JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 02
2025

Research Article
https://doi.org/10.56979/902/2025

A Hybrid Intrusion Detection System for Security of Edge-Based IIoT

Nimra Sajjad Hussain[1], Amna Sattar[1], Mariam Fiaz[1], Hira Mustafa[1*], Zainab[1], and Soha Ali[1]

[1]Department of Computer Science, Bahauddin Zakariya University, Multan, 60000, Pakistan.
[*]Corresponding Author: Hira Mustafa. Email: hiramustafa20@gmail.com

Received: July 05, 2025 **Accepted:** August 20, 2025

Abstract: Emergence of cloud computing and IoT technology in healthcare, telecommunications and Industry 4.0 (IIoT), has revolutionized most of the daily services. But this development has also made the aspect of security to be more advanced and complicated. IIoT system security is one of the primary concerns of any industry and researchers. IDS have also materialized as a key part of identifying malicious activity and in attempts to further enhance the security of the IIoT networks. IDS are highly adopted in detecting the real time attacks and making secure decisions. This study proposes a machine learning base intrusion detection system comprises of PCA and XGBoost for edge-based IIoT. The framework combines the techniques of misuse and anomaly detection. It employs Principal Component Analysis (PCA) for dimensionality reduction of the features and Extreme Gradient Boosting (XGBoost) as the intrinsic classifier. PCA makes training faster whereas XGBoost makes detection more accurate The system is evaluated using NSL-KDD and Bot-IoT benchmarks. On NSL-KDD, It obtained detection rate of 98.5%, accuracy of 99.2% and false alarm of 2.6%. It recorded 98.3% accuracy, 97.7% detection rate and 2.8 % false alarm rate on Bot-IoT. These findings indicate that the suggested framework is superior to current IDS models.

Keywords: Edge-based IIoT; IoT Security; Intrusion Detection; Machine Learning; PCA; XGBoost; NSL-KDD; Bot-IoT

1. Introduction

In the age of cloud computing and Industry 4.0, network security and protection of confidential information is becaming more challenging. Both to corporations and individual users can get effective and precise services from these technologies[1-4]. Industry 4.0 is a synonym of IIoT, based on the optimal industrial processes with the help of smart sensors and actuators. These smart edge devices communicate through various network connectivity [5]. With the spreading of IIoT installations, the issue of their safety has also become more challenging. The protection of IIoT network requires sophisticated systems that protect data stores as well as network-attached devices [6, 7]. IDS's are the most common of these solutions that detects both intrusions and malicious activities [8, 9]. A hybrid method, which is a combination of both methods, Often is used to improve the detection accuracy and to increase the overall detection rate [9-11] HIDS and NIDS are two general categories of IDSs [12]. Some of the limitations of IDS are difficulties in real-time invalidation, an abundance of data, and excessive alarms that may limit their precision and detection capability [13]. Two types industrial Intrusion Detection System (IDS) methods are used for Industry which cab be divided into knowledge-based and anomaly-based methods. Nevertheless Traditional rule-based strategies struggle to detect new or unexplored intrusion patterns [5]. To address such limitations, there are several Machine Learning (ML) methods to learn on training data and develop effective detection models that will detect new and unknown threats in a flexible and correct manner. Generalized learning can process unseen data, so it has a better fit on IIoT edge devices where the learning process has to be relatively fast and computational resources are very limited Intrusion detection is an emerging area of research and active research is underway in developing and better methods are explored

by feature engineering [14-16]and improvements in data quality [17]to achieve better and stronger decisions, and better classifiers [18, 19].

We propose and evaluate an effective HID framework known as PCA and XGBoost-based Intrusion Detection System (PX-IDS). The framework uses Principal Component Analysis (PCA) as a method of reducing dimensions and better feature engineering using network traffic data. At the same time, the XGBoost algorithm is used to develop a binary classification model, which is able to make confident decisions on intrusions detection without false positives. Fundamentally, there are two major contributions that the research intends to verify. First, we present feature engineering technique utilizing PCA to enhance the data preprocessing stage in order to ensure the work effectiveness of the XGBoost classifier for simulating intrusion classification with a certain accuracy. Second, we suggest a hybrid system that can consist of misuse detection, which should be accomplished through integration with the SID , and anomaly detection, that can be done with the help of our PCA-enhanced feature selection and XGBoost-based classification.

Evaluation experiments with Bot-IoT and NSL-KDD datasets indicate that PX-IDS performs very well in regard to accuracy (ACC) and detection rate (DR). PX-IDS has much better accuracy, reliability, and data quality compared to the current methods of detection. Section 2 review the previous research on intrusion detection in IoT and IIoT and pay specific attention to ML-based methods applied to boost the level of intrusion detection. In section 3, proposed elements of the PX-IDS framework and its architecture will be described. Section 4 describes the experimental setup. Comparison of the results achieved by the proposed framework with the other existing methods in discussed in section 5. Lastly, the paper ends with the conclusion of the main findings and future research.

