INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD)
© 2026 IJNRD | Volume 11, Issue 4, April 2026 | ISSN: 2456-4184 | IJNRD.ORG

A Hybrid Ensemble Learning Framework for Intrusion Detection in Smart City IoT Networks

Ms. P. Isabella
Computer Science Engineering
Karunya Institute of Technology and Science
Coimbatore, India
isabellap@karunya.edu.in

Mr. S. Basil Xavier
Computer Science Engineering
Karunya Institute of Technology and Science
Coimbatore, India
basilxavier@karunya.edu

Abstract
The Internet of Things is being used more and more in cities and this caused security concerns. So it is need to have systems to detect intrusions. The systems now are not perfect. They have problems with amounts of data, noisy information and attacks that change all the time. This paper delineates a structured hybrid ensemble-based intrusion detection system for large-scale smart city IoT environments.This system uses a combination of Bagged Tree learning algorithms and AdaBoost to make detection more accurate. The Internet of Things intrusion detection system is a priority because the Internet of Things is used much. The system also uses a decision tree to reduce features and make it work better. The new way of doing things gets good results on the smart city IoT traffic data. It gets 99.61% accuracy, 99.93% precision, 99.67% recall and 99.80% F1-score. This is better, than Naïve Bayes, Logistic Regression and XGBoost classifiers. The smart city IoT traffic dataset is used to test the system. The hybrid ensemble proposed here exhibits a solid generalization across a wide range of IoT traffic patterns, effectively detecting the dominant and the rarer intrusion behaviors while keeping false alarms relatively low.

Keywords

AdaBoost, Bagged Trees, Ensemble Learning, Intrusion Detection System, Smart City IoT

1. Introduction

1. The integration of IoT technology in cities has made them smarter and more connected. Smart city applications include smart transportation systems, smart energy management, surveillance systems, and healthcare monitoring, all of which require constant data communication between various devices. While this connectivity has improved efficiency and the quality of services, it has also increased the attack surface that can be exploited by malicious users. Traditional intrusion detection systems are generally designed for traditional enterprise networks and are not appropriate for the dynamic and large-scale nature of smart city IoT networks. Signature-based detection approaches are not adaptable to new attacks, and most traditional machine learning approaches are not able to provide stable performance when handling noisy data, imbalanced datasets, and dynamic attack behaviors. This may result in high false positive rates or false negatives, which are not acceptable in critical city infrastructures where security breaches may have severe operational and societal consequences. The most important task in this case is the design of an efficient intrusion detection system with high precision, low false alarms, and real-time analysis capabilities in the context of the IoT infrastructure of the intelligent city. To this end, the paper proposes the investigation of the hybridization of ensemble learning algorithms, taking advantage of the benefits of multiple classifiers and addressing their limitations. This work is dedicated to the topic of intrusion detection in smart city IoT networks. The issues of preprocessing, dimensionality, stability, and scalability in classification have been discussed. Experiments have been conducted on a smart city IoT dataset to compare this model with the conventional baseline classifiers to prove its usefulness. In conclusion, the proposed work introduces a hybrid ensemble-based intrusion detection system that aims for a balance between efficiency, accuracy, and adaptability. The proposed approach, by using a decision tree-based feature reduction technique and an ensemble-based classification approach, offers a scalable and reliable security solution for the next-generation smart city IoT network. Although ensemble-based approaches have been widely investigated as an intrusion detection technique for IoT networks, most of the existing approaches are only capable of functioning based on a single ensemble approach, such as Bagging, Boosting, Stacking, and Voting, among others. However, in contrast to most existing ensemble-based approaches, the proposed approach utilizes a hybrid ensemble approach, where the variance-reducing Bagged Decision Tree and bias-reducing AdaBoost are combined using a weighted fusion technique appropriate for the smart IoT network.

The novelty is based on three key aspects. Firstly and most importantly, the new approach aims to combine the key aspects of bagging and boosting in a way that tackles both the variance and bias aspects simultaneously, thereby providing greater stability in the ever-changing heterogeneous IoT traffic patterns. Secondly, the new approach aims to incorporate the feature importance aspect through a decision tree, thereby ensuring that there is greater dimension reduction while boosting the output in a way that is linked to computational efficiency and real-time processing. Thirdly, the new approach aims to use a weighted probability-based fused output rather than hard voting, as is the case with most traditional approaches.

