Ensemble Learning Approach for Robust Cyberattack Detection in Heterogeneous IoT Networks

OPEN ACCESS

Volume: 13

Special Issue: 3

Month: February

Year: 2026

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Citation:
Raja, A. Ambeth, et al. "Ensemble Learning Approach for Robust Cyberattack Detection in Heterogeneous IoT Networks." *Shanlax International Journal of Arts, Science and Humanities*, vol. 13, no. 3, 2026, pp. 22–31.

DOI:
https://doiorg/10.34293/sijash.v13iS3-i1-Feb.10257

Dr. A. Ambeth Raja
Associate Professor
PG & Research Department of Computer Science
Thiruthangal Nadar College, India

Mrs. Samundeeswari
Research Scholar
PG & Research Department of Computer Science
Thiruthangal Nadar College, India

Dr. V. Devi
Professor
PG & Research Department of Computer Scienc,
Thiruthangal Nadar College, India

Mrs. S. Jayasutha
Assistant Professor
Department of Criminology and Criminal Justice Science
Thiruthangal Nadar College, India

Abstract

Although rapid development of IoT (Internet of Things), the security issues are becoming serious in recent years because of its heterogeneous traffic with diverse behaviors and highly dynamic traffic pattern. This paper presents a robust and adaptive Weighted Ensemble Learning (WELL) framework to detect the intrusion of IoT networks, which combines systematically data preprocessing, correlation, based feature selection, ensemble of complementary multiple classifiers (RF, XGBoost, SVM and KNN) based weighted voting, and is evaluated by the contemporary resilient CICIoT2023 data, set containing different IoT traffic types and various attacks (DoS, DDoS, Malware, Scanning etc.). It is demonstrated that our ensemble model successfully exceeded all individual classifiers in terms of accuracy of 98.1% and F1 score of 0.981, while still kept an extremely low false alarm rate of 1.6%. It can detect complicated attack from heterogeneous traffic with low false positive rate and adaptively adapt to dynamic traffic patterns. This trusted and scalable reliable system can promise in real time application and shows great potential of ensemble method to boost reliability and efficiency in IoT networks.

Keywords: Internet of Things (IoT), Machine Learning, Security, Detection

Introduction

The tremendous expansion of the Internet of Things (IoT) has revolutionized today's digital environment, enabling the interconnection of smart devices, sensors, and cyber-physical systems among various domains like health-care, smart city, industrial

automation, intelligent transportation and etc. In a massive scale. Although the IoT architectures deliver unmatched operating efficiency and real-time information exchange, they present numerous security threats to smart devices and their interconnected networks due to their intrinsic heterogeneity, resource limitations, distributed nature [1-3]. The major threats on the IoT network consist of denial-of-service (DoS) attacks, botnet propagation, data extraction, spoofing attacks, and infiltration of malicious programs which severely impact system availability, user privacy, and safety of critical infrastructure. To build and ensure the security of heterogeneous IoT systems, an efficient and robust intrusion detection system (IDS) is indispensible [4-6].

Traditional security tools, including firewalls and signature-based intrusion detection systems (SIDS), cannot accommodate dynamic attacks of IoT traffic patterns, nor the high dimensional and volatile traffic characteristics. In addition, IoT traffic behaviors can be affected by numerous factors including the device type, protocol used, and the application in use; resulting in a multitude of complex network behaviors due to varying heterogeneity of IoT devices and hence static rules cannot provide good detection against these features of intrusions [10]. Machine learning methods have been proposed to be the main technique for automating the anomaly detection process and classification of cyber-attacks by being able to identify features of network traffic, learning patterns of the normal behavior, and hence anomalies of normal behavior can indicate malicious traffic [7-9].

Many works addressed single-model ML and deep learning techniques such as decision trees, support vector machine, CNN, recurrent neural networks in IoT intrusion detection, however although they achieve good results in controlled circumstances they tend to perform poorly against skewed traffic distributions, noisy data, and unseen attack types. Models like individual classifiers possess high bias of models, are prone to feature distribution changes, and may overfit in practical IoT scenario. It is also worth noticing that IoT datasets usually have class imbalance and are susceptible to ambiguous attack signatures[10-12].

