

Enhancing SDN security using ensemble-based machine learning approach for DDoS attack detection

Abdinasir Hirsi¹, Lukman Audah^{1,2}, Adeb Salh³, Mohammed A. Alhartomi⁴, Salman Ahmed⁵

¹Advanced Telecommunication Research Center (ATRC), Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia

²Faculty of Electrical Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia

³Faculty of Information and Communication Technology, University Tunku Abdul Rahman (UTAR), Kampar, Malaysia

⁴Department of Electrical Engineering, University of Tabuk, Tabuk, Saudi Arabia

⁵VLSI and Embedded Technology (VEST) Focus Group, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia

Article Info

Article history:

Received Jun 14, 2024

Revised Nov 5, 2024

Accepted Nov 11, 2024

Keywords:

Dataset of SDN

DDoS attacks

Ensemble machine learning

Principal component analysis

SDN security

ABSTRACT

Software-defined networking (SDN) is a groundbreaking technology that transforms traditional network frameworks by separating the control plane from the data plane, thereby enabling flexible and efficient network management. Despite its advantages, SDN introduces vulnerabilities, particularly distributed denial of service (DDoS) attacks. Existing studies have used single, hybrid, and ensemble machine learning (ML) techniques to address attacks, often relying on generated datasets that cannot be tested because of accessibility issues. A major contribution of this study is the creation of a novel, publicly accessible dataset, and benchmarking the proposed approach against existing public datasets to demonstrate its effectiveness. This paper proposes a novel approach that combines ensemble learning models with principal component analysis (PCA) for feature selection. The integration of ensemble learning models enhances predictive performance by leveraging multiple algorithms to improve accuracy and robustness. The results showed that the ensemble of random forests (ENRF) model achieved the highest performance across all metrics with 100% accuracy, precision, recall, and F1-score. This study provides a comprehensive solution to the limitations of existing models by offering superior performance, as evidenced by the comparative analysis, establishing this approach as the best among the evaluated models.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Lukman Audah

Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia

Parit Raja, 86400, Johor, Malaysia

Email: hanif@uthm.edu.my

1. INTRODUCTION

Distributed denial-of-service (DDoS) attacks are web attacks that are designed to disrupt services and deny legitimate user access [1]. These attacks overwhelm the targets with excessive traffic, causing service outages [2]. They can target various layers of the OSI model, making it versatile and challenging to mitigate [3]. DDoS methods have evolved and have become increasingly sophisticated over time [4]. High-rate DDoS attacks generate massive traffic volumes to overwhelm targets quickly, whereas low-rate DDoS attacks use minimal traffic to evade detection and gradually degrade the performance [5], [6]. High-rate attacks are easier

to detect, but cause immediate disruption, whereas low-rate attacks are stealthier and persist longer [7], [8]. Despite advancements in security, DDoS attacks remain a significant threat to software-defined networking (SDN) owing to their centralized control and programmability [9]. Attackers use handlers to control compromised systems and install malware within SDNs [10]. These compromised systems, or “zombies” form botnets that launch coordinated DDoS attacks [11].

Various solutions have been proposed, including traditional security measures, moving target defense strategies, and AI-based methods, such as machine learning (ML) and deep learning (DL) [12]. Although many studies have focused on single or hybrid ML models for DDoS detection, developing ensemble learning methods is crucial for improving accuracy [13]. In addition, studies of [14]-[18] have used generated datasets that are not publicly available, thereby limiting their reproducibility. We used a novel dataset that is publicly accessible in the Mendeley data repository, allowing for broader testing and validation [19]. The core idea of this study is to improve the detection of DDoS attacks by developing an ensemble ML framework that integrates multiple classifiers and leverages their combined strengths to improve the accuracy. It evaluates the effectiveness of traditional ML methods and incorporates principal component analysis (PCA) for optimized feature selection. The proposed approach was compared with existing DDoS detection techniques using novel and CICDDoS19 datasets. Furthermore, this study provides a robust solution for mitigating DDoS threats and contributes valuable insights and resources to the cybersecurity field. To the best of our knowledge, this study uniquely merges the assessment of various ML methods, development of an ensemble framework, and performance comparison using PCA within a single study. The main contributions of this study are as follows.

- Effectiveness assessment: evaluate the effectiveness of various machine learning methods in detecting DDoS attacks.
- Ensemble framework development: develop an ensemble-based machine learning framework that integrates multiple classifiers to enhance detection precision.
- Feature selection with PCA: employ PCA for feature selection to improve model performance by reducing dimensionality and retaining essential features.
- Novel dataset: a major contribution of this study is the creation of a novel, publicly accessible dataset that addresses reproducibility issues found in previous studies.
- Performance comparison: the performance of the proposed ensemble approach was compared with existing DDoS detection techniques using our novel publicly accessible dataset and the CICDDoS19 dataset.

The remainder of this paper is structured as follows: section 2 covers related work; section 3 discusses the proposed model development framework for SDN security; section 4 details the experimental setup and performance evaluation; and section 5 concludes the study with future work.

2. RELATED WORKS

The research community greatly appreciates its pioneering work on ML models that proactively and reactively defend against DDoS attacks in SDN environments. These mechanisms enhance network security by identifying and preventing DDoS attacks on diverse infrastructure, including wired, wireless, mobile, and sensor networks. Their research has not only advanced theory, but also practical solutions to combat these prevalent security threats. Kumar and Selvakumar [20] proposed adaptive learning mechanics to detect DDoS attacks. The ensemble approach combines multiple classifiers to reduce errors and improve detection capabilities. For detection accuracy, the KDD dataset achieved 98.2% accuracy, and the mixed traffic dataset achieved 98.8% and 99.2% on the SSENET2011 dataset. In addition, the NFBoost algorithm achieved a significantly lower false positive rate than the other methods, with an improvement of up to 78.26%. Some studies have focused on enhancing the accuracy of intrusion detection systems (IDS) in classifying traffic as normal or malicious. For example, Jabbar *et al.* [21] expounded that the random forest (RF) average one-dependence estimator (RFAODE) ensemble classifier significantly improves the accuracy and reduces the error rate of IDS compared to individual classifiers such as AODE, Naïve Bayes (NB), and RF. RFAODE achieved an accuracy of 90.51% and a false alarm rate (FAR) of 0.14% using the Kyoto dataset. The analysis used 15 of the 24 available features. Shirmarz *et al.* [22] introduced a new ensemble approach combining decision tree (DT), K-nearest neighbor (KNN), and support vector machine (SVM) techniques. This method aims to improve SDN control threats. The ensemble achieved an accuracy of 99.4%, despite the results of the individual classifiers. Additionally, the system maintained a low false-