2. Literature Review

This section provides a survey of some of the well-known studies regarding intrusion detection, especially, researches that use machine learning (ML) methods to strengthen data and network security. Intrusion detection in IoT is a major and complicated issue. Various intrusion detection systems (IDSs) have incorporated the use of ML and DL in overcoming a variety of attack vectors. The studies further boast of enhanced detection models after utilizing the DL models like CNN [20] and LSTM [21]. Other widely used algorithms are MLP [22], KNN [23], SVM [24], NB [25] and DT[21, 24]. Debateably, a good case study is introduced by [13], who gave the hybrid IDS which added a variety of classifiers, such as Decision Tree, REP Tree, JRIP, and Forest PA, and by which they measured their results on the CICIDS2017 dataset. Moreover, feature engineering has been highlighted as an important process to enhance the preprocessing and increase the accuracy of the classification [26]. In study [27] introduced an IDS that combined DL with the SVM, Random Forest (RF), DT, and NB to achieve better scalability, and tested it on the dataset of UNB ISCX 2012. On the same note, study [7] came up with a hybrid CNN-LSTM IDS that was evaluated using ISCX2012 and UNSW-NB15 data. Moreover, [28] developed an IDS based on reinforcement learning and tested it on NSL-KDD, UNSW-NB15, as well as AWID datasets.

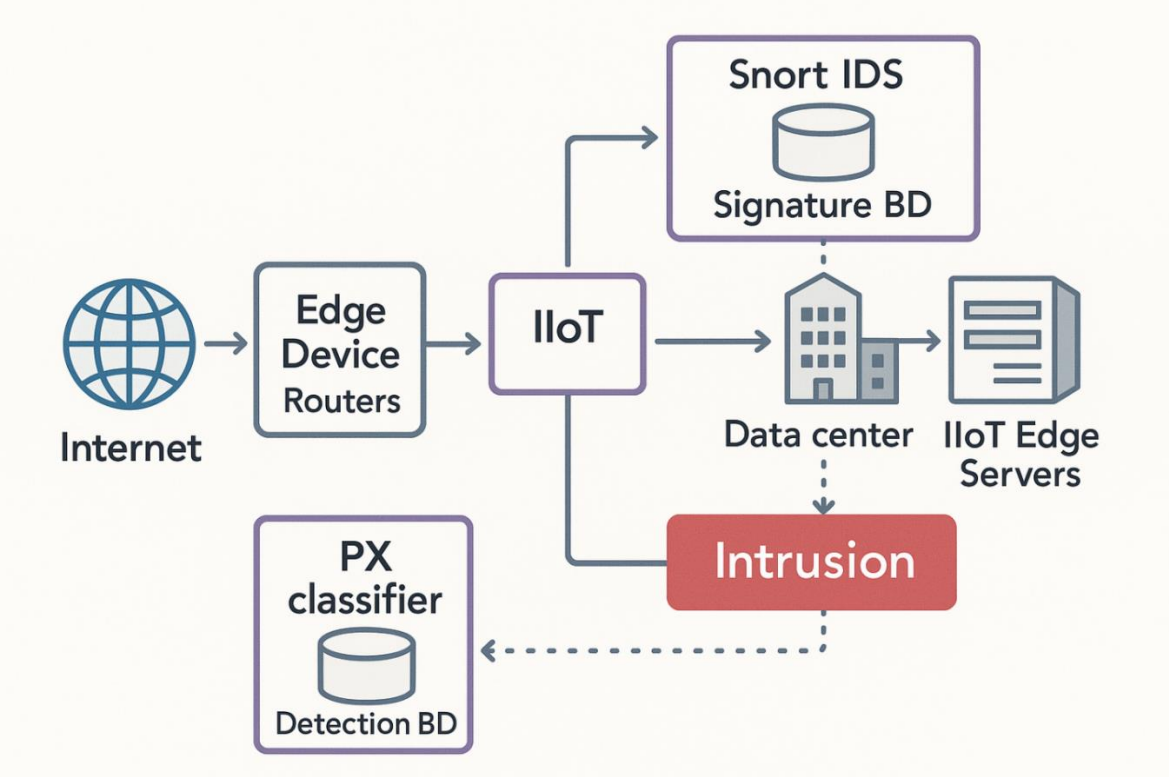
Also, the study [29]constructed an IDS DL in relation to a double PSO metaheuristic and confirmed its performance on CICIDS2017 and NSL-KDD. [3] created an auxiliary IDS in cloud landscape by uniting feature engineering through genetic associations and categorization using the KDD CUP 1999 data. [17]created an IDS system that uses MLP classifier and PcapSocks sniffer to detect network traffic and label it as either a normal or an intrusive activity. At present, the majority of the suggested intrusion detection systems (IDSs) focus on feature selection methods or dimensionality reduction approaches [18, 30] to get rid of irrelevant features that can compromise the accuracy of the detection. Feature engineering aims at retrieving sensible and compressed input features that make the IDS models better [15, 25] . This paper [22] presented a fully featured IDS, based on the SVM ensemble as a classifier and Naive Bayes (NB) as an augmenter of features, and tested on benchmark datasets, including UNSW-NB15, NSL-KDD, CICIDS2017, and Kyoto2006+. Likewise,[24] proposed a combination of IDS that comprises NB and deep learning in which a genetic algorithm is used to choose the best features. The study [26] has proposed a hybrid intrusion detction system using the KNN, RF and XGBoost. [15]built a deep learning-based IDS optimized with a rule-based hybrid feature selection technique, and measured on UNSW-NB15 dataset. The special features identified in an IDS proposed by[25]on the basis of a probabilistic approach, with inclusion of a BRS technique to categorize samples as normal, intermediate or abnormal, was tested on different datasets

