MOD-XGBOOST: AN ADAPTIVE MACHINE LEARNING MODEL FOR INTERNET OF THINGS ENVIRONMENT TO DETECT SPOOFING AND DOS ATTACKS

Sujit N. Deshpande (1), Deipali Vikram Gore (1), Amrapali Shivajirao Chavan (2), Arundhati Nelli (3)*

(1) PES's Modern College of Engineering, Pune, India; (2) All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune; (3) K. L. S Gogte Institute of Technology, Belagavi, India.

* Corresponding Author, e-mail: publication.sujit@gmail.com

Abstract: The rising number of Internet of Things (IoT) devices necessitates robust security to counter threats like Denial-of-Service (DoS) and spoofing attacks. Many Intrusion Detection Systems (IDS) leverage Machine Learning (ML), but challenges like concept drift and class imbalance persist. This study presents an adaptive ML-based IDS framework using a Modified XGBoost (Mod-XGB) model. Mod-XGB incorporates a weighted loss function for class imbalance, adaptive instance weighting for concept drift, and a security penalty term to enhance feature selection. Evaluated on the CICIoV2024 dataset, Mod-XGB achieved 97.96% accuracy, outperforming models like Random Forest, Logistic Regression, and AdaBoost. This innovative approach effectively addresses IoT security challenges, offering significant advancements in IDS performance for improved attack detection and resilience in dynamic environments.

Key words: IoT security, attack detection, XGBoost, concept drift, class imbalance, Modified XGBoost, Intrusion Detection System, CICIoV2024.

1. INTRODUCTION

By allowing everyday objects and products to get connected to the Internet and interact and collaborate with one another, the Internet-of-Things (IoT) has completely changed the way people live. These IoT devices enhance efficiency, convenience, and decision-making capabilities, making life easier and businesses more productive. However, their ubiquitous presence and reliance on connectivity make them vulnerable to a range of cyberattacks [1]. Nevertheless, IoT devices, due to their widespread deployment and often minimal security measures, present a broad attack surface for malicious actors. Cybercriminals exploit vulnerabilities in IoT devices to perform unauthorized activities, compromise sensitive data, or disrupt normal operations. Since many IoT devices lack robust authentication and encryption mechanisms, they are especially prone to attacks. Among the various cyber threats targeting IoT devices, spoofing attacks and Denial-of-Service (DoS) attacks are particularly prevalent and damaging [2], [3]. Spoofing attacks involve an attacker pretending to be a trusted device or entity. For example, an attacker could mimic a smart thermostat and send false signals to disrupt the Heating, Ventilation, and Air Conditioning (HVAC) system of a building [4]. Moreover, DoS attacks overwhelm an IoT device or network with a flood of traffic, causing system resources to be exhausted and rendering the device or network inoperable. An example includes the infamous Mirai botnet attack in 2016, which leveraged thousands of compromised IoT devices, and highlighted the devastating potential of such attacks [5]. Hence, preventing DoS attacks requires strong network monitoring, traffic filtering, and anomaly detection mechanisms.

The use of Artificial-Intelligence (AI), and more specifically Machine-Learning (ML) [6], [7] and Deep-Learning (DL) [8], [9], has recently grown in importance as a means of protecting IoT devices. These techniques are increasingly used to detect, classify, and mitigate cyber threats effectively. Despite the advances in using AI techniques for IoT security, significant challenges remain. Most existing approaches achieve high accuracy, on static datasets. However, they fail to address critical issues such as concept drift and class imbalance. Concept drift occurs when the underlying patterns in data change over time, rendering static models ineffective for real-world scenarios. Class imbalance, where certain attack types are underrepresented in the dataset, leads to biased predictions and poor detection of rare attacks. Furthermore, datasets such as CICIoV2024 [17], [20], which include diverse attack types like spoofing and DoS, have seen limited research. There is a pressing need for adaptive and robust security models that can handle these challenges effectively. Hence, this work aims to address these gaps by proposing a Modified XGBoost (Mod-XGB) model that incorporates mechanisms for handling concept drift, class imbalance, and IoT-specific security challenges, providing enhanced detection of attacks. The proposed work provides significant contributions to the domain of IoT security, particularly in detecting and classifying cyberattacks. These contributions include:

