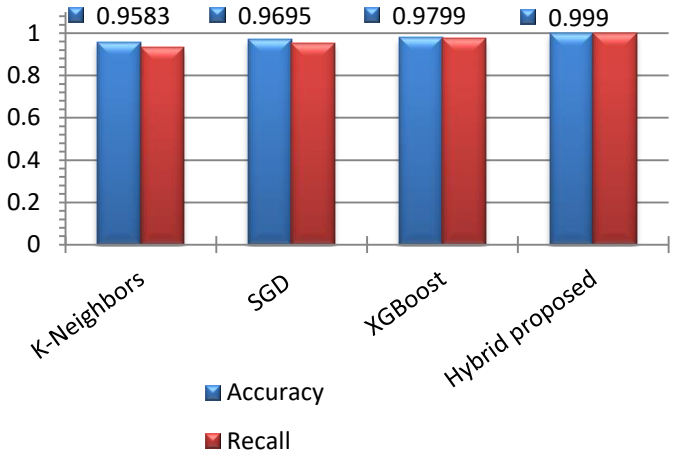

Fig. 3. Accuracy of all classifiers used for the CIC-IDS2017 dataset

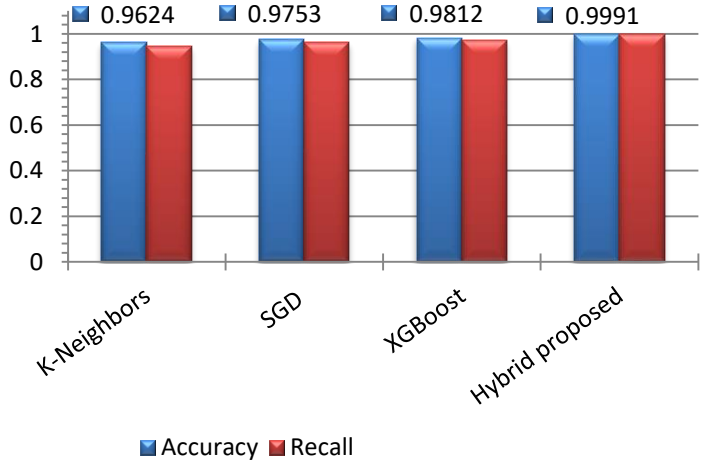

Fig. 4. Accuracy of all classifiers used for the CIC-DDoS2019 dataset

Figure 3 shows the results of the performance of the classification algorithms used and the hybrid model on the CIC-IDS2017 dataset. The K-nearest neighbor algorithm achieved an accuracy of 95.83%, the SGD algorithm achieved an accuracy of 96.95%, and the XGBoost algorithm achieved an accuracy of 97.99%. For the hybrid model, the accuracy was 99.90%. This shows the superiority of the hybrid model over the results of the algorithms alone. For the CIC-DDoS2019 dataset (Figure 4), the accuracy of the K-nearest neighbor algorithm was 96.24%, that of the SGD algorithm was 97.53%, that of the XGBoost algorithm was 98.12%, and that of the hybrid model was 99.91%. A comparison of Figures 3 and 4 reveals that the algorithms used and the hybrid model achieved high performance on both datasets. However, there was a slight improvement in the CIC-DDoS2019 dataset compared with the CIC-IDS2017 dataset. The XGBoost algorithm was the best among all the algorithms used, but it was effective in the hybrid model when combined with the other algorithms. Hence, it was concluded that the model performed well on both datasets and was superior to the separate algorithms

5.2 Comparison of the Hybrid Model with the Extant Models

After presenting the results of the hybrid model in the detection of zero-day threats, a comparison was made with previous works. Table 5 shows a comparison between previous works and the hybrid model based on the CIC-IDS2017 dataset, while Table 6 shows a comparison based on the CIC-DDoS2019 dataset.

