Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.041186

ARTICLE

Internet of Things (IoT) Security Enhancement Using XGboost Machine Learning Techniques

Dana F. Doghramachi[1,*] **and Siddeeq Y. Ameen**[2]

[1]Department of Information Systems Engineering Techniques, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, 44001, Iraq

[2]Department of Energy Engineering, Technical College of Engineering, Duhok Polytechnic University, Duhok, 42001, Iraq

*Corresponding Author: Dana F. Doghramachi. Email: dana.farhad@epu.edu.iq

Received: 13 April 2023 Accepted: 18 July 2023 Published: 31 October 2023

ABSTRACT

The rapid adoption of the Internet of Things (IoT) across industries has revolutionized daily life by providing essential services and leisure activities. However, the inadequate software protection in IoT devices exposes them to cyberattacks with severe consequences. Intrusion Detection Systems (IDS) are vital in mitigating these risks by detecting abnormal network behavior and monitoring safe network traffic. The security research community has shown particular interest in leveraging Machine Learning (ML) approaches to develop practical IDS applications for general cyber networks and IoT environments. However, most available datasets related to Industrial IoT suffer from imbalanced class distributions. This study proposes a methodology that involves dataset preprocessing, including data cleaning, encoding, and normalization. The class imbalance is addressed by employing the Synthetic Minority Oversampling Technique (SMOTE) and performing feature reduction using correlation analysis. Multiple ML classifiers, including Logistic Regression, multi-layer perceptron, Decision Trees, Random Forest, and XGBoost, are employed to model IoT attacks. The effectiveness and robustness of the proposed method evaluate using the IoTID20 dataset, which represents current imbalanced IoT scenarios. The results highlight that the XGBoost model, integrated with SMOTE, achieves outstanding attack detection accuracy of 0.99 in binary classification, 0.99 in multi-class classification, and 0.81 in multiple sub-classifications. These findings demonstrate our approach's significant improvements to attack detection in imbalanced IoT datasets, establishing its superiority over existing IDS frameworks.

KEYWORDS

IoT; detection system; machine learning; SMOTE; XGboost

1 Introduction

The IoT is gaining popularity in various industries, significantly impacting people's daily lives by providing essential services and leisure activities [1,2]. This innovative technology enables the connection of physical objects from anywhere in the world, thanks to its integration with the Internet [3,4]. However, the majority of IoT devices lack sufficient software protection and contain both evident and unnoticed vulnerabilities [5]. Consequently, the development of IoT networks exposes them to exploitation by malicious actors who can launch extensive cyberattacks. These attacks can lead to severe consequences such as infrastructure damage, service disruptions, significant financial losses, and reputational harm to large corporations. Consequently, identifying vulnerable IoT devices and disconnecting them from the Internet before they can be compromised and added to an IoT botnet is a crucial security measure against these attacks [6–8].

Several strategies can be highlighted for identifying and isolating IoT networks through access routers, thereby separating IoT bots and preventing device takeovers [1,9]. Another approach involves passive detection and identification of bot attacks by analyzing all internal and networked IoT activities. However, given the scarcity of human resources and the enormous amount of data to be processed within a specific timeframe, utilizing human analysis for this purpose becomes costly [4]. Hence, the application of artificial intelligence (AI) and machine learning (ML) becomes more practical. ML, as a technical suite of artificial intelligence, is capable of discovering, analyzing, and categorizing data. AI, on the other hand, refers to the ability of a mechanical device to emulate human intellectual processes. Based on these concepts, algorithms can be developed to facilitate automatic development, configuration, and even independent operation [10]. Moreover, this enables us to detect cyberattacks with minimal errors and high speed.

This paper aims to model IoT attacks at the binary, multiple, and sub-classification levels using ML models while addressing the issue of imbalanced data through the use of SMOTE. The study proposes the employment of SMOTE with Ensemble Learning to protect current IoT networks from nine different types of attacks. Balancing the dataset is crucial, and if it exhibits an imbalance, the widely used technique known as SMOTE is applied. This ensures that the dataset is appropriately balanced and ready for further analysis. Furthermore, the size of the data collection is reduced by identifying highly correlated features within the dataset and performing feature reduction. Additionally, a group of ML-based classifiers, namely Logistic Regression (LR), multi-layer perceptron (MLP), Decision Trees (DT), Random Forest (RF), and XGBoost (XGB), were employed. Finally, the effectiveness of the proposed feature selection and categorization methodologies was evaluated and compared to existing methods.

This paper covers the theoretical framework of ML algorithms used in IoT modeling and the data balancing technique. It also discusses related works that have utilized the same dataset, followed by the presentation of the proposed methodology and the implementation and evaluation of the analysis system.

2 Contributions

The study addresses the challenge of imbalanced class distributions in IoT security datasets, and the contributions can be summarized as follows:

1. A proposed methodology includes dataset preprocessing techniques and using SMOTE to address the class imbalance.
2. Multiple ML classifiers, including LR, MLP, DT, RF, and XGBoost, are evaluated for modeling IoT attacks, and XGBoost is identified as a superior model for attack detection accuracy.
3. Evaluate the proposed method using the IoTID20 dataset, representing modern imbalanced IoT scenarios and demonstrating its effectiveness in different classification scenarios.
4. The proposed approach outperforms existing IDS frameworks in detecting attacks in imbalanced IoT datasets based on accuracy metrics and comparison with other classifiers.

3 Related Work

Various ML techniques are used to detect attacks in IoT systems. Some studies have focused on identifying attacks by analyzing abnormal patterns in network traffic. One such approach is the Self-Evolving Host-based Intrusion Detection System (SEHIDS), which utilizes a lightweight Artificial Neural Network (ANN) IDS system for IoT networks [11]. The core concept of SEHIDS involves equipping each IoT device with a miniature ANN architecture and a resource mechanism that enables the architecture to be trained and enhanced whenever the IoT device's performance deteriorates.

Another collaborative IDS system, MidSiot, is introduced and deployed at Internet and IoT local gateways [12]. This IDS system operates in three phases: firstly, it identifies each IoT device present in the IoT network; secondly, it distinguishes between legitimate and erroneous network traffic; and finally, it determines the types of attacks directed at IoT devices. However, it should be noted that these methods often suffer from drawbacks in terms of cost and resource requirements, making them less feasible in practical implementations.