positive rate, making it practical for real-world applications. PCA was employed to reduce the feature set from 76 to 24, thereby enhancing classifier performance. Firdaus *et al.* [23] introduced ensemble technique that integrates K-means clustering and RF classification to improve the detection accuracy of service disruption attacks in SDN environment. This study achieved a higher detection accuracy and lower false positive rate (FPR) compared to traditional methods. Experiments were conducted using specified hardware and software setups to ensure the validity of the results. Alashhab *et al.* [24] reported mitigation of overloading attacks using online ensemble method in SDN network. The prototype addresses the limitations of traditional static mechanisms by incorporating online learning approaches to adapt to evolving attack patterns in real-time. The system attained accuracy of 99.2% for any type of denial attack. Overall, their work contributes to handling zero-day, low-rate, evolving disruptive traffic. Finally, Christila and Sivakumar [25], multilayer ensemble learning was proposed to boost service attacks of an SDN controller. Multiple ensemble methods provided improved stability.

3. PROPOSED MODEL DEVELOPMENT FRAMEWORK FOR SDN SECURITY

In this section, we present the proposed model development pipeline to enhance SDN security, as shown in Figure 1. The pipeline consists of eight phases, each meticulously designed to ensure a robust and efficient model for detecting and mitigating threats in SDN environments.

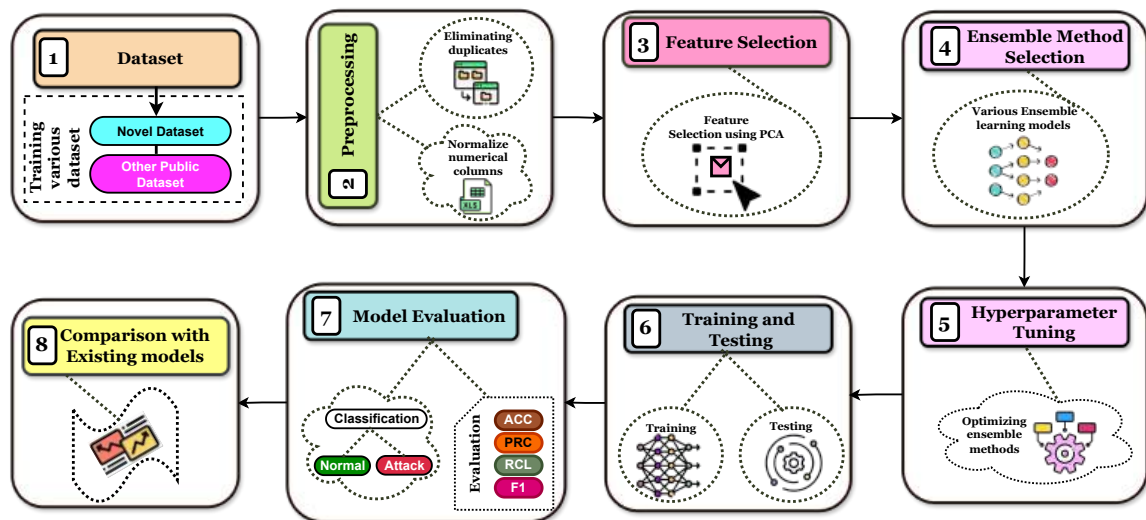


Figure 1. The proposed model development framework for SDN security illustrates the phases from dataset compilation, preprocessing, and feature selection through ensemble method selection, hyperparameter tuning, training and testing, model evaluation, and comparison with existing models

3.1. Dataset

In the first phase of the project, we collected a dataset that included both proprietary data and CICD-DoS2019 dataset. This provides a thorough overview of possible network threats and a strong basis for the next steps.

3.1.1. Generated dataset

We created a new dataset using Mininet, resulting in 1,048,757 rows and 21 columns. Our setup includes 12 switches, an RYU controller, and 24 host devices. The process involves designing a realistic network topology in Mininet, configuring it, and using an RYU controller to manage traffic. We used the MGEN and hping3 tools to generate various types of network traffic, including DDoS attacks. Flow statistics were recorded every 30 s and saved in a CSV file called “SDN-DDoS.Traffic.Dataset.csv,” which is available in Mendeley. The data were then cleaned and normalized to prepare for analysis. Table 1 outlines the DDoS attacks and features included in this dataset. In addition, Table 2 compares various generated datasets, highlighting the features, controllers, attack tools, and environments used in each study.

Table 1. Comparison of different datasets and attacks

Dataset	Attacks	Instance	No. of features
Novel dataset	TCP	350358	16
	UDP	348790	16
	ICM	349727	16
CICDDoS2019	UDP flood	3125400	21
	SYN flood	1851263	21
	UDPlag	625243	21

3.1.2. CIC-DDoS2019

Researchers often use different datasets to test DDoS attack detection models; however, some of these datasets are outdated. Furthermore, the CIC-DDoS2019 dataset is a recent and widely accepted resource for network security [26]-[29]. It includes both normal and malicious traffic and offers a comprehensive tool for evaluating DDoS detection methods. This dataset was created using CICFlowmeter v3, which extracts features such as flow duration, total forward packets, total backward packets, and packet length distribution. These features facilitate a thorough traffic analysis and enhance the effectiveness of DDoS detection models.