Furthermore, the framework is tested on a large public IoT intrusion data set, which contains over 1.19 million instances and includes various types of attacks, thereby proving the performance advantages over traditional machine learning and boosting approaches. This dualization of the framework, along with the reduced feature sets, makes this effort different from most other ensemble-based IoT intrusion detection frameworks.

2. Related Works

A more in-depth examination of intrusion detection in IoT networks was performed by Akif et al. (2025). The authors focused on the problem of real-world dataset variability, which usually misleads conventional models in intrusion detection in IoT networks. The authors proposed hybrid machine learning models that combine supervised and unsupervised learning to tackle a real-world IoT dataset. The hybrids demonstrated high accuracy and lower false positives compared to standalone models. The takeaway is that hybrid ML can be a very efficient approach to detecting complex intrusions in IoT networks [1].

As discussed by Alhowaide (2021), the accuracy of IoT intrusion detection systems is impacted by device heterogeneity. The authors proposed an ensemble detection system that combines multiple classifiers. The approach demonstrated enhanced detection efficiency with lower false positives, which is obviously very efficient [2].

Almotairi (2024) highlighted the inefficiency of single-classifier IDS in heterogeneous IoT networks. The authors proposed a heterogeneous stack classifier model for complex attack pattern detection. The findings demonstrated substantial improvements in accuracy, precision, and handling imbalanced datasets, concluding that stack classifiers can greatly enhance IoT intrusion detection in heterogeneous networks [3].

Alotaibi and Ilyas studied how the narrow processing capacity of IoT devices, along with their constantly changing network behavior, generates special vulnerabilities. They proposed an ensemble learning framework that unites several classifiers in order to detect intrusion in real time. Their experiments demonstrated the gains in terms of accuracy, precision, and recall; these features outline ensemble learning as one of the most important tools for the protection of IoT devices from more sophisticated attacks [4].

Amouri et al., in 2024, addressed intrusion detection in IoT networks over variable traffic patterns. They proposed a novel ensemble based on Kolmogorov-Arnold Networks that combined different learning methods in order to enhance detection efficiency. The results showed better accuracy with reduced false positives compared to conventional models, hence proving that advanced ensembles can significantly improve IoT IDS performance [5].

Chatterjee and Hanawal (2021) addressed privacy-preserving intrusion detection in IoT environments. They came up with a hybrid federated learning ensemble that trains models across a large number of IoT devices without necessarily sharing raw data. Results achieved competitive accuracy with data privacy preserved, hence demonstrating the practicality of federated learning in IoT security. A conclusion was reached that hybrid federated learning techniques can enhance intrusion detection while safeguarding user privacy [6].

Olanrewaju-George and Pranggono (2025) addressed the problem of detecting intrusions in IoT environments with limited labeled information. They proposed a federated learning technique based on a mixture of unsupervised and supervised deep learning models. The mixture outperformed all the individual models and the false acceptance/rejection rates. The lesson learned from this study is that federated learning integrated with deep learning can improve effective intrusion detection in IoT [7].

Hammood and Sadiq in their study (2023) examined the limitations of intrusion detection systems when faced with various types of attacks. They proposed an ensemble learning method for improving the efficiency of the machine learning model. From their study, accuracy, precision, and recall were improved when evaluating different IoT data sets. They concluded that an ensemble learning model was an effective method for improving the efficiency of IoT intrusion detection systems [8].

Alashjaee and Alqahtani's (2025) study focused on the method of enhancing the security level of IoT networks using smart detection systems. They developed a feed-forward neural network that is based on machine learning technology in the intrusion detection system. The results indicated high accuracy with fewer false alarms than the current technologies available for use. The researchers' conclusion was that the integration of neural networks with machine learning can offer efficient security to IoT networks [9].

In addition, Khan et al. (2021) stated that, for an effective detection of all types of intrusions, depending only on one model of an IoT intrusion detector may not be sufficient. To deal with these complications, they proposed an ensemble of voting classifiers, and they believed that the use of vote-based classifiers enhanced the efficiency of the IoT intrusion detection systems [10].

Lazzarini et al., in their research [11], focused on the accuracy challenges associated with deep learning techniques for IoT-based Intrusion Detection. In the research, they proposed the use of a stacking ensemble for deep learning models to effectively detect Intrusion Detection System patterns. The proposal was successful, achieving higher accuracy with a lower false positive rate compared to the use of deep learning techniques alone. It was concluded that stacking ensembles provide a reliable and high-performance solution for Intrusion Detection Systems.