Meanwhile, a group of researchers proposed a model addressing the problem of selecting appropriate hyperparameters for ANN models to detect attacks [13]. In this model, a portion of the dataset is used to determine the hyperparameters that are most suited for reducing the overhead associated with designing the ANN architecture, configuring its functionality, and evaluating its performance. The aim is to detect five categorical attacks and nine sub-categorical assaults.

In addition, another approach suggested in [14] is a deep-convolutional neural network (DCNN)-based IDS. The DCNN architecture consists of three densely connected layers and two convolutional layers. The experiments in this study employed the IoTID20 dataset. The suggested model underwent various optimization approaches, and the performance of optimization algorithms such as Adam, AdaMax, and Nadam was evaluated, with Adam, AdaMax, and Nadam demonstrating the best performance. However, it is worth noting that in certain data types, neural networks may exhibit bias during training toward majority classes, potentially resulting in imbalanced performance.

While most studies have employed traditional ML algorithms and ensemble learning, a particular study [15] investigated the performance of various ML algorithms, such as DT, RF, and XGBoost (XGB), in predicting network attacks on IoT devices. The authors found that DT algorithms generally exhibit higher accuracy than RF and gradient-boosting machines. However, RF algorithms outperformed others regarding Area Under the ROC Curve (AUC) scores since they combined the results of multiple DTs. The study [16] employed the RF algorithm and One Hot Encoding technique with the IoTID20 dataset, which includes three targets, to validate their approach. Their findings reinforced that RF is typically the most accurate algorithm. In another study [17], multiple ML algorithms were applied to detect unusual behavior in IoT networks using the IoTID20 dataset. The researchers identified essential and strongly connected features and ranked them based on importance. They evaluated the dataset using 15 popular ML algorithms and concluded that Gradient Boosting performs best as a classifier.

Additionally, the study [18] proposed a system for identifying compromised IoT devices utilizing various ML methods. The ML model was constructed using the IoTID20 dataset to detect abnormal behavior in IoT networks. For the experiment, 4,000 random records from the dataset were selected. Two algorithms, Pearson's correlation, and LR, were employed to choose the characteristics. Fifteen features were selected to classify packets as normal or anomalous. Based on the performance criteria outlined in the article, except for time, the results indicated that RF and AdaBoost classifiers provided highly similar and top-performing results. Overall, these studies demonstrate the efficacy of different

ML algorithms in detecting attacks and unusual behavior in IoT networks, with DT, RF, and Gradient Boosting often exhibiting strong performance.

The study [19] proposes a hybrid ML model that combines the XGBoost algorithm with decision tree-based feature selection techniques for IoT intrusion detection. The model achieved improved accuracy compared to traditional ML algorithms. In [20], the authors propose an intrusion detection system (IDS) for IoT networks using ensemble techniques such as bagging and boosting. They evaluate various ML algorithms and ensemble combinations to enhance the detection accuracy of IoT attacks. Le et al. [21] presents an ML-based IDS for IoT networks. It incorporates feature selection methods and voting ensemble techniques to improve the detection accuracy of attacks in IoT environments. In [22], the authors compare the performance of multiple ML algorithms, including DT, RF, support vector machines, and neural networks for intrusion detection in IoT networks. They evaluate the algorithms based on accuracy, precision, recall, and F1-score metrics. The study [23] proposes an IDS for IoT systems using ML algorithms. The authors compare the performance of LR, DT, and RF for detecting attacks in IoT networks. Paper [24] proposes an anomaly-based intrusion detection system (IDS) specifically designed for IoT applications. The system aims to detect attacks by identifying abnormal behavior patterns in IoT networks. The authors describe the architecture and functioning of the IDS, which involves collecting network traffic data, feature extraction, and anomaly detection using ML techniques. The study evaluates the performance of the proposed IDS using a dataset of IoT network traffic and compares it with other existing IDS approaches. In [25], they present a quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. The research focuses on addressing the security challenges in healthcare IoT applications. The proposed model incorporates quantum trust and blockchain technology to enhance the security and privacy of healthcare data. The authors discuss the model's architecture, which involves using quantum key distribution, blockchain consensus mechanisms, and smart contracts. The study highlights the model's potential to provide robust security for healthcare IoT systems. In [26], the authors present a novel measurement scheme for evaluating the security and privacy aspects of IoT applications utilizing ML algorithms. The research focuses on developing a comprehensive framework to assess the security and privacy levels of IoT applications. The authors proposed a set of security and privacy metrics and utilize ML algorithms to evaluate and classify IoT applications based on these metrics. The study discusses the implementation of the framework and presents experimental results using real-world IoT datasets. The findings demonstrate the effectiveness of the proposed scheme in assessing the security and privacy aspects of IoT applications.

The gap in the research on methods of detecting IoT attacks using ML algorithms can be summarized in achieving performance accuracy with smaller datasets and fewer attributes that affect attack detection. As a result, the problem can be defined by the need for more recent IoTID20 datasets with many characteristics. Even when dataset sizes grow, most predictions are made using conventional ML techniques that do not improve attack detection accuracy, making it difficult to choose the optimum ML methodology for specific data. Moreover, most studies that use the IoTID20 dataset distinguish the presence of the attack and do not consider the type of attack and its sub-classification. Moreover, there is no indication of the imbalance between the data and its treatment. Finally, studies used single methods to identify feature selection, while more than one method could be hybridized.

4 Machine Learning for IoT Security

The primary focus of this study is the use of ML to detect and categorize system traffic threats. Various supervised ML techniques include LR, MLP, DT, RF, and XGB. In addition to data balancing using SMOTE, LR is one of the ML algorithms and one of the most popular classification algorithms because its steps are simple. It is a classification algorithm to classify data into separate classes when the response variable is categorical [11]. LR aims to find a relationship between properties and the probability of a given outcome [27]. A DT functions by removing representative items from a data collection and arranging them in trees according to the object's value [11,28]. A tree node represents each characteristic, and branches branching from this node indicate the relevant values [29]. The starting node of the tree is at any functional node that best bisects the tree. Different criteria, such as the Gini index and the Information Gain, that best split the training data sets are utilized to pinpoint the first node [30]. Multiple DTs are used in constructing RF to forecast more accurate and fault-tolerant categorization outcomes [15]. Randomly built DTs are taught to provide categorization outcomes based on votes from most participants [31]. While DTs may be seen as parts of RF, there are two different classification algorithms because, in contrast to DTs, which develop a set of rules during training to categorize incoming samples further, RF develops a subset of rules utilizing all DT members [11].