A comparison of the results of the hybrid model with those of previous works revealed that the hybrid model outperformed the other models in previous works in terms of detection accuracy, a lower error rate, and a higher intrusion detection speed. One of the advantages of this model is its training speed, which is achieved through the use of the feature reduction method. The challenge of this work lies in the selection of appropriate classifiers and datasets to detect zero-day threats to IoT networks.

Table 5 shows a comparison of the results of the hybrid model with those of previous works based on the CIC-IDS2017 dataset in terms of the accuracy, recall, precision, F score, false alert, error rate, and execution duration metrics. According to the table, the hybrid model was superior with respect to all the metrics, where the accuracy was 99.90%, the recall was 99.77%, the precision was 99.79%, the F score was 2.0, the false alert was 0.0014%, the error rate was 0.0018%, and the execution duration was 0.27 s. This proved that the model outperformed its peers after being trained on the CIC-IDS2017 dataset.

TABLE V. COMPARISON BETWEEN THE LITERATURE REVIEW AND THE PROPOSED MODEL ON THE CIC-IDS2017 DATASET

Ref	Accuracy	Recall	precision	F_score	False Alarm Rate	Error Rate	Time
[22]	RNN =96.0%, LSTM =97.0%, GRU = 98.0%	96.0% 97.0%, 97.0%	96.0% 97.0%, 97.0%	96.0% 97.0%, 97.0%	-	-	1 min 42 s 1 min 37 s 1 min 27 s
[24]	NB= 80.84% LR=84.13% RF=98.96% XGBoost= 99.11%	80.84% 84.13% 98.96% 99.11%	81.12% 86.04% 98.97% 99.12%	80.43% 83.45% 98.96% 99.12%	0.095% 0.025% 0.012% 0.011%	-	0.03 min 0.43 min 8.48 min 4.43 min
[25]	9915%	99.14%	99.15	99.14	-	-	-
proposed model	**99.90%**	**99.77%**	**99.79%**	**99.71%**	**0.0014%**	**0.0018%**	**0.s 27**

Table 6 shows a comparison of the results of the hybrid model with the models from previous works after being trained on the CIC-DDoS2019 dataset. According to the table, the hybrid model was superior with respect to all the metrics, where the accuracy was 99.91%, the recall was 99.70%, the precision was 99.83%, the F score was 2.0, the false alert was 0.0003%, the error rate was 0.0004%, and the execution duration was 0.22 s. The results revealed that the performance of the hybrid model trained on the CIC-DDoS2019 dataset was better than that of the model trained on the CIC-IDS2017 dataset.

According to the results, the F score was high compared with that of previous works, thus indicating the potential of the hybrid model in detecting attacks and reducing false alarms.

TABLE VI. COMPARISON BETWEEN THE LITERATURE REVIEW AND THE PROPOSED MODEL ON THE CIC-DDOS2019 DATASET

Ref	Accuracy	Recall	precision	F_ score	FAR	E.R	Time
[22]	RNN =99.15%, LSTM =99.43%, GRU = 99.54%	97% 99% 99%	97% 98% 98%	97% 98% 98%	-	-	4 min 16 min30s 7 min3s
[23]	97.0%	-	-	-	-	-	-
[12]	94.55%.	95.3%	93.3%	94.3	-	-	-
[27]	97.0%	96.0%	98%	97%	-	-	-
proposed model	**99.91%**	**99.70%**	**99.83%**	**99.84%**	**0.0003%**	**0.0004%**	**0.22 s**

5.3 Discussion

Despite the large number of studies dealing with the design of cyber-attack detection systems in IoT environments, this study provides new and notable contributions within the framework of IDSs as follows:

- A hybrid approach was created that combined the ML algorithms, XGBoost, K-nearest neighbors, and SGD, using the stacking ensemble technique, taking advantage of the strengths of each algorithm where in the current study, they were used individually or not combined with these selected algorithms. The hyperparameters for each stage of the work were determined via Grid Search CV, which provided an effective and highly accurate model.
- By selecting relevant features via the sparse random projection technique, the number of relevant features was significantly reduced, and at the same time, a high level of training was obtained for the model. This could be attributed to the high accuracy of the tested model as well as its ability to reduce false alarms and its very short detection time.
- Recent datasets with real traffic for cyberattacks were used to prove the effectiveness of the model at a time when many studies focused on the use of a single dataset or nonrecent data. These data indicate that the model is generalizable and adaptable because it has been trained for many scenarios.
- Notably, there was a discrepancy in the results, and the results of this methodology were superior to those of previous studies. This was due to the hybrid method used in designing the model as well as the technique used in selecting the features that were adopted in this work. This was the main goal of the study, which was to design a model that is capable of detecting zero-day cyberattacks on IoT networks with high accuracy and reducing false alarms.
- One of the challenges encountered in the current study was to make the hybrid model adaptable to different environments and diverse circumstances. Therefore, two datasets with different sampling distributions were used to test the efficiency of the model. In the first CIC-IDS2017 dataset, the samples were evenly distributed, whereas in the second CIC-DDoS2019 dataset, the samples were unbalanced, which posed a great challenge in predicting rare samples. This approach enabled the researchers to test the extent to which the model adapted to multiple data movements and diverse datasets. A very high accuracy was obtained, which reflected the efficiency of the hybrid model.

Through these points, the hybrid model represents a real addition and contributes tangible improvements in the field of zero-day cyber-attack detection systems in IoT environments.

5.4 Limitations

With respect to the limitations of this work, the hybrid model proved its effectiveness only in the detection of DDoS attacks, so the work must be expanded to include more than one type of cyber-attack. Although the detection time was very short (0.22 s), attempts must be made to lower the detection time further. The hybrid model was able to overcome computational complexity by reducing the relevant features and choosing appropriate algorithms to ensure a lack of complexity.

6. CONCLUSION AND FUTURE WORK

In the current study, a hybrid methodology was proposed to detect zero-day cyber threats in IoT environments by relying on ML classifiers, where three classifiers were combined via the stacking ensemble technique, the best parameters for each classifier were selected via grid search CV, and the relevant features were selected and reduced, which helped reduce the training time. At the beginning of the work, the sparse random projection technique was used to select and reduce those features that helped increase the speed of training, followed by ensemble learning for the XGBoost, K-nearest neighbors and SGD algorithms, while the best hyperparameters for each algorithm were determined. The model achieved a high accuracy of 99.91% in detecting attacks with the CIC-DDoS2019 dataset. The hybrid model was also able to significantly reduce false alarms. Notably, reducing the number of features helps improve the detection time and reduce the computational complexity. The hybrid methodology provides an effective, applicable, and generalizable solution in IoT environments that require high speed in detecting attacks. It can be used in many fields, including smart homes and camera monitoring systems, and for protecting medical devices. Compared with recent methods, the hybrid model has been shown to be superior. With respect to the limitations of this work, the model was able to detect only one type of attack. Therefore, future work should include other types of attacks, which should be integrated into the hybrid model to make it more comprehensive.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

There is no funding for the paper.

Acknowledgement

The authors would like to thank the University of Technology for their support in conducting the work published in this paper.

References

[1] S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, "Comparative evaluation of ai-based techniques for zero-day attacks detection," *Electronics*, vol. 11, no. 23, p. 3934, 2022.

[2] Y. Wang, Z. Pan, J. Zheng, L. Qian, and M. Li, "A hybrid ensemble method for pulsar candidate classification," *Astrophysics and Space Science*, vol. 364, pp. 1-13, 2019.

[3] S. Balasubramaniam *et al.*, "Optimization enabled deep learning-based DDoS attack detection in cloud computing," *International Journal of Intelligent Systems*, vol. 2023, 2023.