On the other hand, the study conducted by Talukder et al. (2024) focused on the discovery of intrusions using highly imbalanced data sets used in IoT applications. The study proposed a machine learning method that incorporates a stacking feature embedding with feature extraction. The researchers found that using this technique is more effective for detecting intrusions without classifying the majority classes. The key conclusion drawn from the study is that the method works effectively with unbalanced data sets to improve the detection of intrusions that occur in IoT applications.[12]

Maidamwar et al. (2023) explored the accuracy issues in the process of IoT intrusion detection by utilizing standard classifiers. They presented the concept of ensemble learning in the process of network intrusion classification. They used the results of the experiment to conclude that the utilization of ensemble learning is an accurate tool to detect network intrusion in IoT networks.[13]

Premalatha et al. and Ramanujam highlighted in 2025 the importance of precise intrusion detection for IoT systems using precise data. The authors introduced an ensemble learning approach that was tested using the CICIoT2023 data set. The effectiveness of the ensemble learning approach in detecting IoT intrusion was proved by the higher accuracy achieved by comparing traditional classifiers, as ensemble learning is valuable for precise intrusion detection.[14]
In another study, Rahman et al. (2025) analyzed the performance of intrusion detection system against different IoT networks. The extensive survey carried out by the authors demonstrated the advantages of ensemble and hybrid models, such as improving accuracy and minimizing false alarms. They concluded that hybrid models and ensemble methods are necessary for enhancing intrusion detection systems in IoT networks [15].

The paper by Saba et al. deals specifically with anomaly detection in an IoT environment by using a CNN model. The researchers designed a CNN model-based intrusion detection system and successfully performed its evaluation, thereby establishing good detection accuracy while reducing false positive rates significantly when compared to traditional machine learning models. The point here is clear: CNN-based techniques can successfully detect anomalies in an IoT environment.[16]

Sanju (2023) deals with the issue of attaining low accuracy for intrusion detection in IoT systems. Their proposed hybrid model uses a combination of metaheuristics with deep learning methods like a recurrent neural network. The authors' findings show improvements in terms of detection rate and reduction of false alarm ratio, thereby confirming that hybridization of metaheuristics with deep learning techniques improves intrusion detection in IoT systems.[17]

Tiwari, and their team highlight the importance of ensuring the security of Internet of Things and cloud environments. They want security systems that can detect intruders, and they developed a detector with this ability, based on deep learning techniques and further augmented with blockchain and federated learning. They note that their results show the importance of combining learning, blockchain, and federated learning to improve the security of IoT and cloud environments significantly.