Extreme Gradient Boosting is often known as an extreme boosting tree or an expanded version of the Gradient Boosting Machine technique [32]. The Boosting ensemble algorithm can form a strong classifier with higher accuracy after the weighted superposition of multiple weak classifiers with lower accuracy to reduce errors and improve accuracy [33]. The extreme gradient boosting algorithm is improved based on the Boosting algorithm. The objective function is minimized by using gradient descent for each generated tree and based on all the trees generated in the previous step [34]. At the same time, the second-order Taylor expansion of the loss function is carried out in the XGB algorithm, and a regular term is added to the cost function to control the complexity of the model [11].

In ML and data science, imbalanced data distribution is prevalent and usually occurs when observations in one category are much higher or lower than in other categories [35]. ML algorithms tend to improve accuracy by minimizing errors, as they do not consider class distributions. This problem is prevalent in fraud detection, anomaly detection, facial recognition, etc. [36,37]. On the other hand, SMOTE is one of the most commonly used oversampling methods to solve imbalance problems [38]. It aims to balance the class distribution by randomly increasing minority class examples by replicating minority class examples [39]. SMOTE synthesizes new minority instances among existing minority instances. It generates virtual training records by linear interpolation over the minority class. These synthetic training records are generated by randomly selecting one or more k-nearest neighbors for each example in the minority class [40,41]. After the oversampling process, the data is reconstructed, and multiple classification models can be applied to the processed data [38].

5 Proposed ML Techniques for IoT Security Enhancement

5.1 System Layout

To classify IoT attacks, data preprocessing was performed at the first preprocessing stage such that categorical data were converted into values using One-Hot encoding. Next, feature filtering to delete features without any effect on prediction accuracy, high correlation, and features with single values. To accomplish the tasks, three datasets are created according to the type of classification. The dataset is further divided into a training set and a test set. The training set is used to train ML models, and the dataset is used to test the performance of the selected models. After determining the best classifier to classify IoT attacks on the three levels, the balanced data is compared with the basic model, as shown in Fig. 1.

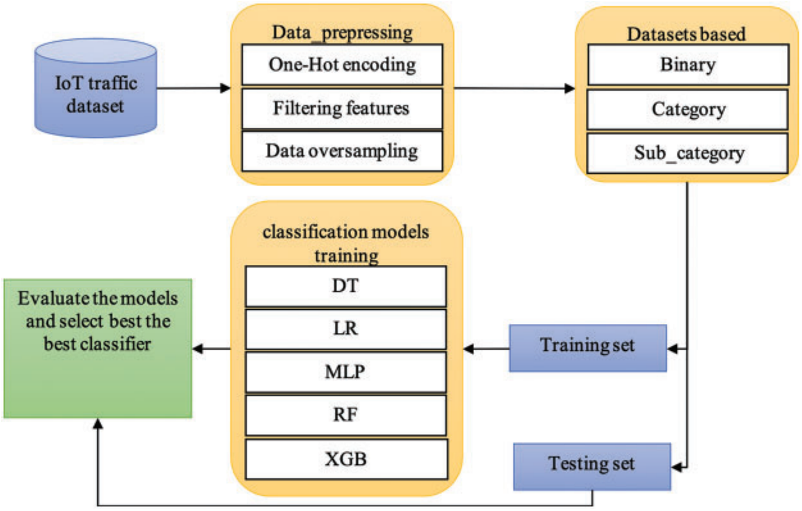


Figure 1: Proposed methodology for modeling IoT attacks

Python has been used to develop models; the pseudocode of the proposed model is represented in Algorithm 1.

Algorithm 1: Pseudocode OF XGB_SMOTE

```
Input: ($XG$: eXtreme Gradient Boosting algorithm, $S$: SMOTE method, $D$: preprocessed IoTID20 dataset)
Data split
    $D_{train}$: 80% of $D$, $D_{test}$: 20% of $D$
    ($D_{x\_train}$, $D_{y\text{-}train}$): split $D_{train}$ based Input and Output
    ($D_{x\_test}$, $D_{y\text{-}test}$): split $D_{test}$ based Input and Output
Use $S$ to minority class in ($D_{x\_train}$, $D_{y\text{-}train}$):
    Instantiate the $S$ object with the desired parameters
    Call the "fit" method of the S object on the ($D_{x\_train}$, $D_{y\_train}$)
    ($S_{x\_train}$, $S_{y\text{-}train}$) = $S$.fit ($D_{x\_train}$, $D_{y\text{-}train}$)
Build Classifier XGmodel using ($S_{x\_train}$, $S_{y\_train}$) and $XG$
    XGmodel = $XG$.fit ($S_{x\_train}$, $S_{y\_train}$)
Predict output based on trained model XGmodel using ($D_{x\_test}$)
    $Y_{predict}$ = XGmodel ($D_{x\_test}$)
Return: $Y_{predict}$
```

5.2 *Dataset Preprocessing*

When developing an ML model, it is essential to decide which features should be used as input for the learning algorithm [32]. Once data has been obtained from the IoTID20, the preprocessing is done using one-hot encoding. It is necessary to convert the tagged data into a numerical format because it is frequently not in a machine-readable form. In addition, the data contains features that are not useful in training classification algorithms, such as correlated or unimportant features. The unstructured data will thus be transformed into structured data using the following preprocessing methods.

5.2.1 One-Hot Encoding

One-Hot encoding is the representation of categorical variables as binary vectors. The One Hot encoding addresses the Category value that changed to a Column value of 0 or 1 [42]. The first column value corresponds to the true row values with a value of 1. The values in the other columns denote false, represented by the integer 0. The real value is between 0 and 1 if the values in the rows and columns match. To turn labels into numeric values, preprocessing one hot encoding is performed.

5.2.2 Filtering Features

In this study, two feature filtering techniques were used, the first is to delete the correlated features, and the second is to delete the features of importance that do not affect the classification accuracy. To find feature correlation, Pearson correlation was used. Pearson correlation generates a percentage correlation coefficient, abbreviated as r, that assesses the strength and direction of linear correlations between data groups [42,43]. Features with a correlation of more than 98% were removed. Table 1 shows the correlation between the features.