[4] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. a. Tawalbeh, "Zero-day attack detection: a systematic literature review," *Artificial Intelligence Review*, vol. 56, no. 10, pp. 10733-10811, 2023.

[5] K. Hamid, M. W. Iqbal, M. Aqeel, T. A. Rana, and M. Arif, "Cyber Security: Analysis for Detection and Removal of Zero-Day Attacks (ZDA)," in *Artificial Intelligence & Blockchain in Cyber Physical Systems*: CRC Press, pp. 172-196.

[6] Y. Mezquita, R. Casado, A. Gonzalez-Briones, J. Prieto, J. M. Corchado, and A. AETiC, "Blockchain technology in IoT systems: review of the challenges," *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp. 2516-0281, 2019.

[7] A. Jamil, M. Q. Ali, and M. E. A. Alkhalec, "Sinkhole attack detection and avoidance mechanism for RPL in wireless sensor networks," *Annals of Emerging Technologies in Computing (AETiC)*, vol. 5, no. 5, pp. 94-101, 2021.

[8] Z. Mahdi, N. Abdalhussien, N. Mahmood, and R. Zaki, "Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on Internet of Things (IoT) Networks Using Machine Learning Algorithms," *Computers, Materials and Continua*, vol. 80, no. 2, pp. 2139-2159, 2024.

[9] M. H. L. Louk and B. A. Tama, "Dual-IDS: A bagging-based gradient boosting decision tree model for network anomaly intrusion detection system," *Expert Systems with Applications*, vol. 213, p. 119030, 2023.

[10] N. M. Zaed Mahdi "A Proposed Intrusion Detection System Based on an Improved Random Forest Using a Double Feature Selection Method," *Trends in Applied Sciences Research*, vol. 19, no. 1, p. 10, 2024.

[11] I. Hidayat, M. Z. Ali, and A. Arshad, "Machine learning-based intrusion detection system: an experimental comparison," *Journal of Computational and Cognitive Engineering*, vol. 2, no. 2, pp. 88-97, 2023.

[12] M. Roopak, S. Parkinson, G. Y. Tian, Y. Ran, S. Khan, and B. Chandrasekaran, "An Unsupervised Approach for the Detection of Zero-Day DDoS Attacks in IoT Networks."

[13] S. Venkatesan, "Design an intrusion detection system based on feature selection using ML algorithms," *Mathematical Statistician and Engineering Applications*, vol. 72, no. 1, pp. 702-710, 2023.

[14] N. Tekin, A. Acar, A. Aris, A. S. Uluagac, and V. C. Gungor, "Energy consumption of on-device machine learning models for IoT intrusion detection," *Internet of Things*, vol. 21, p. 100670, 2023.

[15] U. M. Khaire and R. Dhanalakshmi, "Stability of feature selection algorithm: A review," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1060-1073, 2022.

[16] P. Dhal and C. Azad, "A comprehensive survey on feature selection in the various fields of machine learning," *Applied Intelligence*, vol. 52, no. 4, pp. 4543-4581, 2022.

[17] S. Santhosh Kumar, M. Selvi, and A. Kannan, "A Comprehensive Survey on Machine Learning-Based Intrusion Detection Systems for Secure Communication in Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, p. 8981988, 2023.

[18] O. H. Abdulganiyu, T. Ait Tchakoucht, and Y. K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," *International journal of information security*, vol. 22, no. 5, pp. 1125-1162, 2023.

[19] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 538-566, 2023.

[20] A. M. Koay, R. K. L. Ko, H. Hettema, and K. Radke, "Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges," *Journal of Intelligent Information Systems*, vol. 60, no. 2, pp. 377-405, 2023.

[21] M. B. Praveena and A. Devi, "A Survey on Different Methods for Zero-Day Attack Detection in IoT Edge Devices," *NATURALISTA CAMPANO*, vol. 28, no. 1, pp. 697-703, 2024.