- The work presents an approach for IoT attack detection using the CICIoV2024 dataset, which includes diverse and realistic attack scenarios such as spoofing (Gas, Speed, Steering Wheel, Revolutions per minute (RPM)) and DoS.
- A novel enhancement of the XGB algorithm, referred to as Mod-XGB, is introduced. This model integrates weighted loss functions, adaptive instance weighting, and security penalty terms to address specific IoT challenges, i.e., class imbalance, concept drift, and security.
- By incorporating adaptive instance weighting, the proposed Mod-XGB model ensures scalability and robustness in dynamic IoT environments. This makes the solution applicable to real-world scenarios where attack patterns and data distributions change over time.
- The work evaluates the proposed Mod-XGB model using the CICIoV2024 dataset. The evaluation was done using accuracy, precision, recall, and F-score demonstrating the model's robustness and superiority over traditional methods in detecting and classifying IoT attacks.

The manuscript is structured as follows: Section II provides a comprehensive literature survey, discussing recent approaches for Intrusion Detection Systems (IDS) in

IoT environments. Section III details the methodology, elaborating on the XGB and Mod-XGB models and their implementation. Section IV presents the results of the XGB and Mod-XGB models, comparing their performance with existing models. Finally, Section V concludes the study by summarizing key findings and outlining potential directions for future work.

2. LITERATURE SURVEY

The proliferation of IoT devices has heightened the need for robust security mechanisms to counter various cyberattacks. Numerous studies have leveraged ML approaches to develop IDS designed for IoT environments. M. A. Elsadig et al. [10], presented a lightweight ML approach that used a Gini feature-selection approach incorporated with a Decision Tree (DT) for detecting DoS attacks in an IoT environment. For evaluation of their approach, they utilized the Wireless Sensor Network DoS (WSN-DoS) dataset, which they modified for this work. The findings showed that their approach achieved 99.5% accuracy in the detection of DoS attacks. Moreover, they tested other ML approaches, i.e., Extreme Gradient Boosting (XGB), Random Forest (RF), and K-Nearest Neighbors (KNN), which also achieved better results. B. Taşcı et al [11], presented an enhanced 1-Dimensional Convolutional Neural Network (CNN) (1D-CNN) approach for the detection and classification of IoT security data. In their 1D-CNN approach, their main focus was to avoid overfitting of data. Their approach was evaluated considering multiple security datasets, i.e., CIC-IDS2017, CIC-MalMem-2022, and CIC IoT 2023, which achieved 99.99%, 99.90%, and 98.36% respectively. The findings showed that the approach was good for classifying attacks. A. Muniswamy et al. [12], identified the security issues present in the IoT environment concerning network, software, data, application, cloud, and hardware and hence presented various approaches for avoiding any attacks. Their work also studied different ML approaches used for identifying attack type and presented different works accuracy. Finally, presented the limitations and benefits of different ML approaches. E. Ozdogan et al. [13], studied the different ML approaches presented in recent years for IoT-IDS and identified the best approach. Further stressed the importance of pre-processing and feature selection before training/testing data. They also discussed the problems related to class imbalance. Moreover, they identified from their work that by using appropriate pre-processing steps, they were able to achieve better feature selection and better performance from ML approaches.

M. Ozkan-Okay et al. [14], presented a study on cyber-security review, where different Reinforcement Learning (RL), ML, and DL approaches were discussed which were presented in the past few years. They identified the limitations and advantages of previously presented work. M. K. Nallakaruppan et al. [15], presented a work for classifying different host-based attacks using ML approaches in an IoT environment. They used fuzzy-based recommendations for doing a comparative study on the classification approaches parameters. Further, this work discusses various intrusions that can happen at the side of the IoT host and presented an effective approach for handling host-based intrusion attacks. Various ML approaches, i.e., DT, XGB, RF, and Light Gradient-Boosting (LGB) were evaluated using the CTU-13 dataset, where all achieved