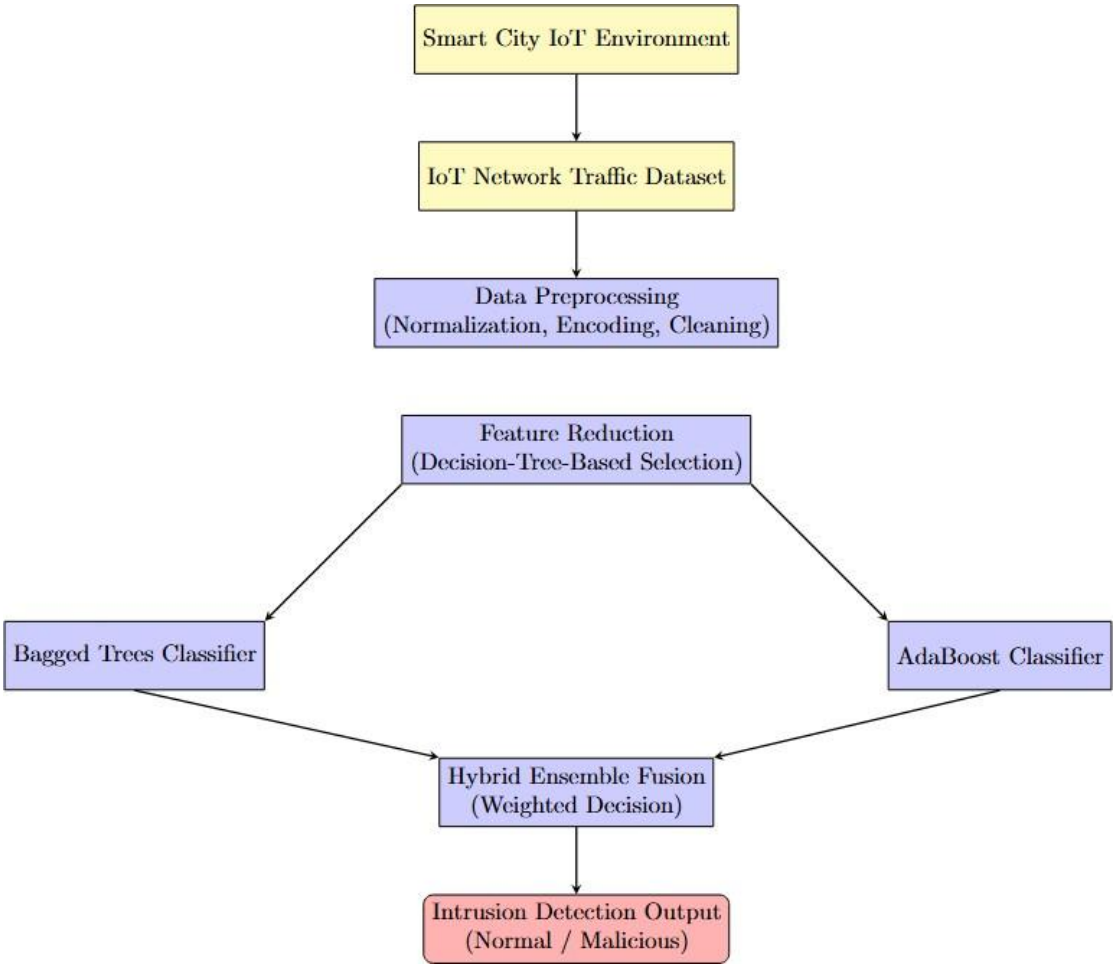
In their latest study, Yin et al. (2023) focus on high-dimensional data in IoT intrusion detection and propose a CNN-based IoT intrusion detection system. In their study, they proved that CNN-based intrusion detection has solid detection accuracy, high feature extraction accuracy, and low false positive rates, indicating its applicability to high-dimensional networks.

Yet again, the importance of efficient Internet of Things (IoT) intrusion detection in heterogeneous networks is emphasized by Rahman et al. (2025). They suggest the use of best techniques through a survey by highlighting ensemble and hybrid techniques as the most efficient methods for intrusion detection in IoT applications.

3. Proposed Framework Formulation to Address Intrusion Detection Issues

The current section outlines an important design structure that can be used to develop an intrusive detection system, targeting its specific use in a Smart City IoT environment. The section discusses commonly encountered issues in a distributed network environment, such as an IoT network, which include changing traffic patterns, numerous and diverse features, and dynamic patterns used in intrusive detection systems. The proposal demonstrates how to seamlessly integrate pre-processing, feature representation, and ensemble-based learning into a singular system, illustrating how pre-processing and representation issues directly relate to ensemble-based strategies and how efficient development of an intrusive detection system is possible to ensure effective classification of an intrusive event while efficiently operating in real-time environments.

3.1 System Model and Assumptions



consider the model of the smart city IoT environment, where numerous devices, such as sensors, controllers, and monitoring devices, are interconnected, resulting in constant network traffic. The traffic is traceable at the monitoring node where the intrusion detector is placed. The environment is assumed to have traffic that contains normal and intrusive behavior, with the latter being less frequent than the former, reflecting the imbalance in the problem. Another assumption in the model is that the traffic features captured from the network flow encapsulate normal and intrusive behaviors. Our model assumes the training, offline model is capable of being run in the online environment without modifying the existing infrastructure.

3.2 Mathematical Formulation of Intrusion Detection

Let the network traffic dataset be represented as

$$\mathcal{D} = \{(x_i, y_i) \mid i = 1,2, \dots, N\},$$

where $x_i \in \mathbb{R}^d$denotes a d-dimensional feature vector corresponding to the i-th network flow, and $y_i \in \{0,1\}$represents the class label, with 0 indicating normal traffic and 1 indicating intrusive behavior. The intrusion detection task is formulated as a binary classification problem that seeks to learn a decision function

$$f: \mathbb{R}^d \rightarrow \{0,1\}$$

such that the predicted label $\hat{y}_i = f(x_i)$minimizes misclassification error. The learning objective is to optimize the classifier parameters so that both false positive and false negative rates are minimized while maximizing overall detection accuracy.