Table 1: Correlation of the features

Features	Correlation feature	Ratio
Tot_Fwd_Pkts	Subflow_Fwd_Pkts	1
Tot_Fwd_Pkts	Fwd_Act_Data_Pkts	0.992120026
Tot_Bwd_Pkts	Subflow_Bwd_Pkts	1
TotLen_Fwd_Pkts	Subflow_Fwd_Byts	1
TotLen_Bwd_Pkts	Subflow_Bwd_Byts	1
Fwd_Pkt_Len_Max	Fwd_Pkt_Len_Mean	0.987378147
Fwd_Pkt_Len_Max	Fwd_Seg_Size_Avg	0.987378147
Fwd_Pkt_Len_Mean	Fwd_Seg_Size_Avg	1
Bwd_Pkt_Len_Mean	Pkt_Len_Mean	0.984314689
Bwd_Pkt_Len_Mean	Bwd_Seg_Size_Avg	1
Flow_IAT_Max	Idle_Max	0.999767661
Bwd_PSH_Flags	PSH_Flag_Cnt	1
Bwd_URG_Flags	URG_Flag_Cnt	1
Flow_IAT_Max	Idle_Max	0.999767661
Bwd_PSH_Flags	PSH_Flag_Cnt	1
Bwd_URG_Flags	URG_Flag_Cnt	1
Pkt_Len_Mean	Pkt_Size_Avg	0.996424609

Feature importance analysis was performed using the built-in mechanism of the sklearn ensemble. The RF classifier method (feature_importances_attribute) implements the entropy approach to feature importance assessment. The results of the importance evaluation showed that there is zero importance in terms of classification accuracy, as shown in Table 2.

Table 2: Lists of features with zero importance

Feature	Importance
Bwd_Pkts/b_Avg	0
Bwd_Blk_Rate_Avg	0
Bwd_Byts/b_Avg	0
Fwd_Seg_Size_Min	0
Fwd_Blk_Rate_Avg	0
Fwd_Pkts/b_Avg	0
Fwd_Byts/b_Avg	0
Fwd_PSH_Flags	0
Fwd_URG_Flags	0
Init_Fwd_Win_Byts	0

5.3 Dataset

The IoTID20 data was created to find IoT network cyberattacks. SKT NGU and EZVIZ Wi-Fi cameras created the dataset utilizing smart home devices [44]. This dataset's key benefit is that it contains new information on detecting network interference and current communication data. This dataset has three label levels: binary, category, and subcategory, totaling 85 IoT network attributes. These categories are distributed for classification, as shown in Fig. 2.

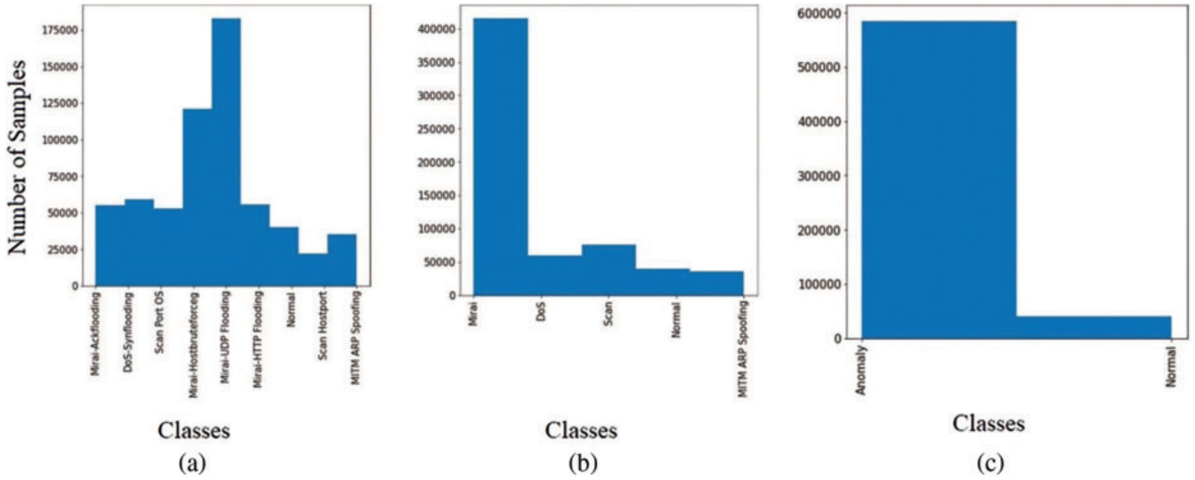
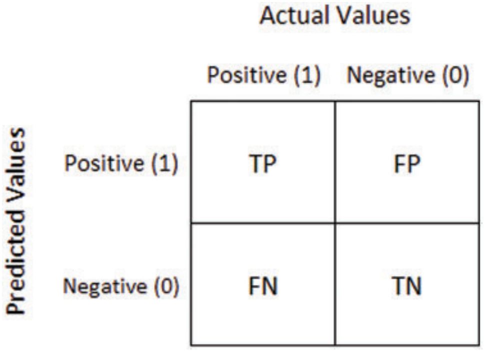


Figure 2: Distribution of the target group at the level of (a) binary, (b) category, and (c) subcategory classifications

5.4 Classification Problem

When choosing a model for solving the considered classification problem, the quality of the most common ML models was assessed on a balanced and preprocessed subsample of IoT attacks of the IoTID20 dataset. The quality of the responses of classifiers (models) was compared using the following metrics (Accuracy, Precision, Recall, and F1). When determining the values of quality metrics, elements of the error matrix (confusion matrix) corresponding to the number of correct and incorrect answers based on the results of classifier testing should be found, as shown in Fig. 3.



		Actual Values	
		Positive (1)	Negative (0)
Predicted Values	Positive (1)	TP	FP
	Negative (0)	FN	TN

Figure 3: Confusion matrix [45]

In Fig. 3, TP (True Positive) denotes a truly positive response, TN (True Negative) an actual negative response, FP (False Positive) a false positive response (False Positive, Type I error), FN (False Negative) a false negative response (missing attack, Type II error) [46]. Taking into account the given designations, the used quality metrics are determined by the following expressions:

$$\text{Accuracy} = \text{TP} + \text{TN}/(\text{TP} + \text{FP} + \text{FN} + \text{TN}) \tag{1}$$

$$\text{Precision} = \text{TP}/(\text{TP} + \text{FP}) \tag{2}$$

$$\text{Recall} = \text{TP}/(\text{TP} + \text{FN}) \tag{3}$$

$$\text{F1} = 2 * \text{Precision} * \text{Recall}/(\text{Precision} + \text{Recall}) \tag{4}$$

Accuracy measures the proportion of all correctly classified instances (both positive and negative) out of the total number of instances evaluated. It provides an overall measure of how well the classifier performs. Precision is the proportion of True Positives (TP) to the total number of predicted positive instances (TP and FP). It represents the percentage of the correct positive predictions. Recall (also known as sensitivity or true positive rate) is the proportion of True Positives (TP) to the total number of actual positive instances (TP and FN). It represents the percentage of positive instances that are correctly identified by the classifier. Considering both metrics, the F1-score is a harmonic mean of precision and recall. It ranges from 0 to 1, with 1 being the best possible score.