99% above accuracy. M. S. Korium et al. [16], presented an IDS approach for detecting various cyberattacks, i.e., DoS, Distributed Denial of Service (DDoS), Sniffing, Botnets, Brute-Force, Distributed Reflection DoS (DR-DoS) in Internet of Vehicles (IoV). Their work's main objective was to detect abnormal behavior for evaluating network traffic, for which presented an IDS approach that used a pre-processing approach, feature-selection and used different ML approaches, i.e., CatBoost (Categorical Boosting), RF, XGB, and LGB which were optimized by hyperparameter selection for avoiding overfitting and provide better attack detection performance. Evaluations were conducted on different datasets, i.e., CIC-DDoS-2019, CSE-CIC-IDS-2018, and CIC-IDS-2017. Findings showed that XGB achieved 99.84% accuracy for achieving better performance for attack detection. C. Pinto et al. [17], presented a novel dataset called CICIoV2024, which consisted of spoofing and DoS attacks. For identifying attacks, they used various ML approaches, mainly RF, Deep Neural Network (DNN), AdaBoost (AB), and Logistic Regression (LR). Findings showed that RF and DNN achieved 95% whereas other approaches failed to achieve better outcomes. A. Alenizi [18], presented an IDS called Q-FuzzyNet which used DL approach. The Q-FuzzyNet used five steps in their work, where first collected datasets, pre-processed, extracted features, reduced dimensionality size of dataset and detected intrusion and mitigated it. They used the CIC-IoV dataset, which went through pre-processing using Mean-Imputation approach, extracted features using their presented improved mutual-information, entropy and correlation approach, reduced dimensionality using their improved linear-discriminant analysis and presented a Quantum-Inspired Fuzzy-Recursive Neural-Network for prediction. When evaluated their Q-FuzzyNet approach on CICIoV dataset, achieved 98.6% accuracy.

While many of these works have demonstrated exceptional performance, achieving accuracies often exceeding 99%, several limitations persist. For instance, M. A. Elsadig et al. [10] utilized a Gini-based feature selection approach integrated with DT, achieving impressive accuracy; however, their work did not address challenges such as concept drift and class imbalance in datasets. Similarly, B. Taşcı et al. [11] focused on mitigating overfitting in their 1D-CNN approach, but issues related to dynamic data shifts remain unaddressed. Other studies, such as those by M. S. Korium et al. [16] and M. K. Nallakaruppan et al. [15], have emphasized pre-processing and hyperparameter optimization but failed to explore the effects of concept drift on model performance. Moreover, while recent datasets like CICIoV2024 [17] have been introduced for IoT-specific attack detection, limited research has utilized this dataset comprehensively. Nevertheless, despite significant advancements in the application of ML for IoT security, many existing approaches as discussed above have failed to address critical challenges such as concept drift and class imbalance, most importantly by A. Alenizi [18], which are prevalent in real-world datasets. These limitations often result in poor generalization and degraded performance when new data is introduced. Additionally, there remains a dearth of studies leveraging the CICIoV2024 dataset, which encapsulates contemporary attack scenarios. To bridge these gaps, the proposed work utilizes a Mod-XGB model that effectively mitigates class imbalance and adapts to concept drift, thereby enhancing the detection of IoT attacks on CICIoV2024 while providing a robust framework for future research in this domain.

3. METHODOLOGY

The architecture of the presented work is structured into a well-defined pipeline to effectively handle IoT attack detection using the CICIoV2024 dataset, as presented in Figure 1. The process begins with the CICIoV2024 binary dataset, which comprises both benign and attack traffic, including diverse spoofing attack types (e.g., Gas, Speed, Steering Wheel, RPM) and DoS attacks. The dataset is then pre-processed and split into training/testing subsets to ensure robust evaluation. During this stage, the highest priority is taken to address potential class imbalance issues, which are a common challenge in real-world datasets. The pre-processed data is fed into two ML models: the baseline XGB model and the Mod-XGB model. The Mod-XGB introduces enhancements to handle key challenges such as class imbalance, concept drift, and security, which ensures the model performs well not only on static datasets but also in dynamic scenarios where data distributions may change over time. Finally, the outputs of both models were evaluated using performance metrics.

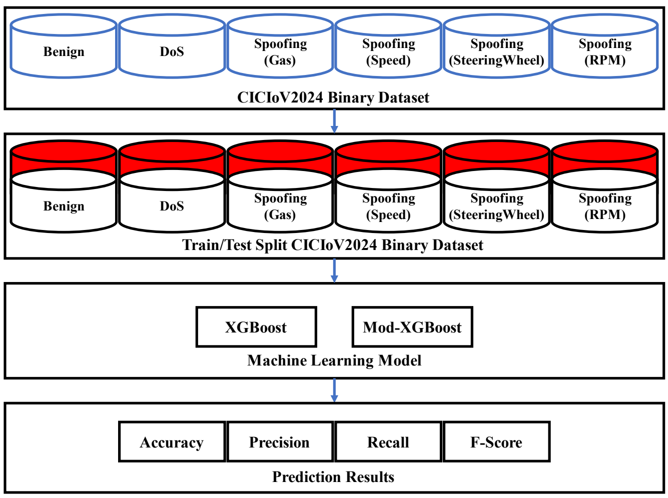

Figure 1. Architecture of Proposed Model.