To enhance the data quality and model precision, [30] introduced a more optimal IDS based on multi-class SVM and multi-linear dimensionality reduction which is verified with NSL-KDD.

Besides, recent studies have also intensive on combining ML and DL approaches suitable for IoT enabled environments. As an example, [3]introduced the network-based IDS with the ML algorithms and addressed open-source platforms and benchmarking datasets to understand IoT intrusion detection. In [13] hybrid intrusion detection system (IDS) with combination of stacked auto-encoder and Support Vector Machine (SVM) kernel approximation method was proposed specifically designed to work in IoT environments. Purposed model was evaluated on NSL-KDD dataset. In their work, [31] also proposed a new system of anomaly detection that used an SVM-based classifier provided at an excellent result of 99.71% accuracy (ACC) and 98.8% detection rate (DR) on the same dataset. [32] have designed anomaly detection framework on machine learning algorithms to protect the IoT against DoS attack. They scored well on CIDDS-001, UNSW-NB15, and NSL-KDD datasets and achieved 96.74% ACC, a 97.5% DR on AdaBoost, and 97.3 sensitivity with Random Tree (RF) and XGBoost (XGB). The study [33] proposed a cybersecurity-oriented IDS named IntruDTree, in which feature selection is added to improve precision. A model was able to achieve good results in 98 percent ACC and 98 percent DR. the study [20]proposed various ML classifiers including NB, SVM and AdaBoost to detect the MITM attacks in IoT networks. On a dataset consisting of 480 sensor records the model reported 98% accuracy and DR; 98% accuracy and 98% DR with Support Vector Machine and AdaBoost; and 97% accuracy and 96% DR with Naive Bayes. However, these developments have not led to the successful development of an effective and robust IDS that can be applied in edge-based IIoT systems because of accessibility to resources, real-time demands, and heterogenous threat environments. The analysis of the available literature shows that learning algorithms and feature engineering are important when it comes to enhancing the IDS accuracy, performance, and overall performance.