3.3 Data Preprocessing Strategy

Before learning, the raw form of the internet of things traffic undergoes systematic preprocessing in order to achieve consistency and reliability. Continuous features are normalized in order to avoid dominance by features that take larger values, and categorical features are coded in a form that is appropriate for learning. Missing or contradicting observations are treated in a manner that avoids noise. This increases the consistency of the feature space at the learning stage.

3.4 Feature Reduction & Representation Learning

Because the data collected from the IoT are of a high-dimensional type, feature reduction is utilized in order to retain only the most relevant features. Dimensionality reduction based on a decision tree gives importance evaluation on how well each feature discriminates the class, and features with reduced discriminative capability are eliminated.

$$x_i^* \in \mathbb{R}^{d'}, d' \ll d.$$

This reduction not only reduces computing needs but also helps in generalization because it lessens the weightage of irrelevant features and thus helps in ensuring a more robust intrusion detection process.

3.5 Bagged Tree Learning Formula

In bagging, a group of decision-tree classifiers is created based on a set of decision trees bootstrapped from the reduced data. A total of B decision trees, or classifiers {h_b(x)}, are independently developed. Then, the output for the bagged model is obtained by aggregating all outputs. As a result, it can reduce variance, which in turn produces stable output that can be applied for IoT traffic patterns for a large-scale network setup.

$$\hat{y}_{\text{bag}} = \text{mode}\{h_1(x), h_2(x), \ldots, h_B(x)\}.$$

This ensemble mechanism reduces variance and stabilizes predictions, particularly in the presence of noisy or fluctuating IoT traffic patterns, making it well suited for large-scale network environments.

3.6 AdaBoost Learning Formula

AdaBoost increases the detection capability of the system by building the weak learners one after the other while giving more weightage to the misclassified instances. The process begins with assigning the same weights to each training example. The weights for the examples are revised after the end of each iteration 't.' The weak learner is given a weight α_T proportional to the correct classification ratio. The resulting boosting function is created using the weak learners. The adaptive strategy increases the sensitivity of the function towards the minority patterns, including the intrusion attempts.

$$\hat{y}_{\text{boost}} = \text{sign}\left(\sum_{t=1}^{T} \alpha_t \, h_t(x)\right)$$

3.7 Hybrid Ensemble Fusion Strategy

The final intrusion decision is obtained by fusing the outputs of the Bagged Tree and AdaBoost classifiers using a weighted probability-based strategy. This weighted combination achieves a good balance between stability and flexibility, hence providing an accurate intrusion detection scheme that is scalable and has a minimal false alarm rate.

4. Experimental Setup

The experimental design used to test the hybrid ensemble-based intrusion detection system is to ensure its accuracy and effectiveness. The experimental design is modeled to closely resemble a real-world smart city IoT network environment, while also offering a fair platform for comparing the proposed method with other learning approaches.

4.1 Dataset Overview

A publicly available IoT-based intrusion detection dataset from Kaggle, which includes real-world smart city network traffic, including normal and attack-related activities. The dataset includes 1,191,264 network flow records, where each record is associated with 47 distinctive features, covering all the statistical and protocol-related attributes of the network packets. These records comprise seven principal categories of attacks, i.e., DDoS, DoS, Brute Force, Spoofing, Recon, Web Based, Mirai, with numerous subcategories of each diversified type of attack, making it quite complex. In this research, it is considered as a binary-class multiclass classification problem, where all the attack-related categories are combined into a single category of "Intrusion," while normal traffic is considered as "Normal." The precise dataset source along with the repository link will be provided in the final manuscript, which will be used to attain such an experimental set-up.

4.2 Data Preparation and Splitting

Before training our model, some arrangement of preparation had to be done to have a stable dataset for efficient training. The dataset was filtered to remove any inconclusive information and normalized to have equal value range in order to remove any biases in value interpretation. Other categorical information had to be represented in numbers for easier processing in machine learning. After this process, stratified sampling was done to ensure equal proportion in both training and testing sets to include both normal and intrusion patterns.

4.3 Model Setup and Parameter Choices

The proposed framework for intrusion detection integrates the efforts of two ensemble models with parameters set optimally to maintain a balance between precision and speed. In bagging, a series of decision tree classifiers are trained on bootstrapped samples with a limit on decision tree depth to cure overfitting. In boosting, the implementation of the AdaBoost algorithm involves the use of decision trees with limited depth as weak classifiers, enabling the identification and revision of erroneous classifications with precision while maintaining low complexity. The weight parameters of the fusion approach were selected through experiments to ensure balanced participation of the ensemble models. Comparing classifiers with parameters tuned to default values ensures fairness.