XGB is an advanced approach of gradient-boosting which optimizes performance and scalability [19]. It is particularly suitable for handling large datasets and complex tasks such as multiclass classification or detection. The main objective function in XGB is to combine the loss function and a regularization term as presented in Eq. (1).

$$\mathcal{L}(\phi) = \sum_{i=1}^{N} \ell(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \quad (1)$$

In Eq. (1). $(y_i, \hat{y}_i)$ is loss-function for predictions, y_i is true-label for i^{th} instance, $\hat{y}_i$ is anticipated likelihood vector for i^{th} instance, $\Omega(f_k)$ is a regularization term for the k^{th} tree, N is no. of instances in the dataset, K is no. of trees and ϕ is a set of all parameters of the model. For multiclass detection or classification, the XGB loss function can be defined using Eq. (2).

$$\ell(y_i, \hat{y}_i) = -\sum_{c=1}^{C} 1(y_i = c) \log\left(\hat{y}_{i,c}\right) \quad (2)$$

In Eq. (2), C is no. of classes, $1(y_i = c)$ is indication-function, i.e., it will be 1 only when $y_i = c$, else 0 otherwise and $\hat{y}_{i,c}$ is an anticipated likelihood for class c for the i^{th} instance. The regularization in Eq. (1), i.e., $\Omega(f_k)$ is evaluated using Eq. (3).

$$\Omega(f_k) = \Upsilon T + \frac{1}{2}\lambda \sum_{j=1}^{T} w_j^2 \tag{3}$$

In Eq. (3), T is no. of leaves in the tree, w_j is the weight of j^{th} leaf, Υ is the regularization parameter for no. of leaves and λ is the regularization parameter for leaf-weights. As an IoT environment consists of numerous heterogenous devices, whose patterns in data evolve over time due to changes in attack vectors or device behavior, hence, it is important to handle class imbalance problems during training the model and address concept drift simultaneously. Hence, this work presents a Mod-XGB model which is discussed in detail in the next section. For handling class imbalance, and concept drift and to provide security, this work presents the Mod-XGB model. In the Mod-XGB model, for handling class imbalance, Eq. (2) is modified by introducing a weighted loss function as presented in Eq. (4).

$$\ell(y_i, \hat{y}_i) = -\sum_{c=1}^{C} \alpha_c 1(y_i = c) \log\left(\hat{y}_{i,c}\right) \tag{4}$$

In Eq. (4), α_c is a weight inversely proportional to the class frequency. Hence, from this, the Mod-XGB weighted objective function is defined using Eq. (5).

$$\mathcal{L}(\phi) = \sum_{i=1}^{N} \alpha_{y_i} \ell(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{5}$$

Moreover, the weights w in Eq. (3) is modified for handling concept drift using Eq. (6).

$$w_i^{(t+1)} = w_i^{(t)} \exp\left(-\beta \cdot l\left(y_i, \hat{y}_i^{(t)}\right)\right) \tag{6}$$

In Eq. (6), $w_i^{(t+1)}$ is weight of i^{th} instance at iteration t and β is the learning rate for weight adjustment. For providing security, this work introduced a security penalty term based on feature importance in Eq. (3) as presented in Eq. (7).

$$\Omega'(f_k) = \Omega(f_k) + \eta \sum_{j=1}^{T} I(j) w_j^2 \tag{7}$$

In Eq. (7), η is the security sensitivity parameter and $I(j)$ is the importance score of features j. The complete process of Mod-XGB is presented in Algorithm 1.

Algorithm 1. Mod-XGB

Input	Dataset $D = \{(x_i, y_i)\}_{i=1}^{N}$, learning rate η, regularization parameters λ, Υ and class weights α_c.
Output	Model $\phi = \{f_k\}_{k=1}^{K}$.
Step 1	Initialize and compute initial predictions as the average class probabilities.
Step 2	For each tree k
Step 3	Compute gradients g_i and hessians h_i as $g_i = \frac{\partial \ell(y_i, \hat{y}_i)}{\partial \hat{y}_i}$ and $h_i = \frac{\partial^2 \ell(y_i, \hat{y}_i)}{\partial \hat{y}_i^2}$, where $\ell(y_i, \hat{y}_i)$ is done using Eq. (4).
Step 4	Build tree f_k to minimize the weighted loss using $$\mathcal{L}_{tree} = \sum_{i \in leaf} \left(g_i w_i + \frac{1}{2} h_i w_i^2\right) + \Omega'(f_k)$$

Step 5 Update predictions using $\hat{y}_i \leftarrow \hat{y}_i + \eta f_k(x_i)$
Step 6 End for
Step 7 Update instance weights $w_i^{(t+1)}$ for concept drift handling using Eq. (6).
Step 8 Combine all trees $\{f_k\}$ into the final ensemble.