Ensemble learning has garnered significant attention as a valuable framework for achieving better prediction accuracy and robustness by merging together different weak learners into a collective learning architecture. Various classifiers combined with unique learning schemes help in reducing both variance and bias and ultimately generalizing better to a heterogeneous dataset. Methods like bagging, boosting, stacking, weighted voting etc., outperformed simple learning techniques in different cybersecurity applications, since they can encode the sophisticated attack pattern more efficiently than individual learning techniques [13-15]. Notwithstanding their advantages, however, ensemble-based intrusion detection in heterogeneous IoT network has been inadequately studied and there is room for improvement in feature representation and designing effective tradeoff between detection sensitivity and computational cost, feasible for real-time operation.

To overcome the problems mentioned, this paper focuses on a hybrid ensemble learning based cyber-attack detection framework for heterogeneous IoT networks. This system combines diverse decision boundary-enabled multiple classifiers in order to increase the capability of intrusion identification for different kinds of traffic profiles. An additional preprocessing and feature optimization pipeline is introduced to handle noisy, redundant, and unbalanced data in order to produce a more trustworthy system. Weighted voting is applied to ensemble the outcomes of the several individual classifiers to obtain the maximal detection accuracy and least number of false alarms. Large scale experiments on standard IoT intrusion datasets are performed to evaluate performance of proposed framework compare to others state of the art.

The main contributions of this study are summarized as follows:

- To develop a robust ensemble based intrusion detection framework for heterogeneous IoT environments.

- Combine different machine learning classifiers to improve the accuracy and generalization ability for attack detection.
- The implementation of feature selection and balancing methods for increased stability of detection.
- A thorough performance evaluation on diverse cyberattack types and through standard performance indexes.

The remainder of this paper is organized as follows. Section 2 reviews related work on IoT intrusion detection and ensemble learning techniques. Section 3 describes the proposed ensemble-based detection framework in detail. Section 4 presents the experimental setup and performance evaluation results. Section 5 discusses the findings and comparative analysis, and Section 6 concludes the paper with future research directions.

Related Work

In the realm of IoT networks, machine and deep learning have been instrumental in solving the problem of intrusion detection that is ever more dynamic and heterogeneous. Recently, researches have been concerned with smart traffic analysis, hybrid architectures, and ensemble decision making.

In 2025, Kharoubi et al. Have proposed an intrusion detection system (NIDS-DL-CNN) based on convolutional neural networks in IoT security domain. In this approach, deep features from network traffic flows are extracted to classify malicious events accurately without human intervention. Although they have proved that CNN is a capable model in capturing spatial correlations in traffic flows, using only one deep model made it difficult to cope with data distribution changes and new types of attacks.

Jose & Jose (2023) researched deep learning for intrusion detection on the CIC-IDS2017 dataset, with a set of different neural network architectures to identify types of attack. Jose & Jose (2023) demonstrated that deep learning algorithms outperform the conventional machine learning methods when attempting to distinguish the intricate patterns in intrusions. However, it became apparent that due to their computational intensive nature, deep learning algorithms may be problematic to apply and deploy in a time-sensitive IoT environment with limited computational resources.

As a consequence of the shortcomings of single classifier, ensemble learning approaches have been extensively studied. Comparative study on different ensemble learning machine learning models combined with feature selection for network intrusion detection was conducted by Das et al. (2021). Experimental results showed that ensemble classifiers performed much better than single classifier in detection accuracy and false positives. However, these methods were tested mainly on traditional network environment with no attention on characteristics of heterogeneous IoT traffic.

Multiple machine learning techniques were benchmarked by Maseer et al. (2021) for anomaly-based Intrusion Detection against the CICIDS2017 dataset, showing tree-based models and ensembles performed consistently well. The authors highlight that feature selection is critical to increase robustness. The article does not mention issues specific to the heterogeneous environment of an IoT, or real-time constraints.

In the recent researches hybrid deep learning and ensemble intelligence has been combined to further enhance the capabilities of IDS framework. Hybrid deep learning architectures along with ensemble learning has been implemented on a hybrid CNN-LSTM model for detecting intrusions in IoT on heterogeneous data by Nazir et al (2025). An experimental study indicated better performance in identifying time dependent patterns along with generalized prediction. However the hybrid deep learning architecture introduced significant complexity and heavy computation costs for lightweight IoT implementations.

To address the detection of intrusion in the IoT networks, Azzarini et al. (2023) presented a stacking ensemble deep learning model. The proposed architecture was used for consolidating

the outputs from diverse deep architectures resulting in effective attack classification and better stability for handling noise. While this approach showed promising detection results, it was not practical to implement in large scale or in real time IoT environments due to its relatively high training cost and inference delay because of the multiplicity of deep learners.

