THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 5. Issue 1.1 (2025)
https://doi.org/10.62019/h07sd615

ASIAN BULLETIN OF BIG DATA MANAGEMENT
http://abbdm.com/
ISSN (Print): 2959-0795
ISSN (online): 2959-0809

Enhancement of IoT Intrusion Detection: Evaluating ML and DL Approaches with NetFlow Datasets

Mohsin Suleman, Noushin Saba, Afia Zafar*, Mohsina Abid,

Chronicle

Article history
Received: Oct 2, 2025
Received in the revised format: Oct 5, 2025
Accepted: Oct 12 2025
Available online: Oct 23, 2025

Mohsin Suleman, Noushin Saba, are currently affiliated with the Department of Computer Science NUTECH, Islamabad, Pakistan and **Mohsina Abid** is a student under Department of Computer Science NUST, Islamabad, Pakistan, **Afia Zafar** is currently affiliated with the Department of Computer Science FAST University, Islamabad, Pakistan.

Email: Mohsin.suleman@Nutech.edu.pk
Email: Mohsina.Abid70@gmail.com
Email: Noushin.saba@Nutech.edu.pk
Email: Afia.zafar9@gmail.com

Corresponding Author*

Abstract

The Internet of Things (IoT) is a concept that involves integrating diverse objects to enable seamless interaction between real-world and virtual entities. IoT is now connecting the physical world to networks. IoT devices can sense, process, transmit, and store data collected from the physical world. However, these devices are resource-constrained, creating significant security vulnerabilities in many IoT applications. Implementing effective security measures on such devices is challenging without compromising their performance or potentially causing damage. Consequently, there is a substantial gap between the security capabilities of current IoT devices and their security requirements. Computer security principles, namely Confidentiality, Integrity, and Availability (CIA), can be compromised by malicious intrusions or attacks on computers and information databases. This study proposed and compared 1D CNN and XGBoost for detecting malicious attacks in the IoT environment. The proposed techniques were evaluated on the five variants of NetFlow datasets. The experiments shows that the proposed techniques outperform the Ensemble Tree classifier, achieving better performance in binary and multi-class classification. The results for 1D CNN and XGBoost were compared on the basis of F1 measure, AUC, recall, correctness value, and ppv.. The comparison shows that XGBoost is the better-performing model across the NetFlow datasets. XGBoost's ability to capture complex patterns and optimize the classification task makes it robust and effective.

Keywords: Internet of Things (IoT), Intrusion Detection System (IDS), 1D-CNN, XGBoost, NetFlow datasets, Cybersecurity.

INTRODUCTION

The usage of Internet of Things (IoT) technologies and systems is rapidly increasing at an unprecedented rate. According to Datar Reportal (2023), in January 2023, there were 5.16 billion internet users worldwide, indicating that 64.4 percent of the world's population is currently connected online. While the global internet user total has grown by 1.9 percent in the past year, delays in data reporting imply that the actual growth may be greater than what these figures indicate. Figure 1 shows the total count of individuals using the internet in millions, along with the percentage change from one year to the next in the IoT environment according to Data Reportal (2023).bModern IoT systems are no longer limited to the individual level, as interconnected IoT devices are now widespread across entire cities or even countries. With the aid of the expanding communication speed and bandwidth, IoT devices have the capacity to collect, transmit, and process vast quantities of data (Singh et al., 2024; Mapari et al., 2024). IoT systems, along with the data they collect, present significant prospects for creating and delivering intelligent services in various fields such as intelligent transportation, automated surveillance, and smart cyber-physical systems (Jain et al., 2024; Zafar et al., 2022). According to research conducted by Cisco, it is expected that there will be an average of 75.3 billion IoT devices actively

connected by the year 2025 (Lavanya & Anushiya, 2024; Siddiqui, 2023). Nonetheless, since the data collected by IoT systems may contain sensitive information and most IoT devices are resource constrained, it is essential to focus on privacy protection and reliable data security issues. Numerous security Numerous security holes have also been established by the rapidly increasing internet usage. Numerous smart devices such as sensors and actuators with constrained processing capabilities and heterogeneous hardware make up an IoT system. It is extremely difficult to implement effective security countermeasures on such devices without compromising performance or perhaps causing harm. As a result, there is a substantial gap between the security capabilities of current IoT devices and the security needs. The computer security guidelines, namely Confidentiality, Integrity, and Availability (CIA), may be compromised.

To close these security holes, a variety of technologies are used, including firewalls, data encryption, and user authentication. A variety of attacks can be prevented using these security measures. However, thorough packet analysis is not possible with these security technologies. As a result, the security tools are unable to detect attacks at the desired level. To address these shortcomings, intrusion prevention systems (IPS) and intrusion detection systems (IDS) have been introduced. These systems' algorithms — including machine learning, deep learning, and artificial intelligence — allow them to analyze data more thoroughly than other security systems. IDS systems are only used for intrusion detection and analysis, whereas IPS systems function as both detection and prevention mechanisms (Kizza, 2024; Shahin et al., 2024).