6 Results and Discussion

6.1 Results

In this study, the Python language was used in practical experiments. The Sklearn library was used to build ML models. Scikit-learn (sklearn) is a popular ML library in Python that provides a variety of tools for building predictive models. It is built on top of NumPy, SciPy, and the matplotlib libraries and offers a simple and efficient way to implement a wide range of ML algorithms, including classification, regression, clustering, and dimensionality reduction. The quality of the classifiers was assessed on an imbalanced, preprocessed IoT attack subsample of the IoTID20 dataset with an 80:20 ratio of normal and abnormal traffic (55 of the most significant features). The investigation was conducted with the IoTID20 dataset using a set of ML algorithms and suggested using the XGB algorithm for classification with SMOTE to balance data in the case of subcategory classifications.

Initially, all models, DT, LR, MLP, RF, and XGB, values of quality measures are obtained using binary classification as shown in Fig. 4.

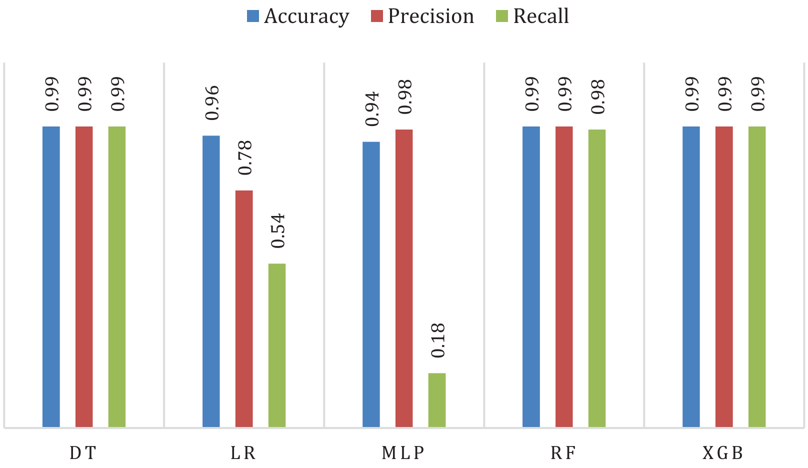


Figure 4: Performance of classification algorithms in binary classification

It is clear from Fig. 4 that DT and XGB models achieved the best accuracy, as it was 0.99 on various scales, followed by RF, which was 0.99 using accuracy and precision, and 0.98 using the Recall scale. While the performance of MLP and LR was acceptable on the Accuracy scale. MLP and LR were low on the Recall scale, indicating that these two models have a bias due to the imbalanced data set. In the second stage, models were tested in the case of multiple classifications of the attack type. The average precision and recall rates were taken in the results since the classification is multi-class.

Another test on the five models compares different models' performance in predicting the attack type, as shown in Fig. 5.

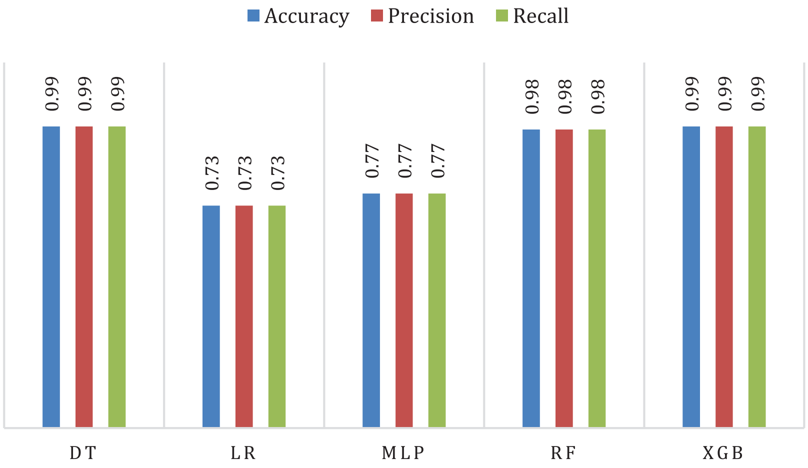


Figure 5: Performance of classification models in category classification

It is clear from Fig. 5 that in the case of multiple classifications, DT and XGB achieved the best performance, as it was 0.99 for the three measures, followed by RF, which was 0.98. It is also noted that the performance of the models is balanced for the various algorithms, as it was 0.77 using MLP and 0.73 using LR for the three measures.

Extra test for classification is achieved on the models based on the types of attacks and their sub-classifications. It is important to note that SMOTE data balancing techniques are used even if classes are imbalanced. This will increase the number of tested models to six to have XGB_SMOTE. The results of this test are shown in Fig. 6.

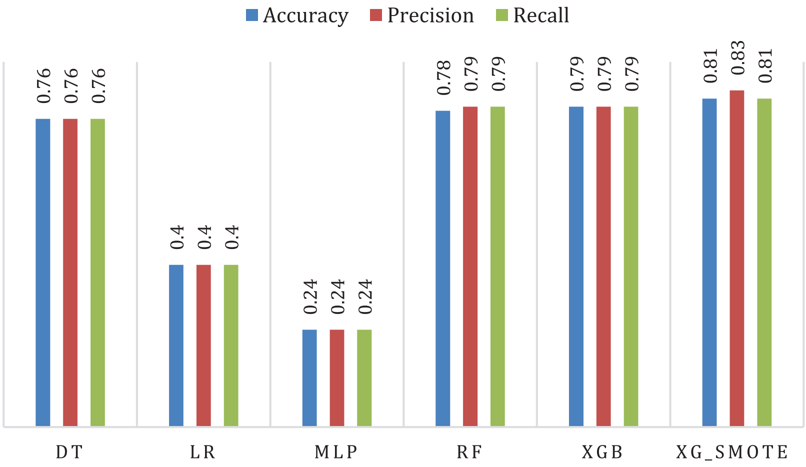


Figure 6: Performance of classification models in subcategory classification

It is clear from Fig. 6 that in the multiple classification and subclassification, the SMOTE algorithm with XGB achieved the best performance was 0.81 according to accuracy and recall and 0.83 according to the precision scale, followed by the XGB algorithm without the balancing technique 0.79 for the three measures. To evaluate the performance of the proposed model, the receiver operating characteristic curve (ROC) is used to determine the discrimination threshold for each class in the sub-multiple classification. Fig. 7 presents the ROC for each attack.