The Mod-XGB algorithm as presented in Algorithm 1 enhances the traditional XGB to address challenges specific to IoT environments, including class imbalance, concept drift, and security needs. As class imbalance is common in IoT datasets, where attack samples (e.g., DoS, spoofing) are much rarer than normal data. Mod-XGB incorporates class weights α_c as presented in Eq. (4) directly into the loss function, as shown in Step 3 in Algorithm 1. This ensures that rare classes contribute more significantly to the gradient g_i and hessian h_i, amplifying their influence during tree building. Consequently, the model becomes sensitive to minority classes, improving detection of rare attacks. Moreover, IoT environments are dynamic, with changing data patterns due to evolving attack strategies or device behavior. Step 7 introduces adaptive instance weighting using Eq. (6). This mechanism increases the weights of misclassified samples, forcing subsequent trees to focus on recent changes. It ensures the model adapts to new patterns, maintaining accuracy over time. Also, security in this work was enhanced through regularization term $\Omega'(f_k)$ (Step 4), which penalizes overly complex trees and prioritizes features with high importance for detecting attacks. This model minimizes overfitting while emphasizing security-critical features, such as packet anomalies and device identifiers. Additionally, by leveraging ensemble learning, Mod-XGB combines multiple trees, reducing the risk of model exploitation through adversarial attacks. Nevertheless, the Mod-XGB ensures robust, adaptive, and scalable predictions for IoT environments, addressing their unique challenges effectively, as discussed in the results and discussion section in the next section.

4. RESULTS AND DISCUSSION

For the proposed work evaluation, a system with the following specifications was utilized. The system was equipped with 16 GB RAM and an Intel i7 processor, which facilitated faster execution of computations and training of ML models. Windows 11 served as the operating system, providing a stable and efficient environment for the execution of the work. Python was used as the programming language to implement the entire framework. Both XGB and Mod-XGB models were executed on the same platform to ensure consistency and fairness in the evaluation process. This standardized setup provided a reliable basis for performance comparison of XGB and Mod-XGB models under identical conditions. For evaluation of the work, the CIC-IoV 2024 dataset [17], [20] was considered, which focuses on advancing cybersecurity solutions for IoV systems. It included data from a 2019 Ford vehicle, which underwent various spoofing and DoS attacks through the CAN-BUS protocol. The dataset, CICIoV2024, provides detailed information on intra-vehicular communication, and it is a valuable resource for testing ML-based cybersecurity techniques for an IoT environment. The performance metrics used to evaluate XGB and Mod-XGB models include accuracy, precision, recall, and f-score which are evaluated using Eq. (8), Eq. (9), Eq. (10), and Eq. (11)

respectively, where TN denotes true-negative, TP denotes true-positive, FN denotes false-negative and FP denotes false-positive.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

$$Precision = \frac{TP}{TP+FP} \quad (9)$$

$$Recall = \frac{TP}{TP+FN} \quad (10)$$

$$F - Score = \frac{2 \times Precision \times Recall}{Precision+Recall} \quad (11)$$

The results of the Mod-XGB model demonstrate a clear improvement when compared with the performance of XGB, as presented in Figure 2.