According to the latest Check Point Research (2023) cybersecurity report, in 2022, the global landscape witnessed a notable surge in cyber threats. Malware attacks experienced a 2% year-on-year increase, reaching a staggering 5.5 billion incidents. Intrusion attempts, on the other hand, witnessed a substantial rise of 19%, with an alarming total of 6.3 trillion attempts. Cryptojacking attacks, a concerning cyber threat, saw a significant surge as well, hitting a count of 139.3 million attacks — a 43% increase compared to the previous year. Meanwhile, the Internet of Things (IoT) sector also faced severe challenges, with IoT malware witnessing an alarming 87% spike, accounting for a total of 112.3 million incidents. These statistics underscore the growing intensity and sophistication of cyber threats, emphasizing the vital necessity of strong cybersecurity defenses to protect people, businesses, and governments against the constantly changing cyber environment. As we move forward, it becomes imperative for all stakeholders to remain vigilant and proactively address these escalating cyber threats to ensure a safer digital environment for everyone.

LITERATURE REVIEW

ML based and DL based NIDS's performances are greatly influenced by network data features. However, analyzing ML and DL models is frequently inaccurate because every ML-based NIDS and DL-based NIDS is trained and verified utilizing various features that might not contain security measures. Hence, commonality feature selection from numerous datasets is necessary for assessing the potential of ML-based and DL-based algorithms to generalize across datasets. Sarhan et al. (2021) demonstrated the NetFlow dataset. Four standard datasets NTW-NP15, BoF-IoT, ToN-IoT, and CES-CIC-IDS were used in the extraction of the NetFlow dataset. To create NetFlow datasets, the publicly accessible packet capture (pcap) files for each dataset are used. Ntop's nProbe software was used to transform the pcap files into NetFlow version 9 format. Twelve features were chosen for extraction. An Ensemble Tree Classifier was utilized for the evaluation of performance on five datasets.

Experimental results showed that NetFlow dataset performance decreases as compared to the benchmark dataset performance. Rashid et al. (2022) offered a tree-based hybrid ensemble approach and evaluated the model's efficacy on NTL-KDD and USNW-NB15. The approach was based on hybrid ensemble learning. The Select Best model was utilized to determine the k best features, with k equal to 20, yielding the top 20 important features ranked by their predictive score. The study evaluated 20 features with the highest scores out of the 41 and 42 features in both datasets. A higher-scoring characteristic has a greater impact in discriminating between typical and anomalous applications. The study improved the suggested technique by including feature selection approaches to choose the most appropriate characteristics. The study concentrated on detecting network traffic as normal or attack and did not concentrate on identifying the different classes. Saeed (2022) aimed to ameliorate the efficacy of classifiers in identifying unknown attacks by focusing on boosting the classifier's performance.

Furthermore, the main goals of the work were to implement and investigate the most generally used classifiers, i.e., KNN and Bayes, in the deployment of IDS, to autonomously assess classifiers' performance separately, and then use these two classifiers to build a hybrid classifier. NSL-KDD and KDD 1999 datasets were used in the investigation. Aslan et al. (2023) proposed a technique based on BGAN to improve the performance of ML approaches RF, DT, and ANN. BGAN is utilized to produce a wider range of data that can be employed for further analysis. The outcomes indicate that the data model proposed can significantly improve the efficacy of RF, DT, and ANN.

In another study, Jain et al. (2024) presented a unique multi-stage optimized ML-based NIDS architecture that can decrease computation time and cost while retaining detection efficiency. The suggested framework's performance was evaluated on CICIDS-2017 and UNSW-NB 2015 datasets. Jimmy (2024) first assessed four unsupervised machine learning algorithms on two current datasets. The outcomes revealed that although these methods exhibited impressive classification scores on one dataset, they were not competent in preserving the consistent degree of correctness value when applied to another dataset with similar features. Another ML-based study was presented by Bui et al. (2024). ML algorithms DJ, RF, and SVM were proposed. These models address the issue that arises when IDS enhances system performance by reducing false alarm rates while increasing actual alarm rates. KDD and CICIDS2017 datasets were used to evaluate the performance of detecting intrusions from network-based ML approaches.

Traditional NIDS are policy based. With the increase in technology new algorithms have been developed for generation of IoT Bots. These Bots are more complicated and sophisticated that already designed NIDS are unable to detect these attacks in the network traffic. So new and improved deep learning-based solutions are required to prevent this limitation. The following is a list of issues with current solutions:

- Traditional based NIDS are not so much capable of detecting sophisticated and complicated IoT Botnets and are less efficient in producing high correctness value, ppv, recall with low false alarm rates.
- Most the datasets used in the existing models are outdated and are not proficient enough of detecting new emerging attacks.
- Traditional based NIDS are not proficient enough of detecting and categorizing types of malicious traffic in the network.
- Traditional based NIDS have high false alarm rate.

PROPOSED METHODOLOGY

The proposed system architecture used in this paper is shown in Figure 4. We have devised and compared two separate architectures based on ML and DL for detecting attacks and threats IoT environment. The first architecture is based on XGBoost, while the second architecture utilizes a 1D-CNN.