Table 2. Comparison of our novel dataset with other existing datasets

Ref.	Dataset	Features	Controller	Attack tools	SDN environment
[23]	InSDN	15	RYU	Hping3	Mininet using 4 OvS switches
[24]	Custom dataset	22	RYU	Scapy, Iperf, and Hping3	Mininet using 80 hosts
[25]	Custom dataset	Not mentioned	RYU	Hping3	Mininet emulator
[29]	InSDN	77	ONOS	Tcpdump, hping3, and LOIC	Mininet with 1 OvS
This paper	SDN-DDoS dataset	21	RYU	MGEN and Hping3	Mininet with 12 OvS switches

3.2. Preprocessing

During pre-processing, we cleaned and transformed the raw data. This involved handling missing values, normalizing the data, and encoding categorical variables to prepare the dataset for analysis and feature selection.

3.3. Feature selection

A critical aspect of our methodology is the selection of features used for training ML models. Given the vast amount of data generated, we encountered the challenge of limited feature space and computational complexity. The concept of a limited feature space refers to the restriction on the number of features that can be feasibly processed and analyzed owing to computational constraints and the risk of overfitting. To address this issue, we used PCA from the “sklearn.decomposition” module to select important features and reduce the dataset’s complexity [30], [31]. PCA removes redundant and irrelevant features, thereby improving model performance [32]. In our study, we configured PCA to maintain 20 key components. This is represented by (1).

$$PCA = PCA(N_{\text{ofcomponents}} = 20) \quad (1)$$

This configuration reduced to 20 features, which encapsulated the most significant variance in the data. To identify the most influential features from the original dataset, we applied the following method in (2).

$$\text{Selected_Features} = X.\text{Columns}[\text{PCA.Componentets}.\text{argmax}(\text{axis} = 1)] \quad (2)$$

This technique identifies the original features with the highest contribution to each of the 20 principal components. The “pca.components_” attribute represents the principal axes in the feature space, and “argmax(axis=1)” locates the feature with the maximum weight for each component. As a result, “selected_features” lists the most critical original features, allowing for a more focused and effective analysis. Overall, PCA offers significant benefits and assumes that the principal components capture the linear relationships among features. In cases where the underlying relationships are nonlinear, PCA may not effectively capture complex interactions, potentially leading to suboptimal feature representation. Table 3 lists the features extracted in the experiments. These features were selected to provide a comprehensive representation of the network traffic, enabling effective DDoS detection.

Table 3. Recorded features of the datasets

Extracted features
Packet count per flow, flow duration (minutes), source IP address, port bandwidth usage, aggregate duration, destination IP address, packet transmission rate, flow count, Packet in messages count, bytes per flow, port number, flow duration (seconds), total packet count, transmitted byte volume, byte accumulation, received byte volume

3.4. Ensemble method selection

The fourth phase involved selecting an appropriate ensemble method. Ensemble methods that combine the predictions of multiple models are chosen to leverage their ability to improve the accuracy and robustness over single models [33]. Various ensemble techniques were evaluated to identify the most effective approach to the dataset. RF emerged as the best-performing model for our purposes. RF operates by constructing a multitude of DT during training and outputting the class that is the mode of the classes (classification) or the mean prediction (regression) of the individual trees [34]. Ensemble of random forest (ENRF) leverages this mechanism to effectively detect DDoS attacks. Each tree is trained on a random subset of the dataset to ensure diversity among the trees. During detection, an incoming packet is passed through all decision trees, and each tree independently classifies it as either normal or abnormal. The detection process in ENRF is as follows:

- Packet evaluation: each packet is evaluated by all decision trees in the forest.
- Majority voting: each tree provides a vote on whether a packet is normal (benign) or abnormal (malicious). The final classification is determined based on the majority vote of the trees.
- Anomaly detection: by combining the outputs of multiple trees, ENRF enhances the robustness and accuracy of DDoS detection, reducing the likelihood of false positives and negatives.

Algorithm 1 effectively identifies normal and abnormal packets by learning the patterns and characteristics of benign and malicious traffic from a dataset. Specifically, the RF DDoS detection algorithm was applied to our dataset to distinguish between benign and malicious attacks, thereby demonstrating its efficacy in identifying DDoS threats. This ensemble approach ensures that the model generalizes well to unseen data and maintains a high performance in real-world scenarios. Furthermore, Figure 2 illustrates the workflow process for each received packet, detailing the steps from packet arrival to packet handling, using a Python script in the RYU controller.

Algorithm 1. Ensemble of decision trees for DDoS detection

```

1: Initialize the Ensemble: Initialize a set  $T$  of decision trees.
2: Build the Decision Trees:
3: for  $t = 1$  to  $T$  do
4:   Feature Selection: Randomly sample  $m$  features from the input features.
5:   Tree Construction: Construct a new decision tree  $D_t$  by recursively partitioning the dataset based on the selected features.
6:   At each node:
7:     Select the feature that maximizes the information gain.
8:     Continue splitting until the maximum tree depth is reached or all instances belong to the same class.
9:   Add Tree to Ensemble: Add  $D_t$  to the ensemble.
10: end for
11: Classify Instances:
12: for each instance  $x_i$  in the training set do
13:   Feature Extraction: Generate a feature vector  $z_i$  by extracting relevant features using PCA.
14:   Prediction with Trees: For each decision tree  $D_t$ , determine the class prediction  $y_{i,t}$  by following the decision path of  $x_i$ .
15:   Aggregate Predictions: Combine predictions to derive  $y_i$ :
16:   if majority of the trees predict  $y_i = 1$  then
17:     classify  $x_i$  as a DDoS instance.
18:   else
19:     classify  $x_i$  as a normal instance.
20:   end if
21: end for
22: Output the Ensemble: Provide the ensemble of decision trees as the final output.