[22] M. Ramzan *et al.*, "Distributed denial of service attack detection in network traffic using deep learning algorithm," *Sensors*, vol. 23, no. 20, p. 8642, 2023.

[23] M. Mittal, K. Kumar, and S. Behal, "DL-2P-DDoSADF: Deep learning-based two-phase DDoS attack detection framework," *Journal of Information Security and Applications*, vol. 78, p. 103609, 2023.

[24] S. Farhat, M. Abdelkader, A. Meddeb-Makhlouf, and F. Zarai, "Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset," in *ICISSP*, 2023, pp. 287-295.

[25] S. Wang, W. Xu, and Y. Liu, "Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things," *Computer Networks*, vol. 235, p. 109982, 2023.

[26] Y. K. Beshah, S. L. Abebe, and H. M. Melaku, "Drift Adaptive Online DDoS Attack Detection Framework for IoT System," *Electronics*, vol. 13, no. 6, p. 1004, 2024.

[27] Z. M. Jiyad, A. Al Maruf, M. M. Haque, M. S. Gupta, A. Ahad, and Z. Aung, "DDoS Attack Classification Leveraging Data Balancing and Hyperparameter Tuning Approach Using Ensemble Machine Learning with XAI," in *2024 Third International Conference on Power, Control and Computing Technologies (ICPC2T)*, 2024, pp. 569-575: IEEE.

[28] Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," *Computer communications*, vol. 198, pp. 175-185, 2023.

[29] T. Zoppi, A. Ceccarelli, and A. Bondavalli, "Unsupervised algorithms to detect zero-day attacks: Strategy and application," *Ieee Access*, vol. 9, pp. 90603-90615, 2021.

[30] M. Soltani, B. Ousat, M. J. Siavoshani, and A. H. Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," *Journal of Information Security and Applications*, vol. 76, p. 103516, 2023.