NetFlow Dataset

The dataset leveraged in this work consists of variants of the NetFlow dataset. These datasets are publicly accessible (Sarhan et al., 2021). The NF-USNW-NT15 dataset contains 1,623,118 instances categorized into nine attack classes. The NF-TON-IoT dataset has 600,100 instances divided into four attack classes. The NF-BoN-IoT dataset includes 1,379,274 records, with 80.4% benign and 19.6% attack samples, classified into nine classes. The CSE-CIC-IDS2018 dataset comprises 8,392,401 records, with 87.86% benign and 12.14% attack samples, categorized into various attack types. The NF-UQ-NIDS dataset combines the previous datasets, resulting in 11,994,893 records with 76.77% benign and 23.23% attack samples, demonstrating the feasibility of creating a comprehensive and diverse NIDS dataset. A summary of the dataset is presented in

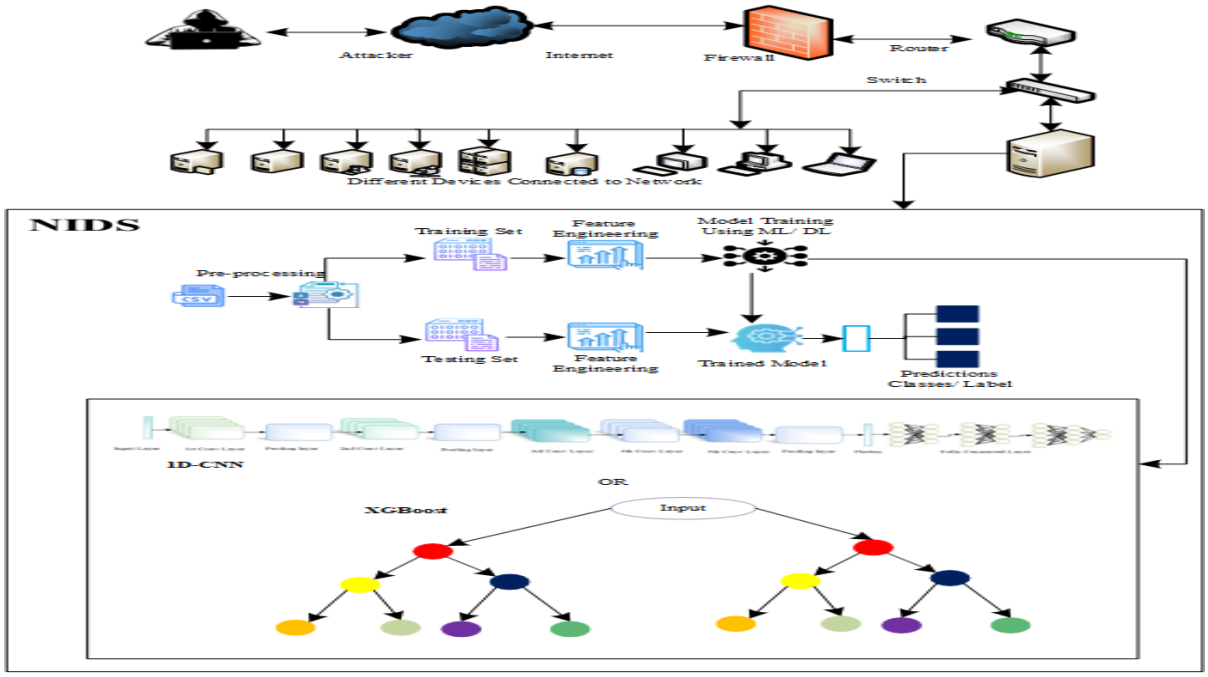

Figure 1.
Proposed Architecture

Preprocessing Phase

Captured network traffic data must be pre-processed before training the model. This involves handling empty fields or NaN values, converting categorical data (such as IP addresses) to numeric values, and scaling the data using MinMax or Standard Scaler. Attack-indicating labels are converted to numerical values through One Hot Encoding. Following that, the dataset is separated into subsets training (75%), and testing (25%).

Proposed Algorithms

The following two algorithms are used in paper for detecting malicious attacks from the network traffic.

1. 1D-CNN
2. XGBoost

Proposed 1D-CNN

The five convolutional layers including three fully linked layers, each one having a unique set of parameters, constitute the proposed 1D-CNN architecture. Pooling layers are subsequent after first, second, and fifth convolutional layers. The activation function used in each layer is relu, with exception of the output layer, which uses softmax. Architecture of 1D-CNN is presented in Table1.

Table 1:
Architecture of 1D- CNN

Layers		Feature Map No of Filters/ Neurons	Filter Size/ Kernel Size	Stride	Size of Feature Map	Padding	Activation Function
Input Layer	**Image**	-	-	-	227x227x3	-	relu
First Layer	**Convolution**	96	11	4	55x55x96	same	relu
	Pooling	96	3	2	27x27x96	-	
Second Layer	**Convolution**	256	5	1	27x27x256	Same	relu
	Pooling	256	3	2	13x13x256	-	
Third Layer	**Convolution**	384	3	1	13x13x384	same	relu
Fourth Layer	**Convolution**	384	3	1	13x13x384	same	relu
Fifth Layer	**Convolution**	256	3	1	13x13x256	same	relu
	Pooling	256	3	2	6x6x256	-	
Sixth Layer	**Fully Connected**	-	-	-	4096	-	relu
Seventh Layer	**Fully Connected**	-	-	-	4096	-	relu
Eighth/ Output Layer	**Fully Connected**	-	-	-	No of Classes	-	softmax
Batch Size		512					
Epoch		10					
Model Optimizer		Adam					
Loss Function		Sparse Categorical Cross Entropy					