```

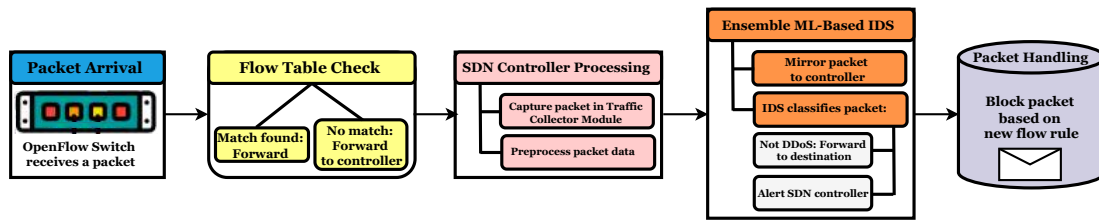


Figure 2. Workflow process for each received packet

3.5. Hyperparameter tuning

Hyperparameter tuning is critical for optimizing the performance of a selected ensemble method [35]. This phase involves systematically adjusting the hyperparameters to determine the best configuration that maximizes the predictive power of the model while avoiding overfitting. The RF classifier in this study was configured with specific hyperparameters to enhance the model performance. The model was constructed with 10 estimators, and bootstrap sampling was utilized with the Gini impurity criterion to evaluate split quality. The number of features considered at each split was set to the square root of the total number of features, with no constraints on the maximum depth of the trees. The minimum number of samples required to split a node was set to 2, and the minimum number of samples for a leaf node was 1. No minimum decrease in impurity was mandated for a split to occur. The random state was fixed at 42 to ensure reproducibility and the model was operated on a single processor. The model did not employ out-of-bag scoring or warm starts, and the default settings were used for the minimum weight fraction of leaves, maximum number of leaf nodes, class weights, and verbosity level.

3.6. Training and testing

The dataset was divided into two parts, 80% for training and 20% for testing. This ensures that the model is well trained while maintaining sufficient data for an objective evaluation.

3.7. Model evaluation

The scheme's performance was measured using metrics like accuracy, precision, recall, and F1-score to evaluate how well it detects and prevents security threats in an SDN environment.

3.8. Comparison with existing models

We compared our new system with existing ML models from recent studies. This comparison highlights the improvements and effectiveness of the proposed approach in enhancing SDN security.

4. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

We used the scikit-learn library for machine learning algorithms and performance evaluations because of its extensive range of efficient tools for data analysis. Scikit-learn, built on NumPy, SciPy, and matplotlib, offers a wide variety of advanced ML models [36]. Its well-documented API makes it easy to integrate into data processing workflows. In this study, we employed ensemble models such as RF, gradient boosting (GB), and bagging (BA) to enhance the performance by combining multiple algorithms.

4.1. Performance metrics and evaluation

We evaluated the model using various metrics, including accuracy (ACC), precision (PRC), recall (RCL), F1-score (F1), area under the curve (AUC), FPR, and true positive rate (TPR). These metrics provide a comprehensive evaluation of the performance of the model in various aspects of classification. Accuracy measures the proportion of correctly classified instances among all instances. This was calculated using in the (3).

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \quad (3)$$

The acronyms true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) represent true positives, true negatives, false positives, and false negatives, respectively. ACC was used to provide general

model correctness. PRC, also known as the positive predictive value, indicates the proportion of TP predictions among all positive predictions. It is defined as (4).

$$PRC = \frac{TP}{TP + FP} \quad (4)$$

Precision is another important parameter to measure the ability to identify actual attacks without falsely alarming benign traffic. RCL or sensitivity measures the proportion of actual positives correctly identified by the model. The equation for recall is as (5).

$$RCL = \frac{TP}{TP + FN} \quad (5)$$

Recall reflects the effectiveness of the model in identifying denial of attacks. The F1-score is the harmonic mean of the precision and recall, providing a balance between the two metrics. It is calculated as (6).

$$F1 = 2 \frac{PRC * RCL}{PRC + RCL} \quad (6)$$

The F1-score is valuable in scenarios where we need to balance precision and recall, which are essential in-service attacks to ensure both true attack detection and the minimization of false alarms. AUC represents the degree or measure of separability, showing how well the model can distinguish between classes. This was derived from the receiver operating characteristic (ROC) curve. A higher AUC indicates a better performance of the model in differentiating between the positive and negative classes. The FPR is calculated as (7).

$$FPR = \frac{FP}{FP + TN} \quad (7)$$

The TPR, or recall, is calculated as (8).

$$TPR = \frac{TP}{TP + FN} \quad (8)$$

The confusion matrix, detailed in Table 4, is a crucial component for evaluating the performance of our classification system. It delineates the results of the classification process and categorizes the outcomes into four distinct types: TP, TN, FP, and FN.

Table 4. Confusion matrix outcomes

Category	Explanation	Outcome
TP	Instances where the model correctly identifies a DDoS attack.	Successful identification of an actual DDoS attack, ensuring appropriate countermeasures are activated.
TN	Instances where the model accurately recognizes legitimate, non-attack traffic.	Accurate recognition of non-attack traffic, allowing normal operations to proceed without disruption.
FP	Instances where the model incorrectly flags normal traffic as a DDoS attack, leading to false alerts.	Incorrect identification of normal traffic as an attack, which could lead to unnecessary interventions and alert fatigue.
FN	Instances where the model fails to detect an actual DDoS attack, posing a potential security risk.	Failure to detect an attack, which can result in undetected malicious activities and potential network breaches.

4.2. Performance analysis and results

Figure 3 and Table 5 show the performance metrics (ACC, PRC, RCL, and F1-score) of the various ML models for DDoS attack detection: ENRF, fuzzy neural network (FNN), SVM, generalized linear model (GLM), NB, and XGBoost. Notable performance improvements across these models were partly due to the feature selection process using PCA. The ENRF model achieved a perfect score across all metrics (100.0%), indicating its exceptional effectiveness in distinguishing between DDoS attacks and legitimate traffic without any false positives or false negatives, making it ideal for critical security applications. The FNN model achieved an accuracy of 99.84%, precision of 96.61%, recall of 96.74%, and F1-score of 96.36%, indicating that it is suitable for environments where slight misclassifications are tolerable. The SVM model performed exceptionally well, achieving 99.92% across all metrics, making it highly effective in detecting attacks. In contrast, the

GLM model achieved 84.34% accuracy, indicating the challenges in distinguishing between attack and non-attack traffic owing to its linear nature. The NB model had an accuracy of 96.85%, with a precision of 85.33%, recall of 82.14%, and F1-score of 80.76%, suggesting a moderate performance with a higher rate of false positives. The XGBoost model also performed impressively, with 99.74% accuracy, 99.95% precision, 99.84% recall, and an F1-score of 90.15%. Despite a slight drop in the F1-score compared with ENRF and SVM, its high precision and recall, along with computational efficiency, make it compatible with large-scale SDN environments. Overall, the use of PCA for feature selection played a critical role in enhancing the performance of these models.