To determine the proposed method's efficiency, a comparison was made with previous studies that used the IoTID20 data set. The studies of [14,47] dealt with binary, multiple, and branching classifications, and the studies of [12,24] dealt with binary and multiple classifications, as shown in Table 3. In contrast, the studies of [27,33] dealt with binary classification; Table 3 presents the accuracy-based comparison for the three classification levels.

In comparison with previous studies, it was concluded that the accuracy was approximately 0.99 by various methods in the case of binary classification. However, in the case of multiple classifications, the study of [12] achieved 0.99 as in the proposed method. In contrast, in the case of multiple sub-classifications, the proposed method achieved the best performance with an accuracy of 0.81.

Assessment and analysis of the results showed the possibility of applying modern ML methods in IoT attack detection systems. Moreover, the results of the proposed XGB with SMOTE for multi-class subcategory classification for a binary and multi-class category can classify attacks. The results showed that DT, RF, and XGB algorithms could identify the presence of an attack at the binary classification level with high accuracy, as shown in Fig. 4. The superiorities of DT and XGB were noted in multiple classifications. In the case of multiple sub-classifications, the performance of collective learning algorithms was the best compared to DT, whereas the XGB is superior. The results indicate that boosting learning is suitable for modeling IoT attacks at the three levels. Despite the superiority of the boosting algorithm, it is still with an accuracy of 0.79. The results showed that the model's performance improved when SMOTE technique was applied to balance the data, as the accuracy reached 0.81. Compared with previous studies, the proposed system achieves better accuracy.

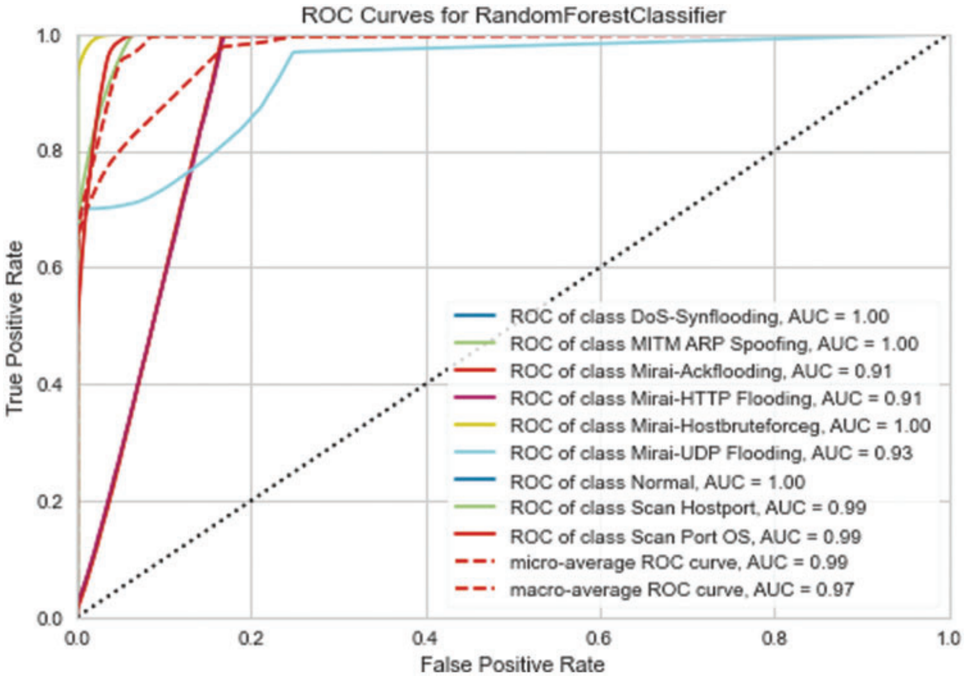


Figure 7: XGB_SMOTE ROC for each attack

Table 3: Accuracy comparison with previous studies

Author	Method	Acc of label	Acc of cat	Acc of sub_cat
Bajpai et al. [47]	XGB	0.98	0.83	0.62
Ullah et al. [14]	DCNN	0.99	0.98	0.77
Alsulami et al. [33]	XGB	0.99	–	–
Arifeen et al. [27]	DT	0.99	–	–
Dat-Thinh et al. [12]	MidSiot	0.99	0.99	–
Bhavsar et al. [24]	PCC-CNN	0.99	0.91	–
Proposed	XGB_ SMOTE	0.99	0.99	0.81

6.2 Discussion

The discussion section provides a comprehensive analysis and interpretation of the study's results. It thoroughly examines the findings' significance and implications, draws comparisons to existing literature, and addresses potential limitations and future research directions.

This study proposed a methodology utilizing XGBoost ML techniques to enhance IoT security. The methodology encompassed various preprocessing techniques for the dataset, including data cleaning, encoding, and normalization to ensure data quality and consistency. Furthermore, it tackled the challenge of imbalanced class distributions in IoT security datasets by incorporating the SMOTE.

The study's results demonstrated the proposed method's effectiveness and robustness in detecting IoT attacks. Evaluated multiple ML classifiers, including LR, MLP, DT, RF, and XGBoost. Among these classifiers, XGBoost integrated with SMOTE achieved outstanding attack detection accuracy. In binary classification, the XGBoost model achieved an accuracy of 0.99, while in multi-class classification, it achieved an accuracy of 0.99. In multiple sub-classifications, the XGBoost model achieved an accuracy of 0.81. These findings highlight the superiority of the proposed approach over existing IDS frameworks in detecting attacks in imbalanced IoT datasets.

The significance of the study lies in its contribution to addressing the challenge of imbalanced class distributions in IoT security datasets. Imbalanced datasets are common in real-world scenarios, and traditional ML algorithms often struggle to achieve accurate results in such datasets. Employing SMOTE effectively balanced the class distribution and improved the performance of the ML models.

The comparison with existing literature revealed that our approach outperformed previous studies that used the same IoTID20 dataset. For example, studies using traditional ML algorithms like DT and RF achieved lower accuracy scores compared to our proposed XGBoost model. This indicates that XGBoost is a more suitable algorithm for detecting IoT attacks in imbalanced datasets.