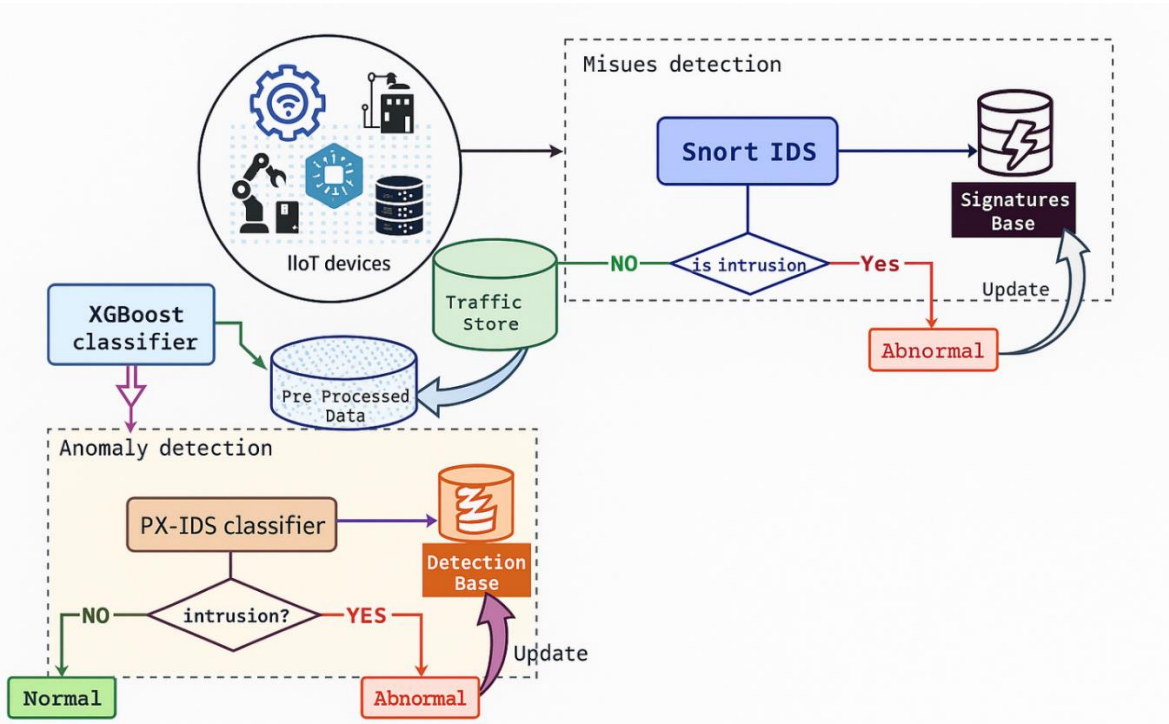
3. Proposed Model

Our hybrid system is designed in accordance with a typical suite of IDS elements distinguished in [17, 34, 35] as four main parts, namely data collection, preprocessing, decision layer and response.The proposed system is shown in Figure 1 and is a hybrid prototype consisting of signature-based detection with Snort IDS and anomaly-based detection mechanism of the XGBoost classifier.



FigureError! No text of specified style in document. **1.** The proposed model for the security of edge based IIoT

In Figure 2, the specific implementation stages of the framework are shown. This is a centralized design, which is installed on a central server with a strong memory and high computing capacity, which enables the framework of the IDS to process extensive jobs. This is especially critical in the light of the adoption of complex ML methods which require a lot of time and memory to compute. Data preprocessing and feature engineering are implemented during the data collection, which is needed to optimize performance to reduce time complexity and decrease the load on IIoT edge resources. As illustrated in Figure 2, the proposed PX-IDS architecture has five major units.



FigureError! No text of specified style in document. **1.** PX-IDS framework for the security of edge based IIoT

3.1. Abuse Detection

Snort IDS is used to perform Abuse Detection. Once a packet has been captured, it is checked and compared with a signature database of pre-established attack rules. In case of match, the system generates an alert with the details about the type of the attack, updates the signature database, and takes an appropriate decision. The normal packets, however, are not tagged and sent to the next layers of the framework.

3.2. Preprocessing and Normalization

Preprocessing and normalization are important aspects in our practice that improve the quality of data. The preprocessing step assists in removing noise and cleaning up the data, and normalization rescales the data between the limits [16] wherein the min-max technique is adopted. This avoids having use of features with large values that will have a disproportionate effect on the model. Each feature is recalculated to have a new value as:

Normalizing the range of a feature variable (since Min and Max are the minimum and maximum value of a particular feature): normalize all the values of features to range 0,1.

3.3. Feature Engineering

At implementation level, we will extract a subset of features to resolve the problems associated with high volumes of data and overhead processing. There are several approaches that can be used to minimize the amount of features prior to training and validating of the model with the use of the dataset. In our example we involve Principal component analysis (PCA), a statistical method that consolidates the number of dimensions of information keeping the key information. This reduction in features reduces the training time and computational costs and also increases the quality of data allowing us to create a better classifier in the PX-IDS framework..

3.4. Training and Validation

In order to endorse our proposed model, we implement the use of 10-fold cross-validation technique which is suggested in [36]. The method splits the data into ten parts equally. Training is done using nine parts and the rest part is used to test. This is repeated ten times and in this way the model is proficient and tested on a diverse subset of data. During the training and validation stages, only the features that pass a given criterion are used to achieve the highest performance of the model.

3.5. Classification

The last phase is classification where the trained classifier gives a class name to each new instance. Through XGBoost algorithm, the model estimates the category of the incoming data relative to the patterns learnt during the training step.

4. Experimental Setup

In this section, the description of the datasets that are involved in experiments and the environment of the evaluation are described, also present the outcomes of performance and compare our suggested method with other studies published in the past.

4.1. Dataset Description

Selection and testing of datasets are critical in justification of intrusion detection methods. IDS models most commonly trained on several publicly available datasets are evaluated against machine learning techniques[35, 37, 38]. In this research, we will use two datasets one is Bot-IoT dataset and other is NSL-KDD dataset to train our model, evaluate our model and then validate the model. These data sets are popular, particularly in IDS.The Bot-IoT dataset was generated in the Cyber Range Lab at UNSW Canberra Cyber, in a simulated network environment designed to be realistic and contains normal network activity and malicious activity.Service scans, DoS, DDoS are the types of attacks present in this dataset. It is made of Pcap files that take 69.3 GB plus 72 million records, and CSV files that require 16.7 GB. Information is divided into several categories and subcategories, offering a wide range of network traffic to be analyzed [35]. Bot-IoT provides large scale, realistic IoT traffic comprising various botnet-driven attacks (e.g., DDoS, DoS and information theft) which is very well suited for evaluating the detection accuracy and scalability under next-generation IIoT circumstances. In contrast, NSL-KDD is a datalink level benchmark dataset but is still widely used and contains several intrusion categories (DoS, Probe, U2R and R2L) that are relevant in IIoT scenarios where legacy equipment and insecure protocols might be employed.