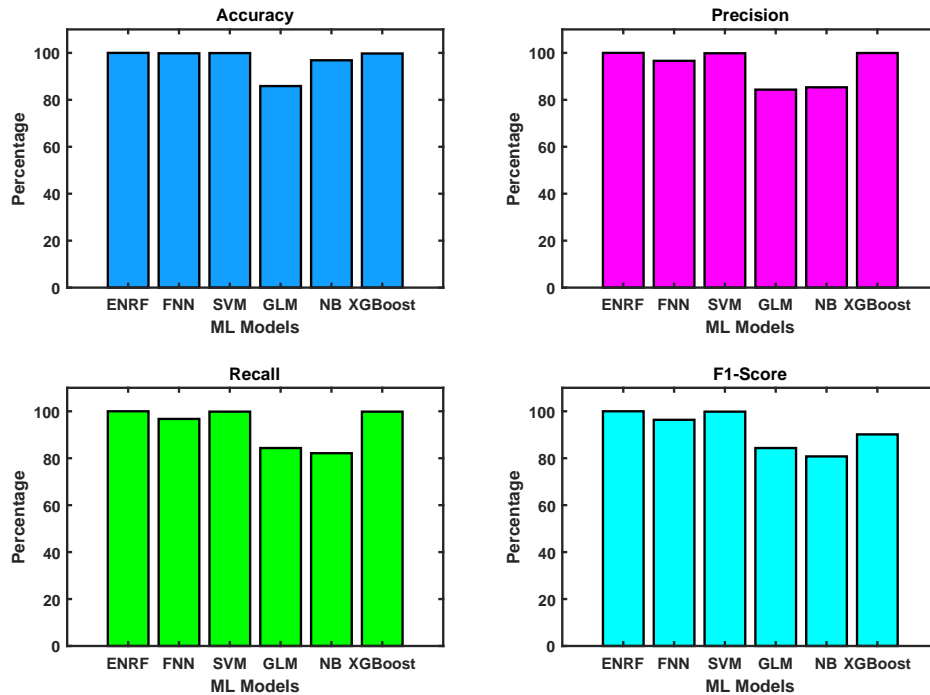


Figure 3. Performance of ENRF and other ML models for DDoS attack detection

Table 5. Performance metrics of different models

Model	Accuracy	Precision	Recall	F1-score
ENRF	100.0%	100.0%	100.0%	100.0%
FNN	99.84%	96.61%	96.74%	96.36%
SVM	99.92%	99.84%	99.84%	99.84%
GLM	85.87%	84.34%	84.34%	84.34%
NB	96.85%	85.33%	82.14%	80.76%
XGBoost	99.74%	99.95%	99.84%	90.15%

Table 6 presents the performance metrics of ensemble-based ML classifiers. The RF classifier demonstrated exceptional performance, with a recall and F1-score of 1.0, indicating flawless detection of DDoS attacks and no FN. An FPR of 0.0000 confirmed its precision, as there were no FP. Furthermore, the low testing time of 0.25364 s underscores RF's suitability of RF for real-time DDoS detection, owing to its high accuracy and efficiency. The GB classifier also performed commendably, with a recall and F1-score of 0.99, reflecting high accuracy in detecting attacks. An FPR of 0.0045 was minimal, indicating a very low rate of false alarms. Although the testing time for GB was 0.53461 s, it remained acceptable for practical applications. The slight increase in testing time was offset by its near-perfect classification performance, making GB a strong candidate for DDoS detection. BA, exhibits a recall of 0.98 and an F1-score of 0.97, which are marginally lower than those of RF and GB. An FPR of 0.0085 suggests a higher false-positive rate, leading to more false alarms. The most significant drawback of the BA is its testing time, which is substantially higher at 10.23563 s. This

extended duration could be a limitation in scenarios that require rapid detection. Despite its high accuracy, the increased computational cost and potential for more false positives may limit BA's practical use in real-time DDoS detection. Overall, the analysis revealed that RF offers the best balance between accuracy, precision, and computational efficiency, making it the most suitable for real-time applications. GB provides nearly equivalent performance with a slight increase in testing time, making it a viable alternative when precision is critical and minor delays are acceptable. Conversely, bootstrap aggregation (BA), while effective, incurs a significant computational overhead, hindering its applicability in time-sensitive environments.

Table 6. Performance metrics of ensemble based ML classifiers

Ensemble based ML classifiers	Recall	FPR	F1-score	Testing time
RF	1.0	0.0000	1.0	0.25364
GB	0.99	0.0045	0.99	0.53461
BA	0.98	0.0085	0.97	10.23563

Figure 4 presents the ROC curves for various ML models evaluated for their effectiveness in detecting DDoS attacks. The models included RF (AUC = 1.000), GB (AUC = 0.987), BA (AUC = 0.983), GLM (AUC = 0.879), SVM (AUC = 0.953), FNN (AUC = 0.929), NB (AUC = 0.970), and XGBoost (AUC = 0.930). Every curve illustrates the trade-off between the TPR and FPR for different threshold settings. The RF model confirmed perfect discrimination with an AUC of 1.000, indicating that RF can differentiate benign and malicious packets without any false positives or negatives. This performance level is optimal for critical security applications that require precision. The performance of the GB and BA models is exemplary, as evidenced by their AUC values of 0.987 and 0.983, respectively. These frameworks are acceptable for real-time DDoS detection because they balance a high TPR with a low FPR. In contrast, the GLM model, with an AUC of 0.879, showed relatively lower performance. This may be due to the linear nature of GLM, which could struggle to capture the nonlinear patterns inherent in the DDoS attack data. The SVM and FNN models, with AUC values of 0.953 and 0.929, respectively, demonstrated strong performance, but still fell short of the ensemble methods. Notably, the NB model (AUC = 0.970) and XGBoost (AUC = 0.930) also showed high effectiveness, although their slightly lower AUC values suggest a tradeoff between design simplicity and computational efficiency. Overall, our results highlight the critical role of advanced ML techniques in enhancing network security and mitigating risks associated with DDoS attacks.