Likewise, Rashid et al. (2022) recommended using tree-based stacking ensemble with feature selection method in the intrusion detection system and proved its effectiveness by attaining better classification stability and dimensionality reduction. In line with, it was reported that the combination of ensembles and selected optimal feature subsets were effective, although this framework was only evaluated on traditional network data and did not take the diversity of IoT traffic pattern into consideration.

Talukder et al. (2023) presented a hybrid machine learning model that integrated various classifiers for more reliable detection. The technique boosted the detection of different kinds of attacks, especially insensitive to data imbalance. However, the hybrid model does not cater to heterogeneous IoT environment, and did not apply any adaptively weighting strategy to contribute to different classifiers..

Research Gap and Motivation

Although existing literature reveals the effectiveness of deep learning, hybrid architectures and ensemble methods for IDS, a number of issues remain outstanding. Primarily, most techniques use computationally expensive deep models that cannot run on resource-limited IoT devices. Also, many of ensemble architectures are tested on standard network datasets and barely take into account for varied IoT traffic pattern and different type of device characteristics. Apart from that, most of the proposed techniques utilize fixed ensemble methods with no dynamic weighting scheme for the classifier contributions to each type of intrusion, thereby results in inferior generalization capability.

These limitations are met in this study, which presents an efficient ensemble learning-based intrusion detection system, especially suited for heterogeneous IoT networks. A combination of lightweight, yet mutually compatible machine learning classifiers, together with effective feature selection and weighted decision fusion, is envisioned to offer the high detection accuracy, and low false alarm rates needed for a real-time IoT security context.

Proposed Ensemble-Based Intrusion Detection Framework

The architecture and the operation workflow of the presented ensemble-learning based intrusion detection framework for offering effective cyberattack detection in heterogeneous IoT environment are given in this section. In this framework, the optimal data preprocessing, discriminative feature selection, and several supplementary machine learning classifiers are combined by a weighted decision fusion scheme. The goal is to improve accuracy, generalization ability and efficiency.

System Architecture Overview

The presented system architecture has five main modules: (i) IoT traffic acquisition, (ii) Data preprocessing, (iii) Feature optimization, (iv) Construction of Ensemble Classifier, and (v) Weighted fusion of attack decisions. In the IoT, large numbers of heterogeneity traffic streams is produced from IoT devices and collected from network gateways or observation nodes. The acquired traffic flows are then converted to feature vectors that can be analyzed by the intelligent system.

During the first phase, IoT traffic acquisition can be made either by the distributed monitoring nodes, the edge gateways or the central network collector. These elements continuously collect the communication flows among all the interconnected devices. Since IoT traffic is heterogeneous, the

data collected presents heterogeneous protocols, sizes of packets, frequencies of transmission and characteristic behaviors from different devices. Each raw traffic flow is converted into structured feature vectors comprising of statistical, temporal and protocol-level attributes such as duration of flow, interarrival of packets, distribution of bytes, state and flags of connection, etc.

In the second stage, the data is preprocessed, which is an important part to improve the quality of the data and to ensure features are uniformly represented. IoT traffic data has a variety of types of anomalies such as null values, outliers, duplicate attributes and imbalance attack classes which severely impact on the learning performance. Data preprocessing in this case involves imputation of missing entries with statistical methods, identification and correction of anomalous values through the use of thresholds, conversion of traffic features from categorical to numerical types for use in algorithms and application of min-max normalization to put all the features into a common range that prevents dominant features from influencing the learning process. Resampling techniques, such as SMOTE or weighted learning methods, can be applied to address the issue of imbalanced attack classes and ensure the ability to identify all kinds of intrusion categories.

The third part of framework is feature optimization, that aims to reduce dimensions while retaining discriminative information. Due to the large dimensions of traffic data, many features can be redundant and contain noise. That increases computation burden and the tendency of over fitting. The relevance of features and their inter-dependencies is assessed by analyzing correlation and mutual information among features. Selected highly correlation to attack label features that have less redundancy contribute to form the optimized feature subset, thereby increasing efficiency and training speed and ability to generalize in diverse traffic.

The construction of the ensemble classifier in the fourth stage involves independent training of a diverse set of machine learning classifiers using the best-set of features. Different classifiers represent varied decision boundaries and viewpoints on the data and learn comprehensive representations of intrusion patterns. Trees provide non-linear representation, boost weak predictors, margin-based methods handle large dimensional separation well, and instance-based methods capture local deviations from expected patterns. Diversity among learners is essential for detection performance robustness against drift in attack patterns.