The original KDD Cup 99 dataset [27, 38] serves as the basis of NSL-KDD dataset. It has 125,973 records of which 113,000 records are training and 22,544 texts of which can be used to test it. In the training data set, there are 22 types of attacks, 41 features, of which 21 characterize the connection itself and 19 the character of the connection of the same host. The NSL-KDD dataset can be described as one of the most useful and convenient resources to conduct intrusion detection research due to the novelty and the number of instances. The Bot-IoT and NSL-KDD is publicly available as used in this research. The Bot-IoT data is located at Bot-IoT Dataset and NSL-KDD dataset is located at NSL-KDD Dataset.

5. Results Discussion

The performance of XGBoost classifier is tested after the pre-processing stage and feature engineering is performed on the gathered traffic data. In determining the level of effectiveness of the model, various common performance measurements are used, namely Accuracy (ACC), Detection Rate (DR), False Alarm Rate (FAR), and the F-score. These evaluation measures are computed using the confusion matrix on which they are structured evaluation measures of the classifier prediction versus actual labels. The confusion matrix is a summary of the distribution of true positive, true negative, false positive, and false negative, thus, providing an insight on the degree to which the XGBoost model distinguishes between normal and anomalous traffic. The confusion matrix used in this evaluation is indicated in Table1.

Table 1. Confusion Matrix

		Predicted Label	
Actual Label		Attack	Normal
	Attack	TP	FN

	Normal	FP	TN

The metrics used in the evaluation of the performance of the classifiers in this study are as follows:

5.1. Accuracy

This measurement is the percentage of correctly identified test examples, which will be classified as normal or attack, to the total number of test samples. Stated differently, it is the overall predictive accuracy of the classifier. ACC is described mathematically in the equation (1).

$$Accuracy = \frac{TP+TN}{(TP+TN+FP+FN)} \quad (1)$$

5.2. Detection Rate

The detection rate describes how many attack cases are accurately recognized as attacks by the classifier. It gives a pointer of how the system is effective in identifying malicious activity. DR is given by the formal definition of Equation (2).

$$Detection\ Rate = \frac{TP}{(TP+FN)} \quad (2)$$

5.3. False Alarm Rate

This measure defines the percentage of normal cases which are wrongly considered attacks. The lower FAR value is a positive indicator of the model to not provide false positives, which is essential in the context of minimizing false alerts in practice. FAR is determined as expressed in Equation (3).

$$FAR = \frac{FP}{(FP+TN)} \quad (3)$$

In this paper, we start our discussion by comparing the performance of our proposed method with the baseline XGBoost classifier in the detection. The comparative findings, as depicted in Figures 3 and 4, demonstrate the disparities in terms of ACC, DR and FAR when used on two benchmark datasets, namely Bot-IoT dataset and NSL-KDD dataset. These visual comparisons give the information to understand to what extent the proposed method can be more effective than the traditional XGBoost model in terms of detection performance.

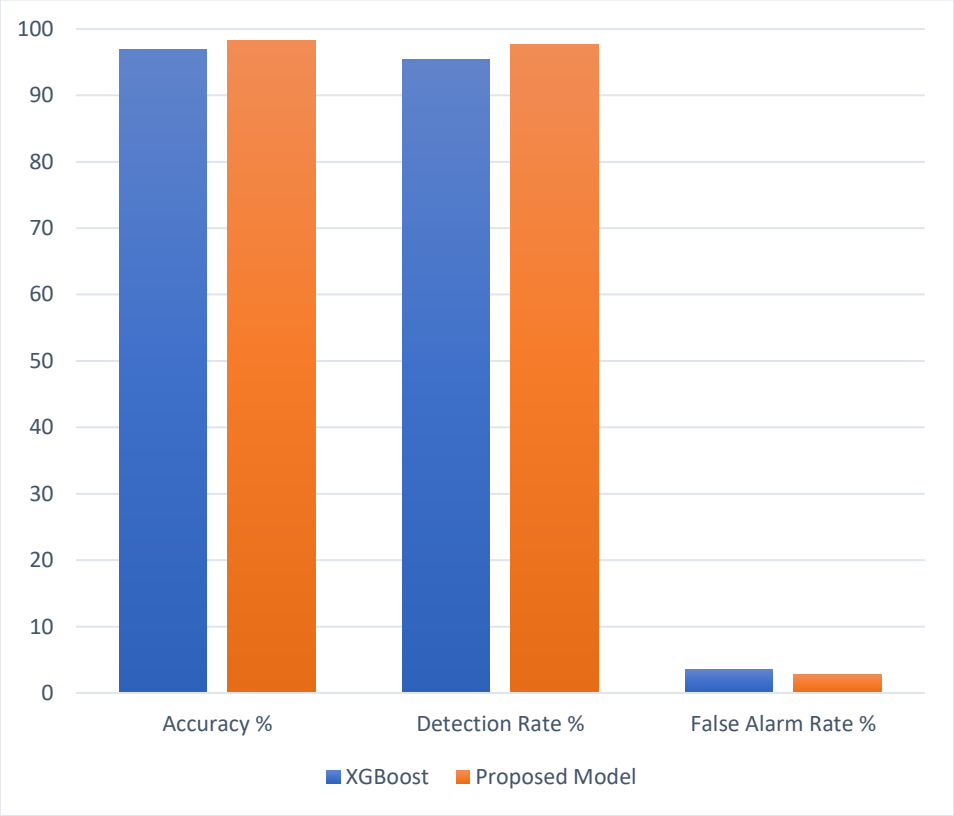


Figure Error! No text of specified style in document.**2.** Comparsion of Proposed Model with Baseline Model XGBoost on Bot-IoT Dataset