Figure 5 depicts the performance metrics of the RF model on the novel and CIC-DDoS2019 datasets. The model achieved perfect scores across all metrics for both datasets, with values of 1.0 for ACC, PRC, RCL, F1-score, and AUC. This indicates that the RF accurately identified DDoS attacks and normal traffic without errors. Moreover, the model performed well on both datasets, thereby demonstrating its reliability and adaptability. Such performance is essential for real-time DDoS detection systems to maintain accuracy and avoid false alarms, thereby ensuring timely threat mitigation.

4.3. Comparative analysis of DDoS detection techniques

Table 7 presents a summary of several schemes, showing key performance metrics, such as ACC, PRC, RCL, and F1-score. NFBBoost, as referenced in [20], confirmed an accuracy of 98.2%. The REAODE model in [21] has an accuracy of 90.51%. According to [22], the boosting ensemble classifier achieved an accuracy of 99.4%. The authors in [23] do not provided the custom dataset. The researches [20]-[23] did not specify the precision, recall, and F1-score for this model. They indicated a strong performance in terms of accuracy, but the lack of information on other metrics leaves a gap in fully evaluating the model's efficiency in distinguishing between attack and non-attack scenarios. Alashhab *et al.* [24], the ensemble online model boasts an accuracy of 99.2%, with precision, recall, and F1-scores at 98.78%, 98.81%, and 98.78% respectively. Christila and Sivakumar [25], an accuracy of 99.42% was achieved. Our ENRF method surpassed all the other models, achieving 100% ACC, PRC, RCL, and F1-scores. This validates that the ENRF model is highly reliable and effective for detecting DDoS attacks, making it the strongest solution among those compared. The critical analysis shows that the reason behind achieving a perfect score is that ENRF utilizes PCA for feature selection, which effectively reduces the dimensionality of the dataset while retaining the most significant features. This minimizes noise and improves the focus of the model on relevant data. In addition, the power of the ensemble, by combining multiple RF, enhances the accuracy by aggregating the predictions of numerous

decision trees, thereby reducing the likelihood of overfitting to any particular dataset. Systematic tuning of hyperparameters, such as the number of estimators, max depth, and criterion for splitting, ensures that the RF classifiers are optimized for the best performance. In future work, the focus will be on ensuring that the novel dataset comprehensively covers all the possible DDoS attack scenarios.

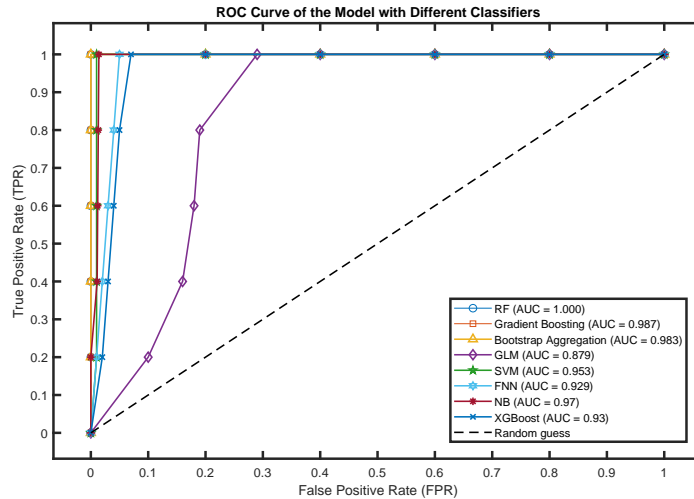


Figure 4. ROC curves for various machine learning models on a novel DDoS detection dataset

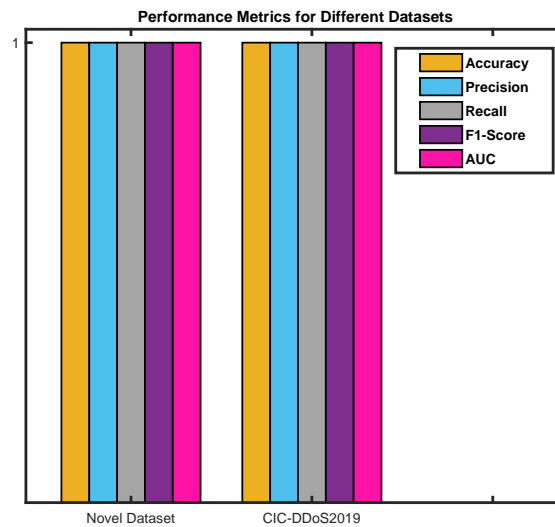


Figure 5. Performance metrics for the RF model on two datasets (novel dataset and CIC-DDoS2019)

Table 7. Comparison of DDoS attack detection models. * stands for not specified

Model with reference	Accuracy	Precision	Recall	F1-score
NFBoost [20]	0.982 - 0.992	*	*	*
RFAODE [21]	0.9051	*	*	*
Boosting ensemble classifier [22]	0.993	0.993	*	0.996
Ensemble K-means and RF [23]	1.0	1.0	1.0	1.0
Ensemble online [24]	0.992	0.9878	0.9881	0.9878
MEDR-DDoSAD [25]	0.9942	0.9938	0.9942	0.9940
Proposed model-ENRF	1.0	1.0	1.0	1.0

5. CONCLUSION

The ENRF algorithm stands out as the optimal solution for mitigating DDoS attacks in SDN control planes. The method uses several decision trees to increase detection accuracy. On the other hand, ENRF can resist overfitting to become an effective approach for detecting complex patterns associated with DDoS attacks. Most studies used unique datasets that are not publicly available, making it difficult for others to test and verify their results. This research ensures that both the generated and other public datasets are utilized to test different models. The proposed framework can be adapted to verify attack patterns and network behavior. Furthermore, the integration of the ENRF technique within the SDN control plane ensures the continuous monitoring and rapid detection of anomalous activities, effectively mitigating potential threats before escalating. Future work will extend this dataset to include diverse real-world network scenarios. This will improve the adaptability to new threats. Additionally, innovative feature selection methods using PCA will be explored to optimize the input features and boost the overall performance and efficiency. These efforts are aimed at providing effective and reliable protection against DDoS attacks from SDN environment.