Proposed XGBoost Algorithm

The XGBoost algorithm has been selected for classifying malicious intrusions in the IoT environment. The model configuration includes a maximum tree depth of 5 to prevent overfitting, a learning rate of 0.1, and 1000 boosting iterations. We set the minimum loss reduction to 0, minimum sum of instance weights to 1, and used an 80% subsample and 80% column sample by tree to introduce diversity. Additionally, L1 regularization (LASSO) with a penalty term of 0.005 was applied to control model complexity and promote sparse feature selection.

RESULTS AND ANALYSIS

The devised architecture was evaluated for both multiclass and binary class classification. For binary class classification these datasets have 2 classes benign and malicious represented by 1 and 0 respectively. For multi-class classification NF-UNSW-NB15 has 10 classes 1 for benign and another 9 for different attacks, NF-BoT-IoT has 5 1 for benign and other 4 for different attacks, NF-ToN-IoT has 10 1 for benign and another 9 for different attacks, NF-CSE-CIC-IDS2018 has 7 classes 1 for benign and

other 6 for different attacks and NF-UQ-NIDS has 21 classes 1 for benign and other 20 for different incursions.

BINARY CLASS CLASSIFICATION

1D-CNN

For For the NF-USNW-NB15 dataset, 1D-CNN obtained 98.64% classification correctness, 0.9419 positive predicted value (ppv), 0.8924 true positive rate (TRP), 0.9156 F measure, and 0.9960 AUC for the NF-UNSW-NB15 dataset. It obtained 98.75% correctness, 0.9577 ppv, 0.7501 TRP, 0.8221 F1 measure, and 0.9866 AUC on the NF-BoT-IoT dataset. It obtained 98.45% correctness, 0.9867 ppv, 0.9641 trp, 0.9749 F1 measure, and 0.9958 AUC for the NF-ToN-IoT dataset. The findings were 99.13% correctess, 0.9911 ppv, 0.9678 trp, 0.9791 F1 measure, and 0.9861 AUC on the NF-CSE-CICIDS2018 dataset. Finally, for the NF-UQ-NDS dataset, 1D-CNN achieved a correctness value of 89.53%, a ppv of 0.8581, a recall of 0.8427, an F1 measure of 0.8499, and an AUC of 0.7820. Figure 5 displays the CM for the binary class classification assessed using the 1D-CNN Algorithm for NF-USNW-NB15, NF-BoT-IoT, NF-ToN-IoT, NF-CSE-CICIDS2018, and NF-UQ-NIDS.

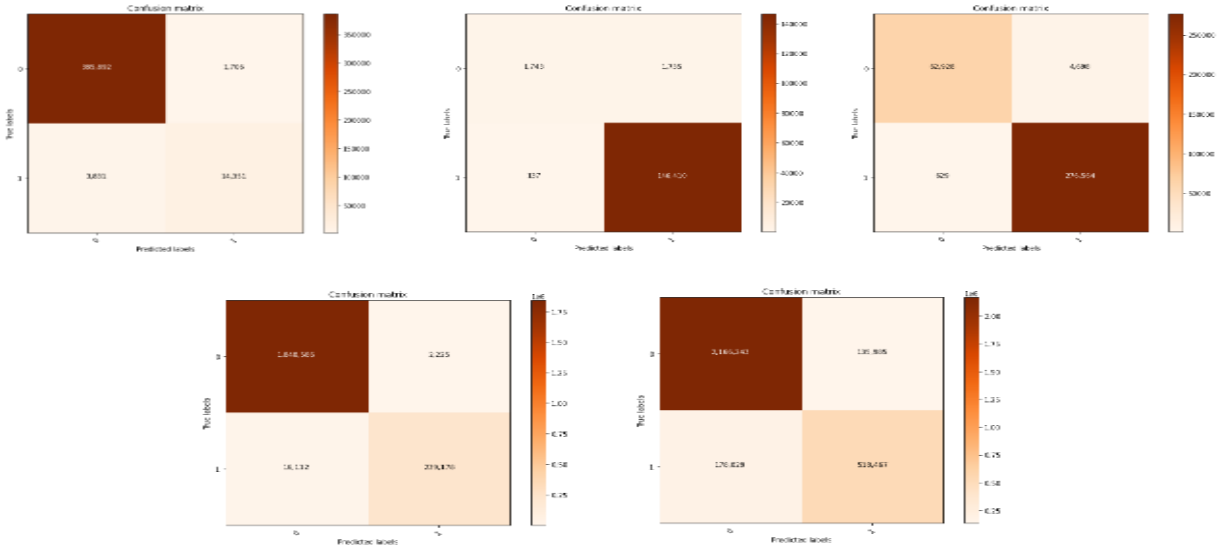

Figure 2.
(Left to Right) Confusion Matrix for NF-UNSW-NB15, NF-BoT-IoT, NF-ToN-IoT, NF-CSE-CICIDS2018, NF-UQ-NIDS Binary class classification evaluated through 1D-CNN Algorithm