Table 2 and Table 3 provide the performance comparison of a few anomaly-based Intrusion Detection System (IDS) models applied on two variants of the NSL-KDD dataset, the original binary-class dataset, and a dimensionally reduced dataset (98% variance retained) generated using Principal Component

Analysis (PCA). Based on these tables, it is possible to note that the Accuracy (ACC) and Detection Rate (DR) on the smaller dataset are mostly similar to the ones on larger dataset, which is higher-dimensional. It means that the dimensionality reduction provided by PCA can simplify the data set successfully but maintain the key discriminatory variables.

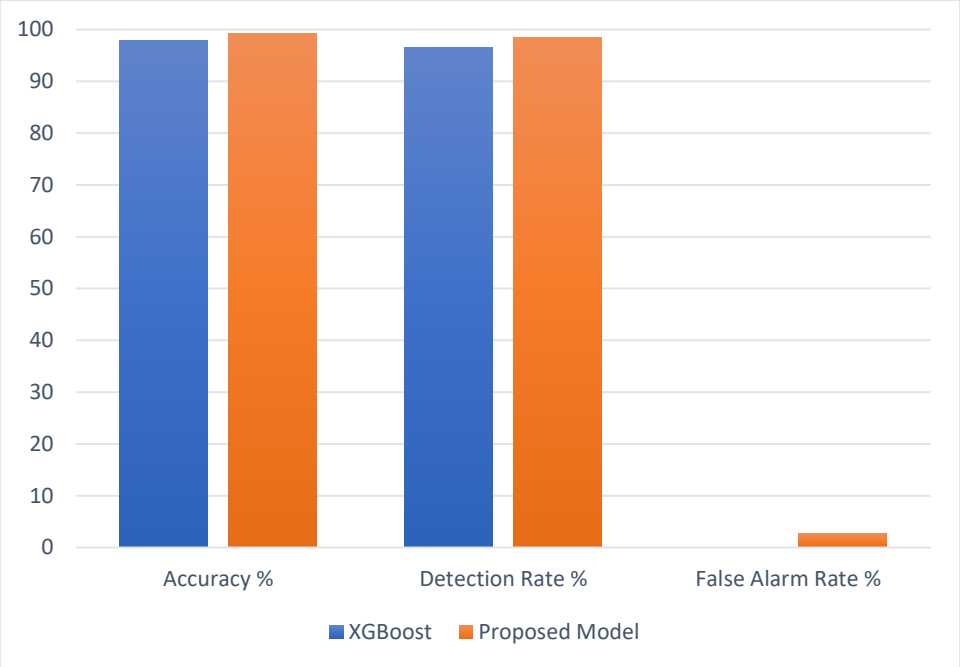


Figure 3. Comparsion of Proposed Model with Baseline Model XGBoost on NSL-KDD Dataset

TableError! No text of specified style in document. **2.** Comparsion of Proposed Model with Baseline Model XGBoost on Bot-IoT Dataset

	Accuracy %	**Detection Rate %**	**False Alarm Rate %**
XGBoost	96.9	95.4	3.5
Proposed Model	98.3	97.7	2.8

Table 3. Comparsion of Proposed Model with Baseline Model XGBoost on NSL-KDD Dataset

	Accuracy %	**Detection Rate %**	**False Alarm Rate %**
XGBoost	97.8	96.6	3.7
Proposed Model	99.2	98.5	2.6

These findings are supported by the results summarized in Tables 2 and 3. In the case of Bot-IoT dataset, the IDS model proposed by us attains a better accuracy of 98.3 percent compared with the baseline XGBoost model at 96.9 percent. The proposed model would have a DR of 97.7% and a FAR of 2.8 for the detection rate and false alarm rate respectively, compared to a lower performance of the XGBoost model with a DR of 95.4% and an FAR of 3.5.

Using our proposed model on NSL-KDD data, we find our model has a very high performance with 99.2% accuracy, 98.5% detection rate, and a loose false alarm rate of 2.6%. On the contrary, the XGBoost model offers an accuracy of 97.8, a DR of 96.6 and a FAR of 3.7.

In general, these findings prove that the suggested IDS model does not only preserve its high performance following dimensionality reduction but also performs much better than the traditional classifiers, i.e., K-NN, decision tree, and XGBoost, in terms of detection effectiveness and reliability.The results obtained allow concluding that the proposed method provides a high level of detection: ACC, DR,

and FAR. To be more precise, the performance indicators of the model show better performance on the NSL-KDD dataset, whereas the marginally lower values are seen on Bot-IoT. However, the results of the evaluation show that the suggested IDS has a high competitive level, in general.