The last step does a weighted fusion of attacks decision to get an intrusion prediction. Unlike a straightforward majority voting approach, each classifier's contribution to the fusion depends on its performance during validation, allowing highly accurate models to have a dominant influence over the decision. By merging classifier decisions based on weights which are relative to their individual validation results, we reduce potential misclassifications and noisy outputs. Hence, through adaptive fusion, the framework yields a highly accurate and stable intrusion detection mechanism that is immune to fluctuations of IoT traffic.

Data Preprocessing and Normalization

In IoT networks raw traffic data can suffer from missing data, outliers, and feature distribution shift which negatively impact the training phase. The model training will depend on the following pre-processing steps:

1. Data Cleaning: The missing values are imputed using one imputation method among those in the list of statistical imputation (mean, median, mode). Outliers are determined using IQR rule and clipped to range.
2. Categorical Encoding: Non-numerical traffic attributes are converted into numerical representations using label encoding or one-hot encoding.
3. Feature Scaling: To ensure uniform learning behavior across classifiers, min–max normalization is applied:

$$x_i^{norm} = \frac{x_i - x_{min}}{x_{max} - x_{min}}$$

where x_i denotes the original feature value, and x_{min} and x_{max} represent the minimum and maximum values of the feature.

4. Class Balancing: Synthetic minority oversampling or weighted sampling is employed to mitigate class imbalance commonly present in IoT intrusion datasets.

Feature Selection and Optimization

The computation costs rise rapidly with high dimension traffic data and the potential exist for the occurrence of redundant and/or irrelevant attributes. CFS (Correlation-based feature selection) algorithm and mutual information analysis are combined together to achieve discriminative attributes.

The relevance of each feature f_i with respect to class label C is quantified using mutual information:

$$MI(fj,C) = \sum_{f_j \in F} \sum_{C \in Y} P(f_j, C)\ log\left(\frac{P(f_j, C)}{P(f_j)\ P(C)}\right)$$

Features with high relevance and low inter-correlation are retained to form the optimized feature subset F*. This process improves detection stability and reduces training overhead.

Ensemble Classifier Construction

To exploit diverse learning characteristics, four complementary machine learning classifiers are incorporated:

- Random Forest (RF): Utilize bagging and the aggregation of decision trees to capture nonlinear relationships and accommodate noise.
- Extreme Gradient Boosting (XGBoost): Enhances weak learners through sequential boosting to improve complex pattern recognition.
- Support Vector Machine (SVM): Constructs optimal hyperplanes for high-dimensional traffic classification.
- k-Nearest Neighbor (kNN): Provides instance-based learning for localized attack pattern detection.

Each classifier M_k is trained independently using the optimized feature set F* to produce predicted class labels:

$$\hat{y}_k = M_k(F^*)$$

where k=1,2,...,K denotes the number of ensemble members.

Weighted Decision Fusion Strategy

Unlike simply taking the majority vote, the hybrid approach adopts a weighted combination using the accuracy of each classifier. The weight w k of classifier M k is given by:

$$w_k = \frac{Acc_k}{\sum_{i=1}^{K} Acc_i}$$

The final intrusion decision Y_{final} is obtained by maximizing the weighted sum of predictions:

$$Y_{final} = arg \max_{c \in C} \sum_{k=1}^{K} w_k . I(\hat{y}_k = c)$$

where I(·) is the indicator function and C represents the set of attack classes.

This dynamically-adjusted weighting provides robustness towards poor classifiers and across diverse heterogeneous IoT traffic distributions.

Algorithm 1: Proposed Ensemble-Based IoT Intrusion Detection

1. Input raw IoT traffic dataset D
2. Perform data cleaning, encoding, normalization, and class balancing
3. Apply feature selection to obtain optimized feature set F*
4. Train RF, XGBoost, SVM, and kNN classifiers using F*
5. Compute classifier weights using validation accuracy
6. Fuse predictions via weighted voting
7. Output final intrusion class label

Feature reduction decreases the dimensionality from n to m, (where mn) which has the benefit of significantly decreasing training costs. Random Forest and XGBoost operate with complexity , where T denotes the number of trees, while SVM and kNN scale with and O(Nm), respectively. The ensemble fusion does not take any significant extra computation time, thus, the system could be applied in real time IoT application.