XGBoost

For For the NF-UNSW-NB15 dataset, XGBoost attained a 99.01% correctness value featuring a ppv of 0.9419, recall of 0.9267, F1 measure of 0.9402, and AUC of 0.9267, reflecting high correctness value in positive instance identification and strong overall efficiency. In the NF-BoT-IoT dataset, XGBoost reached 99.25% correctness value featuring a ppv at 0.9742, recall at 0.8556, F1 measure at 0.9060, and AUC at 0.8556, indicating high ppv but room for improvement in recall and overall discriminatory power. For the NF-ToN-IoT dataset, XGBoost delivered an exceptional 99.96% correctness value with near-perfect ppv (0.9994), recall (0.9992), F1 measure (0.9993), and AUC (0.9992), showcasing excellent efficiency. On the NF-CSE-CICIDS2018 dataset, it achieved 99.35% correctness value with ppv of 0.9960, recall of 0.9734, F1 measure of 0.9844, and AUC of 0.9734, demonstrating high efficiency but with slightly lower recall and discriminatory power. Finally, for the NF-UQ-NIDS dataset, XGBoost had a 99.29% correctness value with ppv of 0.9936, recall of 0.9865, F1 measure of 0.9900, and AUC of 0.9865, reflecting robust efficiency and low false positive and

negative rates. Binary Class Classification Results for 1D-CNN and XGBoost is presented in Table 2.

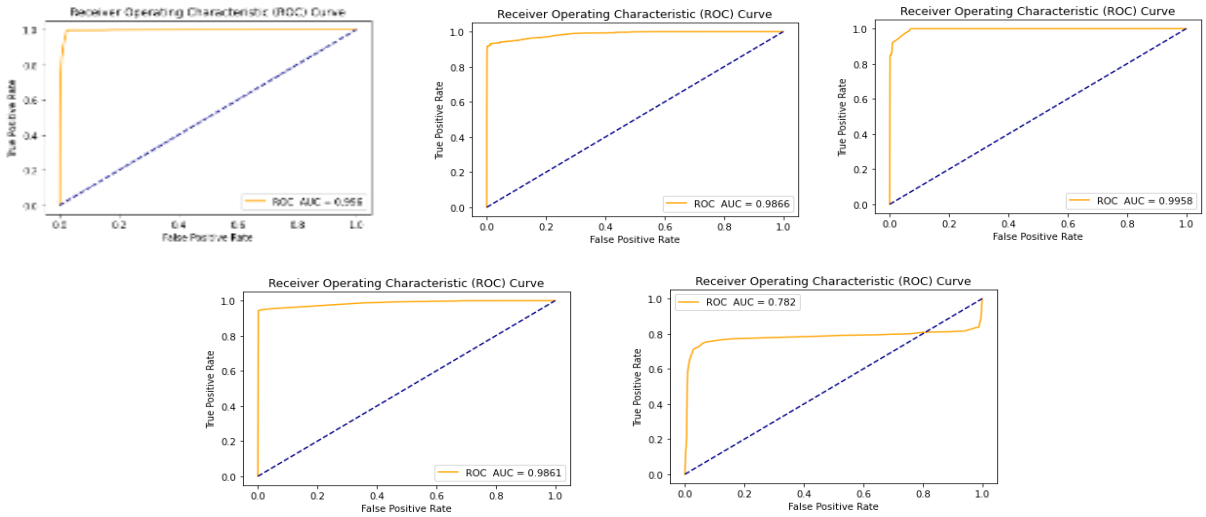

Figure 3.
(Left to Right) ROC Curve for NF-UNSW-NB15, NF-BoT-IoT, NF-ToN-IoT, NF-CSE-CICIDS2018, NF-UQ-NIDS Binary class classification evaluated through 1D-CNN Algorithm

MULTI-CLASS CLASSIFICATION

1D-CNN

For the NF-UNSW-NB15 dataset, 1D-CNN attained a correctness value of 96.86%, with a ppv of 0.3758, recall of 0.2851, F1 measure of 0.2944, and AUC of 0.9672. This indicates a relatively low correctness value in classifying positive instances and a limited ability to capture them, reflected by a high false positive rate (FPR) and false negative rate (FNR), although the high AUC suggests strong discriminatory power. For the NF-BoT-IoT dataset, 1D-CNN reached 80.58% correctness value, with ppv of 0.4319, recall of 0.3934, F1 measure of 0.3966, and AUC of 0.8451. This demonstrates adequate efficiency, with adequate FPR and FNR, and a reasonable AUC. In the NF-ToN-IoT dataset, 1D-CNN achieved 66.97% correctness value, with ppv of 0.3275, recall of 0.3288, F1 measure of 0.3118, and AUC of 0.8365. These results reflect low ppv and recall, high FPR and FNR, and adequate discriminatory power. For the NF-CSE-CICIDS2018 dataset, 1D-CNN attained 97.04% correctness value, with ppv of 0.6682, recall of 0.6291, F1 measure of 0.6134, and AUC of 0.9810. This indicates a adequate ppv and recall, showing reasonable efficiency overall, with strong discriminatory power. Lastly, for the NF-UQ-NIDS dataset, 1D-CNN achieved 83.99% correctness value, with ppv of 0.4165, recall of 0.3316, F1 measure of 0.3000, and AUC of 0.9506. This reflects adequate efficiency, with high FPR and FNR, and good discriminatory power.