[31] B. M. Serinelli, A. Collen, and N. A. Nijdam, "On the analysis of open source datasets: validating IDS implementation for well-known and zero day attack detection," *Procedia Computer Science*, vol. 191, pp. 192-199, 2021.
[32] A. Thakkar and R. Lohiya, "Fusion of statistical importance for feature selection in Deep Neural Network-based Intrusion Detection System," *Information Fusion*, vol. 90, pp. 353-363, 2023.
[33] R. A. Ramadan and K. Yadav, "A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks," *Annals of Emerging Technologies in Computing (AETiC), Print ISSN*, pp. 2516-0281, 2020.
[34] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine learning and deep learning approaches for cybersecurity: A review," *IEEE Access*, vol. 10, pp. 19572-19585, 2022.
[35] I. E. Salem, M. M. Mijwil, A. W. Abdulqader, M. M. Ismaeel, A. Alkhazraji, and A. M. Z. Alaabdin, "Introduction to the data mining techniques in cybersecurity," *Mesopotamian journal of cybersecurity*, vol. 2022, pp. 28-37, 2022.
[36] L. R. Ali, B. N. Shaker, and S. A. Jebur, "An extensive study of sentiment analysis techniques: A survey," in *AIP Conference Proceedings*, 2023, vol. 2591, no. 1: AIP Publishing.
[37] L. A. E. Al-saeedi, F. J. Shakir, F. K. Hasan, G. G. Shayea, Y. L. Khaleel, and M. A. J. M. J. o. C. Habeeb, "Artificial Intelligence and Cybersecurity in Face Sale Contracts: Legal Issues and Frameworks," vol. 4, no. 2, pp. 129-142, 2024.
[38] F. K. H. Mihna, M. A. Habeeb, Y. L. Khaleel, Y. H. Ali, and L. A. E. J. M. J. o. C. Al-saeedi, "Using information technology for comprehensive analysis and prediction in forensic evidence," vol. 4, no. 1, pp. 4-16, 2024.
[39] Z. Shao, M. N. Ahmad, and A. Javed, "Comparison of Random Forest and XGBoost Classifiers Using Integrated Optical and SAR Features for Mapping Urban Impervious Surface," *Remote Sensing*, vol. 16, no. 4, p. 665, 2024.
[40] L. Dhanya and R. Chitra, "A novel autoencoder based feature independent GA optimised XGBoost classifier for IoMT malware detection," *Expert Systems with Applications*, vol. 237, p. 121618, 2024.
[41] P. Kalyani *et al.*, "RETRACTED ARTICLE: Prediction of patient's neurological recovery from cervical spinal cord injury through XGBoost learning approach," *European Spine Journal*, vol. 32, no. 6, pp. 2140-2148, 2023.
[42] V. J. Pandya, "Comparing handwritten character recognition by AdaBoostClassifier and KNeighborsClassifier," in *2016 8th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2016, pp. 271-274: IEEE.
[43] F. Kabir, S. Siddique, M. R. A. Kotwal, and M. N. Huda, "Bangla text document categorization using stochastic gradient descent (sgd) classifier," in *2015 international conference on cognitive computing and information processing (CCIP)*, 2015, pp. 1-4: IEEE.
[44] D. Kalimeris *et al.*, "Sgd on neural networks learns functions of increasing complexity," *Advances in neural information processing systems*, vol. 32, 2019.
[45] M. Lu *et al.*, "A stacking ensemble model of various machine learning models for daily runoff forecasting," *Water*, vol. 15, no. 7, p. 1265, 2023.
[46] N. Pudjihartono, T. Fadason, A. W. Kempa-Liehr, and J. M. O'Sullivan, "A review of feature selection methods for machine learning-based disease risk prediction," *Frontiers in Bioinformatics*, vol. 2, p. 927312, 2022.
[47] A. Kabán and H. Reeve, "Structure discovery in PAC-learning by random projections," *Machine Learning*, pp. 1-46, 2024.
[48] X. Tan, J. Yang, and S. Rahardja, "Sparse random projection isolation forest for outlier detection," *Pattern Recognition Letters*, vol. 163, pp. 65-73, 2022.
[49] N. M. Zaed Mahdi "Intrusion Detection Methodologies Based on Machine Learning:Feature Selection, Datasets, Performance Measures and Results," presented at the 7th National Conference on New Idea on Electrical Engineering, Isfahan, Iran, January 2023, 2023.
[50] D. Kumar, R. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS detection using deep learning," *Procedia Computer Science*, vol. 218, pp. 2420-2429, 2023.
[51] H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic Dos/DDoS attacks detection in software-defined networks," *Applied Sciences*, vol. 13, no. 6, p. 3828, 2023.
[52] A. Rosay, E. Cheval, F. Carlier, and P. Leroux, "Network intrusion detection: A comprehensive analysis of CIC-IDS2017," in *8th International Conference on Information Systems Security and Privacy*, 2022, pp. 25-36: SCITEPRESS-Science and Technology Publications.

[53] M. Cantone, C. Marocco, and A. Bria, "Generalization Challenges in Network Intrusion Detection: A Study on CIC-IDS2017 and CSE-CIC-IDS2018 Datasets," in *1st INTERNATIONAL PhD SYMPOSIUM ON ENGINEERING AND SPORT SCIENCE*, p. 185.

[54] R. Ma, X. Chen, and R. J. E. Zhai, "A DDoS Attack Detection Method Based on Natural Selection of Features and Models," vol. 12, no. 4, p. 1059, 2023.

[55] Z. S. Mahdi, R. M. Zaki, L. J. S. Alzubaidi, and Privacy, "Advanced Hybrid Techniques for Cyberattack Detection and Defense in IoT Networks," p. e471, 2024.

[56] R. M. Zaki, T. W. Khairi, and A. E. Ali, "Secure data sharing based on linear congruetial method in cloud computing," in *Next Generation of Internet of Things: Proceedings of ICNGIoT 2021*, 2021, pp. 129-140: Springer.