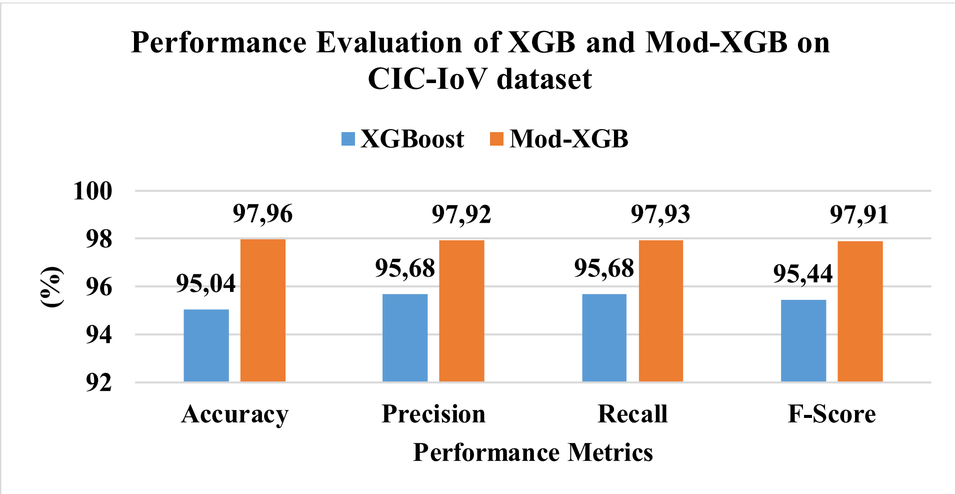

Figure 2. XGB vs Mod-XGB.

The XGB model achieved an accuracy of 95.04%, precision of 95.68%, recall of 95.68%, and an F-score of 95.44%, indicating strong overall performance in detecting and classifying IoT attacks. However, despite its better outcomes, the Mod-XGB model outperformed the XGB model across all metrics. With an accuracy of 97.96%, the Mod-XGB model exhibited a marked improvement of nearly 3%, which reflects its ability to better handle the complexities of the dataset, such as class imbalance, concept drift, and security concerns. In terms of precision, the Mod-XGB achieved 97.92%, slightly surpassing the XGB model's precision of 95.68%. Similarly, the recall for the Mod-XGB model was 97.93%, outperforming the XGB recall of 95.68%, highlighting its enhanced capability to identify both true positives and rare attack instances. The f-score for Mod-XGB also saw an improvement, reaching 97.91%, compared to XGB 95.44%, demonstrating that the Mod-XGB model shows better results. This performance boost can be attributed to the enhancements made in the Mod-XGB, such as the incorporation of a weighted loss function and adaptive instance weighting, which enable the model to effectively address the challenges posed by dynamic IoT environments. The results underscore the efficacy of the Mod-XGB model in improving attack detection, making it a superior choice for IoT security applications.

Moreover, the performance comparison between the different models taken from [17] and [18] for comparison reveals significant differences in their ability to detect and classify IoT-based attacks, as presented in Table 1, where accuracy, precision, recall, and f-score comparison have been presented. LR and DNN both achieved an accuracy of 95%, but their precision, recall, and F-score were relatively lower, with precision and recall both around 74% and 68%, respectively. This indicated that while these models were reasonably accurate, they struggled to effectively differentiate between attack and non-attack instances, resulting in a less balanced detection performance. Similarly, RF achieved the same accuracy as LR and DNN at 95%, but its precision was lower at 60%, suggesting that it misclassified more attack instances as benign, leading to suboptimal performance in attack detection with an f-score of 62%. On the other hand, AB performed the worst, with an accuracy of 87%, precision of 14%, recall of 17%, and an F-score of just 15%. This shows that AB was significantly less effective in identifying attacks, likely due to its inability to properly handle the class imbalance and complexities in the dataset. Further, Q-FuzzyNet achieved 98.6% accuracy, but its precision, recall and f-score was less in comparison with Mod-XGB. Also, in comparison, XGB showed better results, achieving an accuracy of 95.04%, precision of 95.68%, recall of 95.68%, and an f-score of 95.44%, demonstrating its robust performance in both attack detection and classification. However, the Mod-XGB model outperformed all other models by a significant margin, with an impressive accuracy of 97.96%, precision of 97.92%, recall of 97.93%, and an F-score of 97.91%. This enhancement was attributed to Mod-XGB's ability to handle class imbalance, concept drift, and security considerations more effectively, providing superior performance in terms of detecting rare and evolving IoT attacks. Thus, while traditional models like LR and RF showed decent performance, the Mod-XGB model demonstrated its superiority in addressing the unique challenges of IoT security.

Table 1. Comparative Study of Mod-XGB with other models

Model	*Accuracy*	*Precision*	*Recall*	*F-Score*
LR [17]	95	74	68	63
AB [17]	87	14	17	15
DNN [17]	95	74	68	63
RF [17]	95	60	68	62
Q-FuzzyNet [18]	98.6	97	96.8	96.4
XGB [Proposed]	95.04	95.68	95.68	95.44
Mod-XGB [Proposed]	**97.96**	**97.92**	**97.93**	**97.91**