4.4 Performance Evaluation Metrics

For the analysis of the proposed framework, usual set of parameters for classification, including those used in studies on intrusion detection. Accuracy was used to measure the total correct classification of instances. For accuracy on preventing false alarms and correctly identifying malicious actions, precision and recall scores were calculated. The F1 scored provided a combined measure when there was class imbalance. Analysis using the confusion matrix provided greater clarification regarding error distribution for each class.

4.5 Environment of Implementation

All experiments were conducted in a controlled computing environment. A high-level programming environment is used for developing this framework, which makes use of available machine learning libraries for data processing tasks. A computing environment is provided that has sufficient processing capabilities for handling IoT traffic efficiently. The computing infrastructure used in this setup helps in the acceleration of the process, thus making it feasible to develop the intrusion detection system.

4.6 Experimental Validation and Statistical Analysis

To ensure the reliability of the results and prevent overfitting, 10-fold stratified cross-validation is used in the project. The dataset is split into ten parts and then used once as a testing dataset and the remaining times as training data. The test used is the average value. A paired t-test at a 95% confidence level was used to evaluate the statistical significance of the performance improvement achieved by the proposed model over the XGBoost algorithm. The hypothesis test concludes that the performance improvement of the presented ensemble model over the XGBoost algorithm is statistically significant because the p-value is less than 0.05. This confirms that the improvement is not resulting from a random phenomenon. Variance value is presented along with the mean value to provide a better understanding of the stability of the performance values.

5. RESULTS AND DISCUSSION

This last section highlights the results of the experiment on the hybrid ensemble-based intrusion detection system and discusses its effectiveness within a real-world smart cities IoT framework.. Various aspects, including its competency level for intrusion detection, comparative efficiency, error dynamics, and feasibility, are also discussed.

5.1 Overall Classification

Performance Hybrid ensemble method performance for classification was strong in all aspects that were evaluated. This was achieved by Bagged Trees and AdaBoost combining to provide high predictability and for capturing the major and minor patterns in the intrusion traffic in the IoT. It appears that the method is well-suited for a situation that considers the cost of error in both alerts and misses.

5.2 Comparative Analysis with Baseline Models

For a better evaluation, the proposed hybrid ensemble was subjected to both classic and slightly more advanced machine learning models. In addition to Naïve Bayes and Logistic Regression, strong ensemble baselines such as Random Forest and XGBoost were added in order to ensure a challenging and fair benchmark. In the future, this could be extended to include comparisons with gradient boosting variants such as LightGBM, and deep learning–based intrusion detection systems-for

example, CNN- or LSTM-based approaches-with the goal of further validating the scalability of the framework. The results indicate that the hybrid ensemble continuously yields higher precision and recall and an F1-score for addressing class imbalance and more complex intrusion patterns.

Table 1: Performance Comparison of Intrusion Detection Models

Model	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Naïve Bayes	95.47	99.97	95.38	97.62
Logistic Regression	97.94	98.77	99.11	98.94
XGBoost	99.47	99.74	99.71	99.73
Hybrid Ensemble (Proposed)	**99.61**	**99.93**	**99.67**	**99.80**