ACKNOWLEDGEMENTS

This research was supported by Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2022/TK07/UTHM/02/25).





REFERENCES

- [1] M. Gniewkowski, "An overview of DoS and DDoS attack detection techniques," in *International Conference on Dependability and Complex Systems*, 2020, pp. 233–241, doi: 10.1007/978-3-030-48256-5_23.
- [2] A. B. de Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: challenges, open issues and opportunities," *Computer Networks*, vol. 222, p. 109553, 2023, doi: 10.1016/j.comnet.2022.109553.
- [3] S. Sambangi and L. Gondi, "A machine learning approach for ddos (distributed denial of service) attack detection using multiple linear regression," in *Proceedings*, 2020, vol. 63, no. 1, p. 51, doi: 10.3390/proceedings2020063051.
- [4] A. Benmoussa et al., "MSIDN: Mitigation of sophisticated interest flooding-based DDoS attacks in named data networking," *Future Generation Computer Systems*, vol. 107, pp. 293–306, 2020, doi: 10.1016/j.future.2020.01.043.
- [5] A. H. B. Alghuraibawi, R. Abdullah, S. Manickam, and Z. A. A. Alyasseri, "Detection of ICMPv6-based DDoS attacks using anomaly based intrusion detection system: a comprehensive review," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, p. 5216, Dec. 2021, doi: 10.11591/ijece.v11i6.pp5216-5228.
- [6] A. A. Alashhab et al., "A survey of low rate DDoS detection techniques based on machine learning in software-defined networks," *Symmetry*, vol. 14, no. 8, p. 1563, Jul. 2022, doi: 10.3390/sym14081563.
- [7] C. Kannan, R. Muthusamy, V. Srinivasan, V. Chidambaram, and K. Karunakaran, "Machine learning based detection of DDoS attacks in software defined network," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 32, no. 3, p. 1503, Dec. 2023, doi: 10.11591/ijeecs.v32.i3.pp1503-1511.
- [8] A. A. Alashhab, M. S. M. Zahid, A. Muneer, and M. Abdullahi, "Low-rate DDoS attack detection using deep learning for SDN-enabled IoT networks," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 11, p. 371, 2022, doi: 10.14569/IJACSA.2022.0131141.
- [9] L. Bagdadi and B. Messabih, "Distributed denial of service attacks classification system using features selection and ensemble techniques," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 34, no. 3, pp. 1868–1878, 2024, doi: 10.11591/ijeecs.v34.i3.pp1868-1878.
- [10] P. Gulihar and B. B. Gupta, "Cooperative mechanisms for defending distributed denial of service (DDOS) attacks," *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 421–443, 2020, doi: 10.1007/978-3-030-22277-2_16.
- [11] M. Cirillo, M. Di Mauro, V. Matta, and M. Tambasco, "Botnet identification in DDoS attacks with multiple emulation dictionaries," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3554–3569, 2021, doi: 10.1109/TIFS.2021.3082290.
- [12] A. H. Abdi et al., "Security control and data planes of SDN: a comprehensive review of traditional, AI and MTD approaches to security solutions," *IEEE Access*, vol. 12, pp. 69941–69980, 2024, doi: 10.1109/ACCESS.2024.3393548.
- [13] A. Saritha, B. R. Reddy, and A. S. Babu, "QEMDD: quantum inspired ensemble model to detect and mitigate DDoS attacks at various layers of SDN architecture," *Wireless Personal Communications*, vol. 127, no. 3, pp. 2365–2390, 2022.
- [14] K. S. Sahoo et al., "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020, doi: 10.1109/ACCESS.2020.3009733.
- [15] M. M. Raikar, S. Meena, M. M. Mulla, N. S. Shetti, and M. Karanandi, "Data traffic classification in software defined networks (sdn) using supervised-learning," *Procedia Computer Science*, vol. 171, pp.2750–2759, 2020, doi: 10.1016/j.procs.2020.04.299.
- [16] J. A. Perez-Diaz, I. A. Valdovinos, K.-K. R. Choo, and D. Zhu, "A flexible SDN-based architecture for identifying and mitigating low-rate ddos attacks using machine learning," *IEEE Access*, vol. 8, pp. 155 859–155 872, 2020, doi: 0.1109/ACCESS.2020.3019330.
- [17] K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj, and P. Chinnasamy, "Detection of distributed denial of service attacks in SDN using machine learning techniques," in *2021 international conference on Computer Communication and Informatics (ICCCI)*, *IEEE*, 2021, pp. 1–5, doi: 10.1109/ICCCI50826.2021.9402517.
- [18] J. Bhayo et al., "Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks," *Engineering Applications of Artificial Intelligence*, vol. 123, p. 106432, 2023, doi: 10.1016/j.engappai.2023.106432.