XGBoost

For the NF-UNSW-NB15 dataset, XGBoost attained a correctness value of 98.00%, with a ppv of 0.5924, recall of 0.5689, F1 measure of 0.5759, and AUC of 0.7894. This indicates adequate efficiency, with potential for improving the correctness value of positive predictions and capturing more positive instances. In the NF-BoT-IoT dataset, XGBoost reached 80.03% correctness value, with ppv of 0.6265, recall of 0.5809, F1 measure of 0.5999, and a low AUC of 0.4572, suggesting adequate efficiency but significant room for improvement in distinguishing between classes. For the NF-ToN-IoT

dataset, XGBoost achieved 71.99% correctness value, with ppv of 0.5436, recall of 0.5050, F1 measure of 0.4896, and a low AUC of 0.5284, reflecting similar adequate efficiency and potential for enhancement. In the NF-CSE-CICIDS2018 dataset, XGBoost reached 98.06% correctness value, with ppv of 0.7156, recall of 0.6829, F1 measure of 0.6716, and AUC of 0.8378, indicating high correctness value and substantial discriminatory power. Lastly, for the NF-UQ-NIDS dataset, XGBoost achieved 94.35% correctness value, with ppv of 0.6806, recall of 0.5951, F1 measure of 0.5971, and AUC of 0.7462, showing good efficiency but room for improvement in capturing more positive instances and refining discriminatory power.

Comparative Analysis

The devised 1D-CNN and XGBoost algorithm efficiency is assessed by utilizing efficiency metrics including F1 measure, recall, ppv, correctness value, and AUC. These metrics signifies that framework is accomplishing competent in identifying positive samples, with a high degree of ppv and recall, and a balanced F1 measure. The devised algorithms 1D-CNN and XGBoost have performed with great efficacy on all the datasets. Their efficiencys are compared among themselves and ae well as to state-of-art ensemble tree classifier proposed in [19].

Binary Class Classification

For the NF-UNSW-NB15 dataset, XGBoost achieved the highest correctness value of 99.01%, outperforming both Ensemble Tree and 1D-CNN. XGBoost also demonstrated superior ppv (0.9547), recall (0.9267), and F1 measure (0.9402), although 1D-CNN had a higher AUC of 0.9960 compared to XGBoost's 0.9267. In the NF-BoT-IoT dataset, XGBoost again led with 99.25% correctness value, surpassing both Ensemble Tree and 1D-CNN in ppv (0.9742) and F1 measure (0.9060), though 1D-CNN had a higher AUC of 0.9866. For NF-ToN-IoT, XGBoost achieved the highest correctness value (99.96%), ppv (0.9994), recall (0.9992), F1 measure (0.9993), and AUC (0.9992), outperforming Ensemble Tree and 1D-CNN in all metrics. In the NF-CSE-CICIDS2018 dataset, XGBoost scored the highest in correctness value (99.35%), ppv (0.9960), and F1 measure (0.9844), though 1D-CNN had a higher AUC (0.9861). Finally, for NF-UQ-NIDS, XGBoost led with 99.29% correctness value, ppv (0.9936), recall (0.9865), F1 measure (0.9900), and AUC (0.9865), outperforming both Ensemble Tree and 1D-CNN. Overall, XGBoost consistently demonstrated superior efficiency across most datasets, excelling in recall, ppv, correctness value, F1 measure, and Area under the curve.

Table 2.
Binary Class Classification Results for 1D-CNN and XGBoost

Datasets	**NF-UNSW-NB15**		**NF-BoT-IoT**		**NF-ToN-IoT**		**NF-CSE-CICIDS2018**		**NF-UQ-NIDS**	
Algorithms	1D-CNN	XGBoost	1D-CNN	XGBoost	1D-CNN	XGBoost	1D-CNN	XGBoost	1D-CNN	XGBoost
Training Correctness value	97.95%	99.19%	98.59%	99.39%	98.55%	99.99%	99.17%	99.34%	97.51%	99.30%
Testing Correctness value	98.63%	99.01%	98.75%	99.25%	98.45%	99.96%	99.12%	99.35%	89.53%	99.29%
Ppv	0.9419	0.9547	0.9577	0.9742	0.9867	0.9994	0.9911	0.9960	0.8581	0.9936
Recall	0.8924	0.9267	0.7501	0.8556	0.9641	0.9992	0.9678	0.9734	0.8427	0.9865
F1 measure	0.9156	0.9402	0.8221	0.9060	0.9749	0.9993	0.9791	0.9844	0.8499	0.9900
AUC	0.9960	0.9267	0.9866	0.8556	0.9958	0.9992	0.9861	0.9734	0.7820	0.9865