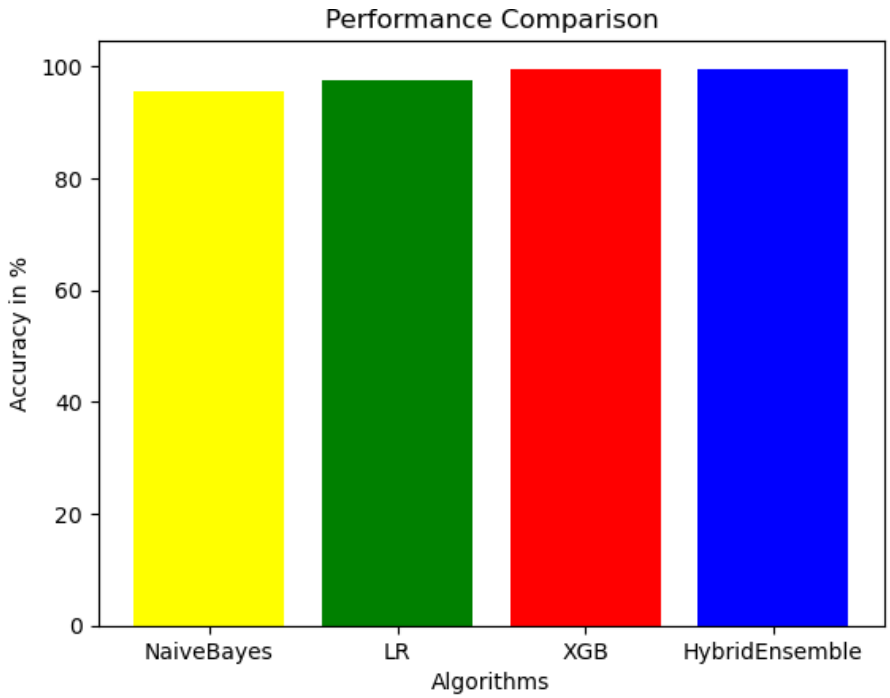


Figure 2. Accuracy Comparison

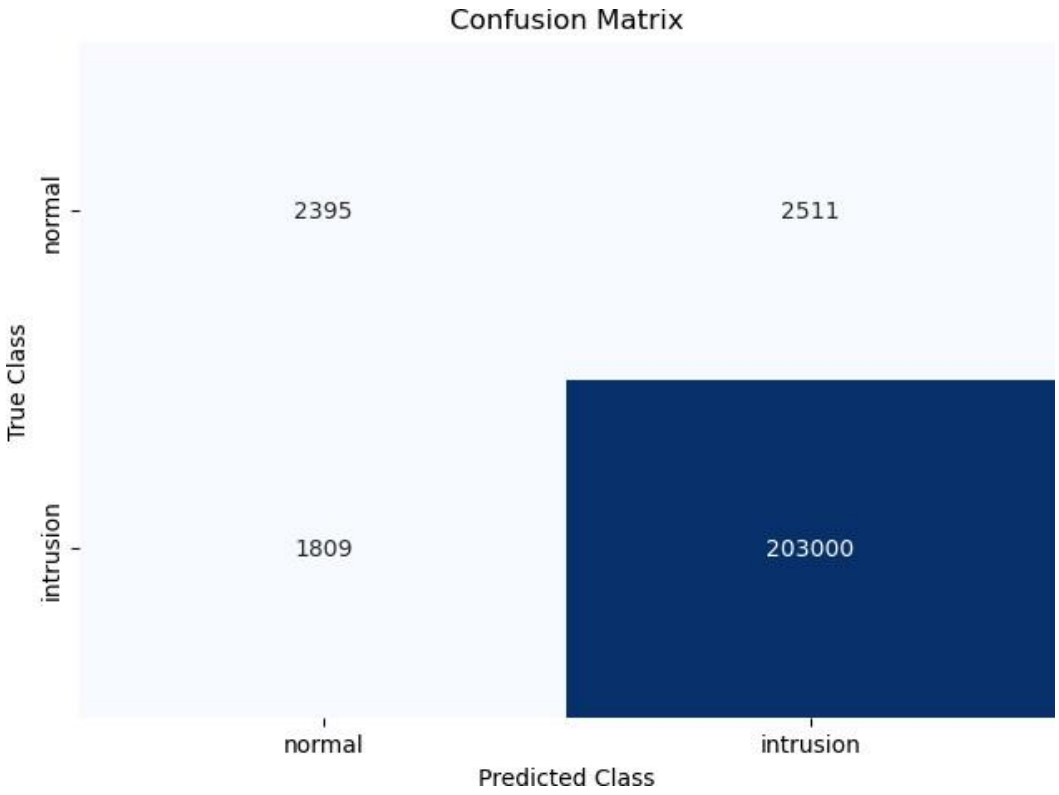


Figure 3 Confusion Matrix of Hybrid Ensemble