5. CONCLUSION

This work presented a robust framework for IoT attack detection, focusing on spoofing and DoS attacks in IoT environments, for which introduced the Mod-XGB model, an enhancement of the XGB algorithm that integrates weighted loss functions for handling class imbalance, adaptive instance weighting to tackle concept drift, and a security penalty term to prioritize important features. The experimental results demonstrated that the Mod-XGB model significantly outperformed the traditional and proposed models in IoT attack detection. With an accuracy of 97.96%, the Mod-XGB model surpassed the standard XGB model, which achieved 95.04% accuracy. This nearly 3% improvement reflects the Mod-XGB model's superior capability in handling complex IoT datasets, particularly those affected by class imbalance and evolving attack patterns. Traditional models such as LR, DNN, and RF exhibited 95% accuracy, but their precision, recall, and F-score remained lower, indicating weaker classification performance. AB performed the worst, with 87% accuracy, proving inadequate for IoT attack detection. In terms of precision and recall, the Mod-XGB model achieved 97.92% and 97.93%, respectively, outperforming the XGB model, which had 95.68% for both metrics. This improvement highlights the Mod-XGB model's enhanced ability to correctly classify both attack and benign instances, reducing false positives and false negatives. Compared to Q-FuzzyNet, which had 97% precision and 96.8% recall, Mod-XGB demonstrated a slight edge, making it one of the most effective models in IoT security applications. The f-score for Mod-XGB also saw an increase to 97.91%, compared to XGB's 95.44%, further confirming its superior balance between precision and recall. Overall, the Mod-XGB model proved to be a highly effective solution for IoT attack detection, outperforming traditional models by a significant margin. Its integration of weighted loss functions, adaptive instance weighting, and security-aware feature selection contributed to its robustness against evolving threats. Future work will explore real-time deployment in IoT networks, integration with deep learning techniques, and adversarial attack resistance to further enhance its reliability in real-world cybersecurity applications.

REFERENCES

[1] Altulaihan, E., Almaiah, M. A., Aljughaiman, A. Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions. *Electronics*, vol. 11, no. 20, Oct. 2022. DOI: 10.3390/electronics11203330.

[2] Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., Iqbal, S. A Comprehensive Survey on IoT Attacks: Taxonomy, Detection Mechanisms and Challenges. *Journal of Information and Intelligence*, vol. 2, no. 6, Dec. 2023. DOI: 10.1016/j.jiixd.2023.12.001.

[3] Mukhtar, B. I., Elsayed, M. S., Jurcut, A. D., Azer, M. A. IoT Vulnerabilities and Attacks: SILEX Malware Case Study. *Symmetry*, vol. 15, no. 11, Oct. 2023, pp. 1978-1978. DOI: 10.3390/sym15111978.

[4] Khan, I. U., et al. A Proactive Attack Detection for Heating, Ventilation, and Air Conditioning (HVAC) System Using Explainable Extreme Gradient Boosting Model (XGBoost). *Sensors*, vol. 22, no. 23, Nov. 2022, p. 9235. DOI: 10.3390/s22239235.

[5] Gelgi, M., Guan, Y., Arunachala, S., Samba Siva Rao, M., Dragoni, N. Systematic Literature Review of IoT Botnet DDOS Attacks and Evaluation of Detection Techniques. *Sensors*, vol. 24, no. 11, Jan. 2024, p. 3571. DOI: 10.3390/s24113571.

[6] Farooqi, A. H., Akhtar, S., Rahman, H., Sadiq, T., Abbass, W. Enhancing Network Intrusion Detection Using an Ensemble Voting Classifier for Internet of Things. *Sensors*, vol. 24, no. 1, Dec. 2023, pp. 127-127. DOI: 10.3390/s24010127.

[7] Talukder, M. A., et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding, and feature extraction. *Journal of Big Data*, vol. 11, no. 1, Feb. 2024. DOI: 10.1186/s40537-024-00886-w.

[8] Altunay, H. C., Albayrak, Z. A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks. *Engineering Science and Technology, an International Journal*, vol. 38, Feb. 2023, p. 101322. DOI: 10.1016/j.jestch.2022.101322.

[9] Deshmukh, A., Ravulakollu, K. An Efficient CNN-Based Intrusion Detection System for IoT: Use Case Towards Cybersecurity. *Technologies*, vol. 12, no. 10, Oct. 2024, p. 203. DOI: 10.3390/technologies12100203.

[10] Elsadig, M. A. Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach. *IEEE Access*, vol. 11, 2023, pp. 83537-83552. DOI: 10.1109/ACCESS.2023.3303113.