Experimental Setup and Results

The experiment to evaluate the proposed ensemble framework was performed on a high-performance computing environment consisting of an Intel Core i7-12700 CPU, 32 GB of RAM, and an NVIDIA RTX 3080 GPU which provides adequate resources for training several ML models on large IoT datasets. The implementation was built using Python 3.11 along with commonly used libraries like Scikit-learn 1.3 (for traditional ML models), XGBoost 1.7 (for gradient boosting), and Pandas and NumPy for data manipulation and pre-processing. In order to strike an effective balance between accuracy and computational time, each classifier was initialized with a set of optimal hyperparameters: the Random Forest was configured with 200 trees and a max_depth of 20, which effectively models complex nonlinear relationship within the data. The XGBoost was implemented with 300 estimators and learning rate = 0.1 along with max_depth = 10 to effectively balance performance of sequential weak learner with overfitting. The SVM with RBF kernel had C = 10 and gamma = 0.01 to ensure adequate margin separation within the high-dimensional feature space. K-NN used Euclidean distance and k=7 to achieve effective neighborhood approximation. Data was split into 70% training set and 30% test set by use of stratified sampling technique to reflect the true distribution of the attack classes in the dataset, which results in less biased evaluations. To aggregate the predicted outputs of individual models, weighted voting technique is applied, wherein the weight of individual classifier contributions are based on its cross-validation accuracy of 5-fold in order to give greater importance to models with higher prediction power which effectively tackles the variety of IoT traffic and improves robust detections. The proposed ensemble is tested only on the CICIoT2023 dataset, which is a large and heterogeneous IoT traffic dataset which simulates real world smart environments. This dataset includes:

- Traffic Sources: Smart home, industrial IoT, and wearable devices
- Attack Categories: Denial-of-Service (DoS), Distributed DoS (DDoS), Malware, Scanning, and Normal traffic

- Features: 85 attributes per flow, including statistical, temporal, and protocol-level features
- Volume: Approximately 3.2 million network flows with labeled attack types and normal behavior
- Source: Publicly available via the Canadian Institute for Cybersecurity IoT Dataset repository

Before testing the ensemble framework effectiveness, each type of attack was first individually assessed on its detect accuracy using the CICIoT2023 dataset. It is known that single-model approach are poor for heterogeneous IoT traffic because the traffic has varied patterns and many different types of attacks (Nazir et al., 2025; Das et al., 2021). Table 1 compares the accuracies and F1-scores of single classifiers and our ensemble to the different classes of attack.

Table 1: Multi-class Detection Performance on CICIoT2023

Attack Type	RF Accuracy	XGBoost Accuracy	SVM Accuracy	kNN Accuracy	Ensemble Accuracy	Ensemble F1-score
DoS	97.1%	97.9%	96.5%	95.8%	98.7%	0.987
DDoS	96.5%	97.2%	95.8%	94.9%	98.2%	0.983
Malware	95.9%	96.8%	95.0%	94.3%	97.5%	0.975
Scanning	95.4%	96.0%	94.6%	93.9%	97.0%	0.970
Normal Traffic	97.5%	98.1%	96.9%	95.8%	98.9%	0.989
Average	96.5%	97.2%	95.8%	94.9%	98.1%	0.981

According to the results in Table 1, ensemble classifier is superior over all the single classifiers with the higher values for the accuracy and F1-score on all the types of attacks. Complex attack patterns, such as Malware and Scanning, were detected with more certainty; this could be due to the ensemble method that used a weight sum of the single classifiers as already shown that the ensemble methods enhance reliability for heterogeneous traffic (Azzarini et al., 2023; Talukder et al., 2023).

Overall ensemble performance in all attack classes is depicted in Table 2 to provide a thorough overview. Accuracy, precision, recall, F1-score and false alarm rate, all common indicators used in IoT intrusion detection research, are reported (Kharoubi et al., 2025; Nazir et al., 2025).

Table 2: Weighted Ensemble Performance Metrics on CICIoT2023

Metric	Ensemble Value
Accuracy	98.1%
Precision	0.981
Recall	0.981
F1-score	0.981
False Alarm Rate	0.016

Table 2 shows that the designed ensemble system provides very good performance in all measures. The detection of attacks has a false alarm rate less than 2%, which gives very good confidence for real IoT environment applications. By using voting weights to give more reliable classifiers proportionally more vote, false positives for ambiguous or rare attacks can be minimized.

Summary of Findings

- The ensemble framework can realize a better detection performance over any single classifier on heterogeneous IoT traffic.
- Weighted voting improves the detection of complex attacks like Malware and Scanning by merging complementing learning models.
- Feature optimization increases computational efficiency without sacrificing the precision; which is feasible for real time applications.
- The generalization ability and robustness are good, and the precision is over 98%, False alarm rate is lower than 1.6%, which accords with previous research that proposes ensemble-based framework for IoT intrusion detection (Das et al., 2021; Azzarini et al., 2023).