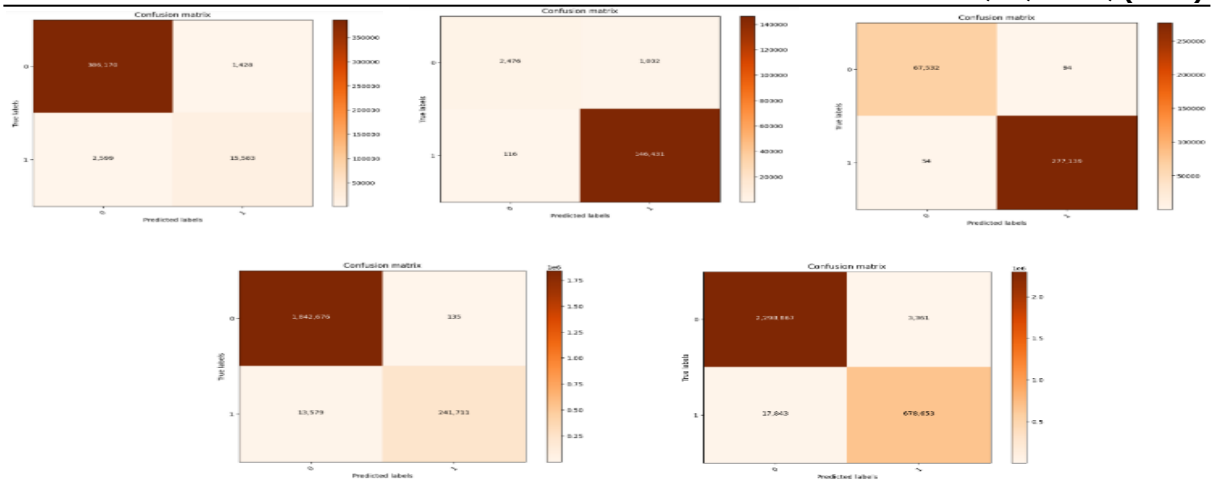

Figure 4.
(Left to Right) Confusion Matrix for NF-UNFW-NB15, NF-boT-IoT, NF-ToN-IoT, NS-CLE-CICIDS2018, NS-UF-NITS Binary class classification evaluated through XGBoost Algorithm

- Implemented using Python and the scikit-fuzzy library, extended to support Q-rung operations.

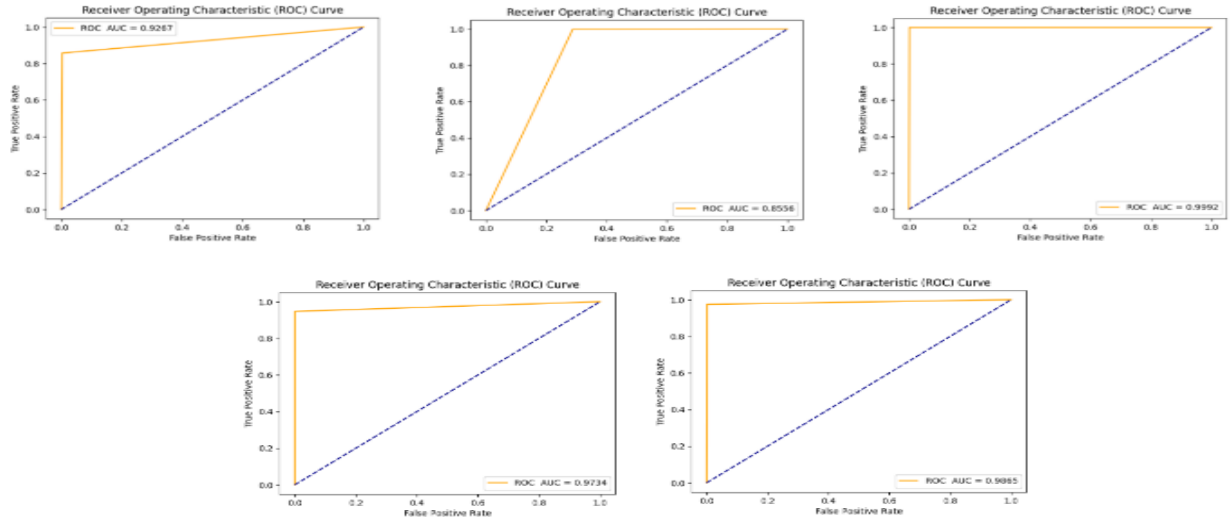

Figure 5.
(Left to Right) ROC Curve for NF-UNW-NS15, NS-boT-IoT, NF-FoN-IoT, NF-CSE-CICIDS2018, Ns-UF-NTTS Binary class classification evaluated through XGBoost Algorithm

Table 1.
Multi-Class Classification Results for 1D-CNN and XGBoost

Datasets	**NF-UNSW-NB15**		**NF-BoT-IoT**		**NF-ToN-IoT**		**NF-CSE-CICIDS2018**		**NF-UQ-NIDS**	
Algorithms	**1D-CNN**	**XGBoost**	**1D-CNN**	**XGBoost**	**1D-CNN**	**XGBoost**	**1D-CNN**	**XGBoost**	**1D-CNN**	**XGBoost**
Training Correctness value	96.60 %	98.53%	83.22 %	85.98%	69.14 %	72.67%	97.73 %	98.06%	92.89 %	94.48%
Testing Correctness value	96.86 %	98.00%	80.58 %	80.03%	66.97 %	71.99%	97.04 %	98.06%	83.99 %	94.35%
Ppv	0.3758	0.5924	0.4319	0.6265	0.3275	0.5436	0.6682	0.7156	0.4165	0.6806
Recall	0.2851	0.5689	0.3934	0.5809	0.3288	0.5050	0.6291	0.6829	0.3316	0.5951