7 Conclusion

The study concluded that the collective learning algorithms were the best in binary and multiple classifications. In the case of subcategory classifications, the XGB algorithm is the best, and the use of the SMOTE increased the accuracy of the classification. The final model achieved 0.81 accuracies and recalled 0.83 according to the precision, which was the best comparison. Comparison of the proposed algorithms also demonstrated superiority over previous studies using the same dataset. However, the security analysis considers only a static mesh topology of IoT devices, while the IoT network is more dynamic, complicated, and diversified. As a result, statistical distribution will use to simulate the dynamic character of expansive IoT networks for future investigation. The proposed study will also pave the way for other studies on lateral movement avoidance in IoT networks.

8 Limitations and Future Work

The study primarily focuses on employing a specific ML technique, namely XGBoost, for IoT attack detection. It is worth noting that different ML algorithms may yield varied outcomes. Furthermore, the evaluation of the proposed method solely relies on a single dataset (IoTID20), necessitating further investigation into its generalizability across diverse datasets and real-world scenarios. Future work should delve into this aspect to enhance the robustness and applicability of the proposed method:

1. The study concentrated on intrusion detection at the network level, and future research could explore the integration of host-based intrusion detection techniques to bolster the overall security of IoT systems.
2. The proposed method can be regarded as real-time or near-real-time attack detection in dynamic IoT environments.

3. Research on the scalability and efficiency of the proposed is better for conducting large-scale IoT deployments with a high volume of network traffic.
4. The impact of adversarial attacks and defenses against them enhance the robustness of the proposed method in real-world scenarios.

Acknowledgement: The authors would like to thank the associate editor and the reviewers for their Time and effort were provided to review the manuscript.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Dana F Doghramachi, Siddeeq Y Ameen; data collection: Dana F Doghramachi; analysis and interpretation of results: Dana F Doghramachi, Siddeeq Y Ameen; draft manuscript preparation: Siddeeq Y Ameen. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The publicly available data set can be found at: https://ieee-dataport.org/open-access/iot-network-intrusion-dataset.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] L. Javed, B. M. Yakubu, M. Waleed, Z. Khaliq and N. G. Mato, "BHC-IoT: A survey on healthcare IoT security issues and blockchain-based solution," *International Journal of Electrical and Computer Engineering Research*, vol. 2, no. 4, pp. 1–9, 2022.

[2] L. Fan, L. He, E. Dong, J. Yang, C. Li *et al.,* "EvoIoT: An evolutionary IoT and non-IoT classification model in open environments," *Computer Networks*, vol. 219, no. 1, pp. 109450, 2022.

[3] R. Ashima, A. Haleem, M. Javaid and S. Rab, "Understanding the role and capabilities of internet of things-enabled additive manufacturing through its application areas," *Advanced Industrial and Engineering Polymer Research*, vol. 5, no. 3, pp. 137–142, 2022.

[4] M. K. Saini and R. K. Saini, "Agriculture monitoring and prediction using Internet of Things (IoT)," in *2020 Sixth Int. Conf. on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, pp. 53–56, 2020.

[5] M. I. Rosca, C. Nicolae, E. Sanda and A. Madan, "Internet of things (IoT) and sustainability," in *7th BASIQ Int. Conf. on New Trends in Sustainable Business and Consumption*, Foggia, Italy, pp. 346–352, 2021.

[6] W. Ennabigha, A. Moutabir and A. Aboudou, "The use of machine learning in the internet of things," *ITM Web of Conferences*, vol. 52, pp. 01009, 2023. https://doi.org/10.1051/itmconf/20235201009

[7] H. Maulana, R. Andriana and H. Kanai, "Development of the 3-dimensional map in the bandung regency government complex," *IOP Conference Series: Materials Science and Engineering*, vol. 662, no. 2, pp. 022113, 2019.

[8] P. Upadhyay and D. Upadhyay, "Internet of things—A survey," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 54, no. 12, pp. 417–438, 2021.

[9] M. Wazzan, D. Algazzawi, O. Bamasaq, A. Albeshri and L. Cheng, "Internet of things botnet detection approaches: Analysis and recommendations for future research," *Applied Sciences*, vol. 11, no. 12, pp. 5713, 2021.

[10] R. Valanarasu, "A review on identifying suitable machine learning approach for internet of things applications," *IRO Journal on Sustainable Wireless Systems*, vol. 3, no. 3, pp. 128–145, 2021.

[11] M. Baz, “SEHIDS: Self evolving host-based intrusion detection system for IoT networks,” *Sensors*, vol. 22, no. 17, pp. 6505, 2022.

[12] N. Dat-Thinh, H. Xuan-Ninh and L. Kim-Hung, “MidSiot: A multistage intrusion detection system for internet of things,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–15, 2022. https://doi.org/10.1155/2022/9173291

[13] S. Sohail, Z. Fan, X. Gu and F. Sabrina, “Explainable and optimally configured artificial neural networks for attack detection in smart homes,” arXiv preprint arXiv:2205.08043, 2022.

[14] S. Ullah, J. Ahmad, M. Khan, E. Alkhammash, M. Hadjouni *et al.,* “A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering,” *Sensors*, vol. 22, no. 10, pp. 3607, 2022.

[15] J. Su, S. He and Y. Wu, “Features selection and prediction for IoT attacks,” *High-Confidence Computing*, vol. 2, no. 2, pp. 100047, 2022.

[16] A. Y. Hussein, P. Falcarin and A. T. Sadiq, “Enhancement performance of random forest algorithm via one hot encoding for IoT IDS,” *Periodicals of Engineering and Natural Sciences*, vol. 9, no. 3, pp. 579–591, 2021.

[17] B. Susilo and R. F. Sari, “Intrusion detection in IoT networks using deep learning algorithm,” *Information*, vol. 11, no. 5, pp. 279, 2020.

[18] R. Shahin and K. E. Sabri, “A secure iot framework based on blockchain and machine learning,” *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 671–683, 2022.

[19] P. Radanliev and D. de Roure, “New and emerging forms of data and technologies: Literature and bibliometric review,” *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 2887–2911, 2023.

[20] P. Radanliev, D. de Roure, R. Nicolescu, M. Huth and O. Santos, “Artificial intelligence and the internet of things in Industry 4.0,” *CCF Transactions on Pervasive Computing and Interaction*, vol. 3, no. 3, pp. 329–338, 2021.

[21] T. T. H. Le, Y. E. Oktian and H. Kim, “XGBoost for imbalanced multi-class classification-based industrial internet of things intrusion detection systems,” *Sustainability*, vol. 14, no. 14, pp. 8707, 2022.