Conclusion

In this paper, a weighted ensemble learning framework for robust cyberattack detection in heterogeneous IoT networks has been presented. The framework encompasses proper data pre-processing, fine-tuned feature selection, and the combination of three heterogeneous and complementary classifiers-Random Forest, XGBoost, SVM, kNN- through weighted voting to classify network attacks. The proposed ensemble specifically targeted the heterogeneous nature of IoT network traffic, different categories of attacks, and the high dimensionality associated with these networks using the CICIoT2023 dataset. Experimental validation showed that the proposed weighted ensemble outperforms each individual classifier with an average of 98.1% accuracy, 0.981 F1-score, and an extremely low false alarm rate of 1.6%. The weighted fusion strategy was very effective in producing robust detections especially for complex attack classes like Malware and Scanning, the traffic generated from these attacks often display heterogeneity in terms of behavior within the IoT network. The optimized features lowered the computational complexity without compromising the accuracy by eliminating irrelevant features in the process, this is suitable for either near real time or real time intrusion detection within IoT systems. For future works, it would be worth exploring incorporation of deep learning-based techniques, adaptive weight adjustment based on traffic nature and domain adaptation for cross-domain IoT based cyberattack detection.

References

1. K. Kharoubi, S. Cherbal, D. Mechta, et al., “Network intrusion detection system using convolutional neural networks: NIDS-DL-CNN for IoT security,” Cluster Computing, vol. 28, p. 219, 2025. doi: 10.1007/s10586-024-04904-7.
2. S. Das, S. Saha, A. T. Priyoti, E. K. Roy, F. T. Sheldon, A. Haque, et al., “Network intrusion detection and comparative analysis using ensemble machine learning and feature selection,” IEEE Transactions on Network and Service Management, 2021.
3. A. Nazir, J. He, N. Zhu, et al., “Empirical evaluation of ensemble learning and hybrid CNN-LSTM for IoT threat detection on heterogeneous datasets,” J. Supercomput., vol. 81, p. 775, 2025. doi: 10.1007/s11227-025-07255-1.
4. J. Jose and D. V. Jose, “Deep learning algorithms for intrusion detection systems in Internet of Things using CIC-IDS 2017 dataset,” International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 1, pp. 1134–1141, 2023.
5. R. Azzarini, H. Tianfield, and V. Charissis, “A stacking ensemble of deep learning models for IoT intrusion detection,” Elsevier, 2023, Art. no. 110941.
6. Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, “Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset,” IEEE Access, vol. 9, pp. 22351–22370, 2021.

7. M. Rashid, J. Kamruzzaman, T. Imam, S. Wibowo, and S. Gordon, “A tree-based stacking ensemble technique with feature selection for network intrusion detection,” Applied Intelligence, 2022, pp. 1–14.
8. M. A. Talukder, K. F. Hasan, M. M. Islam, M. A. Uddin, A. Akhter, M. A. Yousuf, et al., “A dependable hybrid machine learning model for network intrusion detection,” Journal of Information Security and Applications, vol. 72, Art. no. 103405, 2023.
9. D. Javeed, T. Gao, M. S. Saeed, and P. Kumar, “An intrusion detection system for edge-envisioned smart agriculture in extreme environment,” IEEE Internet of Things Journal, 2023.
10. M. Driss, I. Almomani, Z. E. Huma, and J. Ahmad, “A federated learning framework for cyberattack detection in vehicular sensor networks,” Complex & Intelligent Systems, vol. 8, no. 5, pp. 4221–4235, 2022.
11. M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, “Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning,” IEEE Access, vol. 10, pp. 40281–40306, 2022.
12. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine learning in IoT security: Current solutions and future challenges,” IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1686–1721, 3rd quarter 2020, doi: 10.1109/COMST.2020.2986444.
13. J. Zhang, S. Liang, F. Ye, R. Q. Hu, and Y. Qian, “Towards detection of zero-day botnet attack in IoT networks using federated learning,” in Proc. IEEE International Conference on Communications (ICC), Rome, Italy, 2023, pp. 7–12.
14. Y. Alotaibi and M. Ilyas, “Ensemble-learning framework for intrusion detection to enhance Internet of Things’ devices security,” Sensors, vol. 23, p. 5568, 2023. doi: 10.3390/s2312556.
15. Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, “Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset,” IEEE Access, vol. 9, pp. 22351–22370, 2021.