F1 measure	0.2944	0.5759	0.3966	0.5999	0.3118	0.4896	0.6134	0.6716	0.3000	0.5971
AUC	0.9672	0.7894	0.8451	0.4572	0.8365	0.5284	0.9810	0.8378	0.9506	0.7462

The most optimal framework depends on the specific needs and significances of the task. XGBoost's overall strong efficiency makes it a favorable choice when accurately classifying instances and capturing positive instances are crucial. However, if a high AUC and differentiation between positive and negative instances are of utmost importance, 1D-CNN may be considered.

CONCLUSION

This study implemented and evaluated the effectiveness of 1D-CNN and XGBoost, comparing them with the cutting edge ensemble tree classifier across both multiclass and binary classification tasks on five NetFlow datasets: NF-USNW-NB15, NB-FoT-IoT, NT-ToN-IoT, NF-CSE-CICIDS2018, and NF-QU-NDS. Both methodologies surpassed the ensemble tree classifier, (Rashid et al., 2022) each offering unique strengths for different scenarios. XGBoost consistently achieved the highest correctness value, showcasing its superior ability to correctly classify instances. It also demonstrated high ppv and recall, effectively capturing and predicting positive instances. XGBoost's exceptional F1 measure underscores its overall efficiency in balancing ppv and recall. While 1D-CNN exhibited higher AUC scores on some datasets, XGBoost's robust efficiency across various metrics establishes it as the superior model.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally in the creation of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Bui, H. T., Aboutorab, H., Mahboubi, A., Gao, Y., Sultan, N. H., Chauhan, A., ... & Yan, S. (2024). Agriculture 4.0 and beyond: Evaluating cyber threat intelligence sources and techniques in smart farming ecosystems. Computers & Security, 103754.

Caton, S., & Haas, C. (2024). Fairness in machine learning: A survey. ACM Computing Surveys, 56(7), 1–38.

Check Point Research. (2023). Cyber Security Report 2023.

DataReportal. (2023). Digital 2023 Global Overview Report. Retrieved from https://datareportal.com/reports/digital-2023-global-overview-report

Jain, V., Yie, L. W., & Teyarachakul, S. (2024). Convergence of IoT, blockchain, and computational intelligence in smart cities (R. Kumar, Ed.). CRC Press.

Jimmy, F. N. U. (2024). Cyber security vulnerabilities and remediation through cloud security tools. Journal of Artificial Intelligence General Science (JAIGS), 2(1), 129–171.

Kizza, J. M. (2024). System intrusion detection and prevention. In Guide to computer network security (pp. 295–323). Cham: Springer International Publishing.

Lavanya, V. S., & Anushiya, R. (2024). A novel autoencoder-based federated deep transfer learning and weighted k-subspace network clustering for intelligent intrusion detection for the Internet of Things. Salud, Ciencia y Tecnología–Serie de Conferencias, 3.

Mapari, S., Veeraiah, V., Manchala, M., Dhamodaran, S., Anand, R., & Kaur, S. (2024, March). Challenges in remote big data transmission in IoT environment. In 2024 2nd International Conference on Disruptive Technologies (ICDT) (pp. 1464–1468). IEEE.

Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. World Journal of Advanced Research and Reviews, 21(1), 2286–2295.

Rashid, M., et al. (2022). A tree-based stacking ensemble technique with feature selection for network intrusion detection. Applied Intelligence, 52(9), 9768–9781.

Ren, Z., Wang, S., & Zhang, Y. (2023). Weakly supervised machine learning. CAAI Transactions on Intelligence Technology, 8(3), 549–580.

Saeed, M. M. (2022). A real-time adaptive network intrusion detection for streaming data: A hybrid approach. Neural Computing and Applications, 34(8), 6227–6240.

Sarhan, M., Layeghy, S., Moustafa, N., & Portmann, M. (2021). NetFlow datasets for machine learning-based network intrusion detection systems. In Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (LNICST) (Vol. 371, pp. 117–135).

Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing network security in industrial IoT: A deep dive into AI-enabled intrusion detection systems. Advanced Engineering Informatics, 62, 102685.

Siddiqui, A. (2023). SUTMS–Unified threat management framework for home networks.

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges, and solutions. Journal of Ambient Intelligence and Humanized Computing, 1–18.

Taofeek, A. O. (2024). Development of a novel approach to phishing detection using machine learning. ATBU Journal of Science, Technology and Education, 12(2), 336–351.

Zafar, A., Aamir, M., Nawi, N. M., Ali, S., Husnain, M., & Samad, A. (2022). A comprehensive convolutional neural network survey to detect glaucoma disease. Mobile Information Systems, 2022(1), 3971516.