- [19] A. Hirsi, L. Audah, and A. Salh, "SDN-DDoS traffic dataset," Mendeley Data, 2024, [Online]. Available: <https://data.mendeley.com/datasets/b7vw628825/1>.
- [20] P. A. R. Kumar and S. Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems," *Computer Communications*, vol. 36, no. 3, pp. 303–319, 2013, doi: 10.1016/j.comcom.2012.09.010.
- [21] M. A. Jabbar *et al.*, "RFAODE: a novel ensemble intrusion detection system," *Procedia computer science*, vol. 115, pp. 226–234, 2017, doi: 10.1016/j.procs.2017.09.129.
- [22] A. Shirmarz, A. Ghaffari, R. Mohammadi, and S. Akleylek, "DDoS attack detection accuracy improvement in software defined network (SDN) using ensemble classification," in *2021 International Conference on Information Security and Cryptology (ISC-TURKEY)*, 2021, pp. 111–115, doi: 10.1109/ISCTURKEY53027.2021.9654403.
- [23] D. Firdaus, R. Munadi, and Y. Purwanto, "DDoS attack detection in software defined network using ensemble k-means++ and random forest," in *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, 2020, pp. 164–169, doi: 10.1109/ISRITI51436.2020.9315521.
- [24] A. A. Alashhab *et al.*, "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model," *IEEE Access*, vol. 12, pp. 51630–51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
- [25] S. A. Christila and R. Sivakumar, "Multi-layer ensemble deep reinforcement learning based DDoS attack detection and mitigation in cloud-SDN environment," in *2022 4th International Conference on Circuits, Control, Communication and Computing (I4C)*, pp. 451–455, 2022, 10.1109/I4C57141.2022.10057641.
- [26] H. J. Hadi, U. Hayat, N. Musthaq, F. B. Hussain, and Y. Cao, "Developing realistic distributed denial of service (DDoS) dataset for machine learning-based intrusion detection system," in *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2022, pp. 1–6, doi: 10.1109/IOTSMS58070.2022.10062034.
- [27] A. A. Najjar *et al.*, "A robust DDoS intrusion detection system using convolutional neural network," *Computers and Electrical Engineering*, vol. 117, p. 109277, 2024, doi: 10.1016/j.compeleceng.2024.109277.
- [28] S. Rajagopal, P. P. Kundapur, and K. S. Hareesha, "Towards effective network intrusion detection: from concept to creation on Azure cloud," *IEEE Access*, vol. 9, pp. 19723–19742, 2021, doi: 10.1109/ACCESS.2021.3054688.
- [29] M. S. Elsayed, N.-A. Le-Khac, and A. D. Jurcut, "InSDN: a novel SDN intrusion dataset," *IEEE Access*, vol. 8, pp. 165263–165284, 2020, doi: 10.1109/ACCESS.2020.3022633.
- [30] M. S. El Sayed, N.-A. Le-Khac, M. A. Azer, and A. D. Jurcut, "A flow-based anomaly detection approach with feature selection method against ddos attacks in sdns," *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1862–1880, 2022, doi: 10.1109/TCCN.2022.3186331.
- [31] S. K. Dash *et al.*, "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal*, vol. 25, p. 100450, 2024, doi: 10.1016/j.eij.2024.100450.
- [32] M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," *Computers and Security*, vol. 88, p. 101645, 2020, doi: 10.1016/j.cose.2019.101645.
- [33] M. A. Hossain and M. S. Islam, "An ensemble-based machine learning approach for botnet-based DDoS attack detection," in *2023 IEEE International Conference on Telecommunications and Photonics (ICTP)*, 2023, pp. 1–5, doi: 10.1109/ICTP60248.2023.10490528.
- [34] Y. Wei and Y. Sekiya, "Sufficiency of ensemble machine learning methods for phishing websites detection," *IEEE Access*, vol. 10, pp. 124103–124113, 2022, doi: 10.1109/ACCESS.2022.3224781.
- [35] E. Elgeldawi, A. Sayed, A. R. Galal, and A. M. Zaki, "Hyperparameter tuning for machine learning algorithms used for arabic sentiment analysis," in *Informatics*, 2021, vol. 8, no. 4, p. 79, doi: 10.3390/informatics8040079.
- [36] S. Raschka, J. Patterson, and C. Nolet, "Machine learning in python: main developments and technology trends in data science, machine learning, and artificial intelligence," *Information*, vol. 11, no. 4, p. 193, Apr. 2020, doi: 10.3390/info11040193.

BIOGRAPHIES OF AUTHORS






Abdinasir Hirsi (Graduate Student Member, IEEE)     holds a B.S. degree in telecommunication engineering from the Mohammad Ali Jinnah University (M.A.J.U), Karachi, Pakistan, which he received in 2019. He also obtained an M.S. degree in electrical engineering, specializing in communication engineering, from Bahria University, Karachi, Pakistan, in 2021. Currently, he is pursuing a Ph.D. degree in electrical engineering at Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia. His research interests include software-defined networking (SDN) security, DDoS attack detection and mitigation, cybersecurity, AI techniques such as ML and DL techniques for network intrusion detection. He can be contacted at email: enr.abdinasir@gmail.com.






Lukman Audah (Member IEEE)     received the Bachelor of Engineering degree in Telecommunications from the Universiti Teknologi Malaysia, in 2005, and the M.Sc. degree in communication networks and software and the Ph.D. degree in electronic engineering from the University of Surrey, U.K. He is currently a Senior Lecturer with the Communication Engineering Department, Universiti Tun Hussein Onn Malaysia. His research interests include wireless and mobile communications, internet traffic engineering, network system management, data security, and satellite communications. He can be contacted at email: hanif@uthm.edu.my.




Adeb Salh (Member IEEE)    received a Bachelor of Electrical and Electronic Engineering degree from IBB University, Yemen, in 2007, and masters and Ph.D. degrees in electrical and electronic engineering from the University Tun Hussein Onn Malaysia, in 2015 and 2020, respectively. From 2007 to 2012, he worked as a Lecturer Assistant with the Yareem Community College. From 2020 to 2023 he worked as a Postdoctoral Researcher at UTHM and UTM respectively. Currently working as an Assistant Professor at Universiti Tunku Abdul Rahman, Faculty of Information and Communication Technology. His research interests include 5G, 6G wireless communications, massive MIMO, artificial intelligence (AI), and the IoT. He can be contacted at email: adebali@utar.edu.my.



Mohammed A. Alhartomi (Member IEEE)    received the Ph.D. degree in electronic and electrical engineering from Leeds University, U.K., in 2016. He is currently an Assistant Professor with the Department of Electrical Engineering, University of Tabuk. His research interests include wireless and mobile communications, signal processing, optical wireless systems design, and visible light communications. He can be contacted at email: malhartomi@ut.edu.sa.



Salman Ahmed (Graduate Student Member IEEE)    received a Bachelor's in Electronic Engineering from Mehran University of Engineering and Technology Jamshoro, Pakistan, in 2015 and a Master of Engineering in Industrial Automation and control from Quaid e Awam University of Science and Technology Nawabshah, Pakistan, in 2021. He is currently pursuing his Ph.D. degree and working as a graduate research assistant (GRA) at the Faculty of Electrical and Electronics Engineering, Universiti Tun Hussein, Malaysia (UTHM). He worked as a lecturer in Electronics Engineering in Sukkur IBA University, Pakistan, from 2017 to 2022. His research interests include network security, cryptographic, and resource-constrained IoT devices. He can be contacted at email: he220025@student.uthm.edu.my.