[11] Taşcı, B. Deep-Learning-Based Approach for IoT Attack and Malware Detection. *Applied Sciences*, vol. 14, no. 18, 2024, p. 8505. DOI: 10.3390/app14188505.

[12] Muniswamy, A., Rathi, R. A Detailed Review on Enhancing the Security in Internet of Things-Based Smart City Environment Using Machine Learning Algorithms. *IEEE Access*, vol. 12, 2024, pp. 120389-120413. DOI: 10.1109/ACCESS.2024.3450180.

[13] Ozdogan, E. A Comprehensive Analysis of the Machine Learning Algorithms in IoT IDS Systems. *IEEE Access*, vol. 12, 2024, pp. 46785-46811. DOI: 10.1109/ACCESS.2024.3382539.

[14] Ozkan-Okay, M., et al. A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions. *IEEE Access*, vol. 12, 2024, pp. 12229-12256. DOI: 10.1109/ACCESS.2024.3355547.

[15] Nallakaruppan, M. K., et al. Enhancing Security of Host-Based Intrusion Detection Systems for the Internet of Things. *IEEE Access*, vol. 12, 2024, pp. 31788-31797. DOI: 10.1109/ACCESS.2024.3355794.

[16] Korium, M. S., Saber, M., Beattie, A., Narayanan, A., Sahoo, S., Nardelli, P. H. J. Intrusion detection system for cyberattacks in the Internet of Vehicles environment. *Ad Hoc Networks*, vol. 153, Feb. 2024, p. 103330. DOI: 10.1016/j.adhoc.2023.103330.

[17] Pinto, C., et al. CICIoV2024: Advancing realistic IDS approaches against DoS and spoofing attack in IoV CAN bus. *Internet of Things*, May 2024, pp. 101209-101209. DOI: 10.1016/j.iot.2024.101209.

[18] A. Alenizi, "Q-FuzzyNet: A Quantum Inspired QIF-RNN and SA-FPA Optimizer for Intrusion Detection and Mitigation in Intelligent Connected Vehicles," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 11, 2024, doi: 10.14569/ijacsa.2024.0151122.

[19] Chen, T., Guestrin, C. XGBoost: a Scalable Tree Boosting System. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining - KDD '16*, 2016, pp. 785-794. DOI: 10.1145/2939672.2939785.

[20] IoV Dataset 2024 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. UNB. URL: https://www.unb.ca/cic/datasets/iov-dataset-2024.html (Visited on 12.01.2025).

Information about the authors:

Dr. Sujit N. Deshpande – He is currently working as an Assistant Professor in the Department of Computer Engineering at PES's Modern College of Engineering (Autonomous), Shivajinagar, Pune, Maharashtra, India. He has 15 years of teaching experience. He received his B.E. and M.E. degrees in Computer Science and Engineering (CSE) from Solapur University and a Ph.D. in (CSE) from Visvesvaraya Technological University, Belagavi, Karnataka. He has published 15+ research papers in refereed International Journals and Conferences. He has received the Best Paper Award for research work at the International Conference. He has published one patent on research work. His areas of interest include IoT, Cloud Computing, Machine Learning, Deep Learning, and Security. He is a Life Member of ISTE.

Dr. Deipali Vikram Gore – She is an academician and researcher in the field of Computer Engineering. She holds a Ph.D. in Computer Engineering with a specialization in Machine Learning and Deep Learning, reflecting her expertise in these advanced technologies. Dr. Deipali Vikram Gore, is currently an Associate Professor in the Department of Computer Engineering at PES Modern College of Engineering, where she has been a faculty member for over 25 years. Her extensive experience encompasses research, teaching, and mentoring in diverse areas of computer science, including Machine Learning, Deep Learning, and their real-world applications.

Dr. Amrapali Shivajirao Chavan – She is working as an Assistant Professor in the Computer Engineering Department at the All-India Shri Shivaji Memorial Society's Institute of Information Technology, Pune, Maharashtra, India. With a Ph.D. in Computer Engineering from Kalinga University, Raipur She has 12+ years of teaching experience. She has authored numerous research papers in SCI/SCOPUS-indexed journals and actively participates in international IEEE/Springer conferences.

Dr. Arundhati Nelli – She is an Assistant Professor at K. L. S Gogte Institute of Technology, Belagavi, Karnataka. She completed her Ph.D. from Visveswaraya Technological University, Belagavi. Her research interests are Cloud Computing, Soft Computing, and sMachine Learning.

Manuscript received on 13 January 2025