[22] T. M. Alam, K. Shaukat, H. Mahboob, M. Sarwar, F. Iqbal *et al.,* “A machine learning approach for identification of malignant mesothelioma etiological factors in an imbalanced dataset,” *The Computer Journal*, vol. 65, no. 7, pp. 1740–1751, 2022.

[23] T. Ghrib, M. Benmohammed and P. S. Pandey, “Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 950–961, 2021.

[24] M. Bhavsar, K. Roy, J. Kelly and O. Olusola, “Anomaly-based intrusion detection system for IoT application,” *Discover Internet of Things*, vol. 3, no. 1, pp. 5, 2023.

[25] S. Selvarajan and H. Mouratidis, “A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems,” *Scientific Reports*, vol. 13, no. 1, pp. 7107, 2023.

[26] W. Alhalabi, A. Al-Rasheed, H. Manoharan, E. Alabdulkareem, M. Alduailij *et al.,* “Distinctive measurement scheme for security and privacy in internet of things applications using machine learning algorithms,” *Electronics*, vol. 12, no. 3, pp. 747, 2023.

[27] M. Arifeen, A. Petrovski and S. Petrovski, “Automated microsegmentation for lateral movement prevention in industrial internet of things (IIoT),” in *2021 14th Int. Conf. on Security of Information and Networks (SIN)*, Edinburgh, UK, pp. 1–6, 2021.

[28] L. H. Al Fryan, M. I. Shomo, M. B. Alazzam and M. A. Rahman, “Processing decision tree data using internet of things (IoT) and artificial intelligence technologies with special reference to medical application,” *BioMed Research International*, vol. 2022, no. 2, pp. 8626234, 2022. https://doi.org/10.1155/2022/8626234

[29] S. M. Elghamrawy, M. O. Lotfy and Y. H. Elawady, “An intrusion detection model based on deep learning and multi-layer perceptron in the internet of things (IoT) network,” in *Int. Conf. on Advanced Machine Learning Technologies and Applications*, Huangshan, China, pp. 34–46, 2022.

[30] Y. Qi and H. Wu, "Terminal security protection system of power internet of things based on machine learning," in *2021 Int. Conf. on Applications and Techniques in Cyber Intelligence*, Fuyang, China, pp. 58–65, 2021.

[31] Kurniabudi, S. Deris, J. Darmawijoyo, I. Mohd, D. Sarjon *et al.,* "Improvement of attack detection performance on the internet of things with PSO-search and random forest," *Journal of Computational Science*, vol. 64, no. 4, pp. 101833, 2022. https://doi.org/10.1016/j.jocs.2022.101833

[32] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, pp. 29, 2023.

[33] A. A. Alsulami, Q. Abu Al-Haija and A. Tayeb, "Anomaly-based intrusion detection system for IoT networks with improved data engineering," *Artificial Intelligence and Machine Learning*, 2022. https://doi.org/10.20944/preprints202210.0431.v1

[34] S. Garg, V. Kumar and S. Rao Payyavula, "Identification of internet of things (IoT) attacks using gradient boosting: A cross dataset approach," *Telematique*, vol. 21, no. 1, pp. 6982–7012, 2022.

[35] F. Thabtah, S. Hammoud, F. Kamalov and A. Gonsalves, "Data imbalance in classification: Experimental evaluation," *Information Sciences*, vol. 513, pp. 429–441, 2020. https://doi.org/10.1016/j.ins.2019.11.004

[36] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *Journal of Big Data*, vol. 6, no. 1, pp. 1–54, 2019.

[37] A. Mahani and A. R. Baba-Ali, "Classification problem in imbalanced datasets," in *Recent Trends in Computational Intelligence*. London: IntechOpen, 2020. https://doi.org/10.5772/intechopen.89603

[38] A. Arafa, N. El-Fishawy, M. Badawy and M. Radad, "RN-SMOTE: Reduced noise SMOTE based on DBSCAN for enhancing imbalanced data classification," *Journal of King Saud University—Computer and Information Sciences*, vol. 34, no. 8, pp. 5059–5074, 2022.

[39] K. M. Dolo and E. Mnkandla, "Modifying the SMOTE and safe-level SMOTE oversampling method to improve performance," in *4th Int. Conf. on Wireless, Intelligent and Distributed Environment for Communication*, University of KwaZulu-Natal, South Africa, pp. 47–59, 2022.

[40] Q. Chen, Z. L. Zhang, W. P. Huang, J. Wu and X. G. Luo, "PF-SMOTE: A novel parameter-free SMOTE for imbalanced datasets," *Neurocomputing*, vol. 498, pp. 75–88, 2022. https://doi.org/10.1016/j.neucom.2022.05.017

[41] S. Riaz, S. Latif, S. Usman, S. Ullah, A. Algarni *et al.,* "Malware detection in internet of things (IoT) devices using deep learning," *Sensors*, vol. 22, no. 23, pp. 9305, 2022.

[42] H. Yu and A. D. Hutson, "Inferential procedures based on the weighted Pearson correlation coefficient test statistic," *Journal of Applied Statistics*, vol. 22, pp. 1–16, 2022. https://doi.org/10.1080/02664763.2022.2137477

[43] M. Coscia, "Pearson correlations on complex networks," *Journal of Complex Networks*, vol. 9, no. 6, cnab036, 2021.

[44] I. Ullah and Q. H. Mahmoud, "A scheme for generating a dataset for anomalous activity detection in IoT networks," in *Canadian Conf. on Artificial Intelligence*, Ottawa, ON, Canada, pp. 508–520, 2020.

[45] M. Douiba, S. Benkirane, A. Guezzaz and M. Azrour, "Anomaly detection model based on gradient boosting and decision tree for IoT environments security," *Journal of Reliable Intelligent Environments*, vol. 9, pp. 1–12, 2022. https://doi.org/10.1007/s40860-022-00184-3

[46] M. A. Arshed, M. A. Jabbar, F. Liaquat, U. M. Chaudhary, D. Karim *et al.,* "Machine learning with data balancing technique for IoT attack and anomalies detection," *International Journal of Innovations in Science and Technology*, vol. 4, no. 2, pp. 490–498, 2022.

[47] S. Bajpai and K. Sharma, "A framework for intrusion detection models for IoT networks using deep learning," *SN Computer Science*, 2022. https://doi.org/10.21203/rs.3.rs-2010844/v1