Comparing the results with those of the baseline model based purely on XGBoost, it is obvious that the offered network intrusion detection strategy is rather effective. This model has always shown to give larger values of ACC, DR and smaller FAR thus confirming its strength in detecting malicious traffic at a small number of false alarms. Besides this base comparison, we go further with the analysis and benchmark our IDS with other more recently suggested intrusion detection techniques on the Bot-IoT data and the NSL-KDD data. The state of the-art methods usually combine the machine learning algorithms, including Support Vector Machines (SVM), Naive Bayes (NB), AdaBoost, and Classification and Regression Trees (CART). Table 4 summarizes the comparative outcomes of the detailed comparison results of the study and illustrates further the benefits of the proposed approach over the existing models. Altogether, the IDS approach suggested is effective and reliable with good scores on the Bot-IoT and NSL-KDD datasets. It uses the fast data quality techniques to guarantee effective training and high performance in comparison to other models. Due to its strength, the solution can be incorporated into various systems including the IoT networks and cloud computing systems.

Table 4. Comparsion of Proposed Model with Different models on NSL-KDD Dataset

Reference	Method	ACC %	DR %
[32]	CART	96.6	95.9
[32]	AB	97.8	97.5
[33]	IntruDTree	98.4	98.1
[39]	SVM	98.7	97.8
[39]	NB	97.1	96.4
[39]	Adabost	98.3	98.1
Proposed Model	PCA, XGBoost	99.2	98.5

6. Conclusions

This paper has presented PX-IDS, a hybrid intrusion detection system incorporates Snort IDS to detect misuse, the XGBoost classifier and feature engineering through the use of PCA to boost the capacity to identify anomalies. Data heterogeneity and enhanced training efficiency, accuracy and detection rate were PCA. The model was verified on Bot-IoT and NSL-KDD data sets and shows strong and high-quality results compared with the current methods. Although creating IDS to match edge-based IIoT security is a difficult task, the future development will see the extension of PX-IDS with the implementation of sophisticated artificial intelligence-based approaches specific to IIoT.

References

1. L. Atzori, A. Iera, and G. J. C. n. Morabito, "The internet of things: A survey," vol. 54, no. 15, pp. 2787-2805, 2010.
2. M. Azrour, J. Mabrouki, R. J. S. Chaganti, and C. Networks, "New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT," vol. 2021, no. 1, p. 5546334, 2021.
3. Z. Chiba, N. Abghour, K. Moussaid, M. J. c. Rida, and security, "Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms," vol. 86, pp. 291-317, 2019.
4. A. Čolaković and M. J. C. n. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," vol. 144, pp. 17-39, 2018.
5. H. Yao, P. Gao, P. Zhang, J. Wang, C. Jiang, and L. J. I. N. Lu, "Hybrid intrusion detection system for edge-based IIoT relying on machine-learning-aided detection," vol. 33, no. 5, pp. 75-81, 2019.
6. M. Azrour, J. Mabrouki, A. Guezzaz, A. J. S. Kanwal, and C. Networks, "Internet of things security: challenges and key issues," vol. 2021, no. 1, p. 5533843, 2021.
7. M. Ingham, J. Marchang, and D. J. I. i. s. Bhowmik, "IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN," vol. 14, no. 4, pp. 368-379, 2020.
8. B. I. Farhan, A. D. J. I. J. F. C. S. Jasim, and Mathematics, "Survey of Intrusion Detection Using Deep Learning in the Internetof Things," vol. 3, no. 1, p. 9, 2022.
9. A. Guezzaz, A. Asimi, Y. Asimi, Z. Tbatou, and Y. J. I. J. N. S. Sadqi, "A Global Intrusion Detection System using PcapSockS Sniffer and Multilayer Perceptron Classifier," vol. 21, no. 3, pp. 438-450, 2019.
10. Ü. J. A. I. Çavuşoğlu, "A new hybrid approach for intrusion detection using machine learning methods," vol. 49, no. 7, pp. 2735-2761, 2019.
11. U. Rashid et al., "Anomaly Detection using Clustering (K-Means with DBSCAN) and SMO," vol. 7, no. 02, 2024.
12. G. T. Francis, A. Souri, and N. J. T. o. E. T. T. İnanç, "A hybrid intrusion detection approach based on message queuing telemetry transport (MQTT) protocol in industrial internet of things," vol. 35, no. 9, p. e5030, 2024.
13. S. C. Avik et al., "Challenges in Blockchain as a Solution for IoT Ecosystem Threats and Access Control: A Survey," 2023.
14. H. Alazzam, A. Sharieh, and K. E. J. E. s. w. a. Sabri, "A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer," vol. 148, p. 113249, 2020.
15. F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, and J. B. J. I. S. J. A. G. P. Awotunde, "Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection," vol. 29, no. 6, pp. 267-283, 2020.
16. U. Rashid, A. Abbas, M. M. Aqib, S. H. Shah, U. J. I. J. o. I. S. Khattab, and C. Technologies, "Enhancing Random Forest Performance through Optimal Instance Subset Selection using Genetic Algorithm," vol. 4, no. 2, pp. 27-36, 2025.
17. A. Guezzaz, Y. Asimi, M. Azrour, A. J. B. D. M. Asimi, and Analytics, "Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection," vol. 4, no. 1, pp. 18-24, 2021.
18. A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, "A novel hierarchical intrusion detection system based on decision tree and rules-based models," in 2019 15th international conference on distributed computing in sensor systems (DCOSS), 2019, pp. 228-233: IEEE.
19. P. M. Chanal and M. S. J. W. P. C. Kakkasageri, "Security and privacy in IoT: a survey," vol. 115, no. 2, pp. 1667-1693, 2020.
20. K. S. Kiran, R. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. J. P. C. S. Karthi, "Building a intrusion detection system for IoT environment using machine learning techniques," vol. 171, pp. 2372-2379, 2020.
21. A. Guezzaz, S. Benkirane, M. Azrour, S. J. S. Khurram, and C. Networks, "A reliable network intrusion detection approach using decision tree with enhanced data quality," vol. 2021, no. 1, p. 1230593, 2021.
22. J. Gu, L. Wang, H. Wang, S. J. C. Wang, and Security, "A novel approach to intrusion detection using SVM ensemble with feature augmentation," vol. 86, pp. 53-62, 2019.
23. A. Zaman, S. A. Khan, N. Mohammad, A. A. Ateya, S. Ahmad, and M. A. J. F. I. ElAffendi, "Distributed denial of service attack detection in software-defined networks using decision tree algorithms," vol. 17, no. 4, p. 136, 2025.
24. S. N. Abd, M. Alsajri, H. R. J. I. J. F. C. S. Ibraheem, and Mathematics, "Rao-SVM machine learning algorithm for intrusion detection system," vol. 1, no. 1, p. 5, 2024.
25. M. Prasad, S. Tripathi, and K. J. A. S. C. Dahal, "An efficient feature selection based Bayesian and Rough set approach for intrusion detection," vol. 87, p. 105980, 2020.

26. U. Rashid, M. Qadir, M. Alam, and S. J. T. J. Farid, "A Hybrid Machine Learning Model to Enhance Cybersecurity: An Integration of KNN, RF and XGBoost," vol. 29, no. 04, pp. 25-32, 2024.
27. S. N. Mighan and M. J. I. J. o. I. S. Kahani, "A novel scalable intrusion detection system based on deep learning," vol. 20, no. 3, pp. 387-403, 2021.
28. K. Sethi, E. Sai Rupesh, R. Kumar, P. Bera, and Y. J. I. J. o. I. S. Venu Madhav, "A context-aware robust intrusion detection system: a reinforcement learning-based approach," vol. 19, no. 6, pp. 657-678, 2020.
29. W. Elmasry, A. Akbulut, and A. H. J. C. N. Zaim, "Evolving deep learning architectures for network intrusion detection using a double PSO metaheuristic," vol. 168, p. 107042, 2020.
30. B. N. Kumar, M. S. Bhadri Raju, B. V. J. I. J. o. I. E. Vardhan, and Systems, "Enhancing the Performance of an Intrusion Detection System Through Multi-Linear Dimensionality Reduction and Multi-class SVM," vol. 11, no. 1, 2018.
31. M. Bagaa, T. Taleb, J. B. Bernabe, and A. J. I. a. Skarmeta, "A machine learning security framework for iot systems," vol. 8, pp. 114066-114077, 2020.
32. A. Verma and V. J. W. P. C. Ranga, "Machine learning based intrusion detection systems for IoT applications," vol. 111, no. 4, pp. 2287-2310, 2020.
33. I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. J. S. Khan, "Intrudtree: a machine learning based cyber security intrusion detection model," vol. 12, no. 5, p. 754, 2020.
34. M. A. Ferrag, L. Maglaras, S. Moschoyiannis, H. J. J. o. I. S. Janicke, and Applications, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," vol. 50, p. 102419, 2020.
35. A. Khraisat, I. Gondal, P. Vamplew, and J. J. C. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," vol. 2, no. 1, pp. 1-22, 2019.
36. G. Fernandes Jr, J. J. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. J. T. S. Proença Jr, "A comprehensive survey on network anomaly detection," vol. 70, no. 3, pp. 447-489, 2019.
37. N. Moustafa and J. J. I. S. J. A. G. P. Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," vol. 25, no. 1-3, pp. 18-31, 2016.
38. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE symposium on computational intelligence for security and defense applications, 2009, pp. 1-6: Ieee.
39. S. Mukherjee and N. J. P. T. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction," vol. 4, pp. 119-128, 2012.