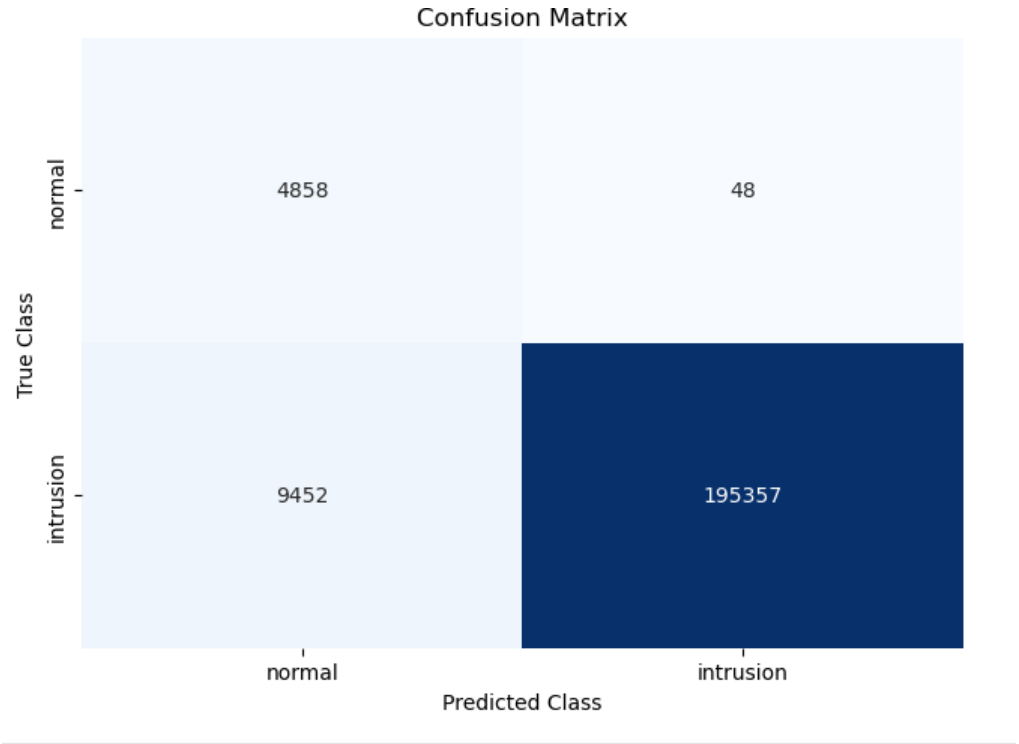


Figure 4 Confusion Matrix of Logistic Regression

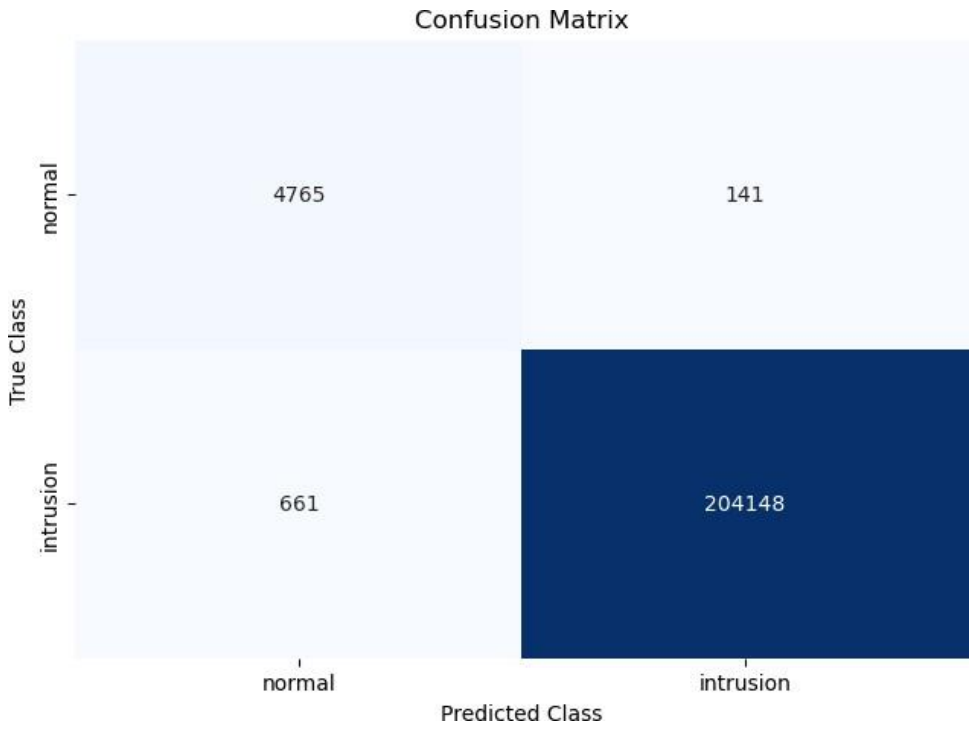


Figure 5 Confusion Matrix of . Naïve Bayes

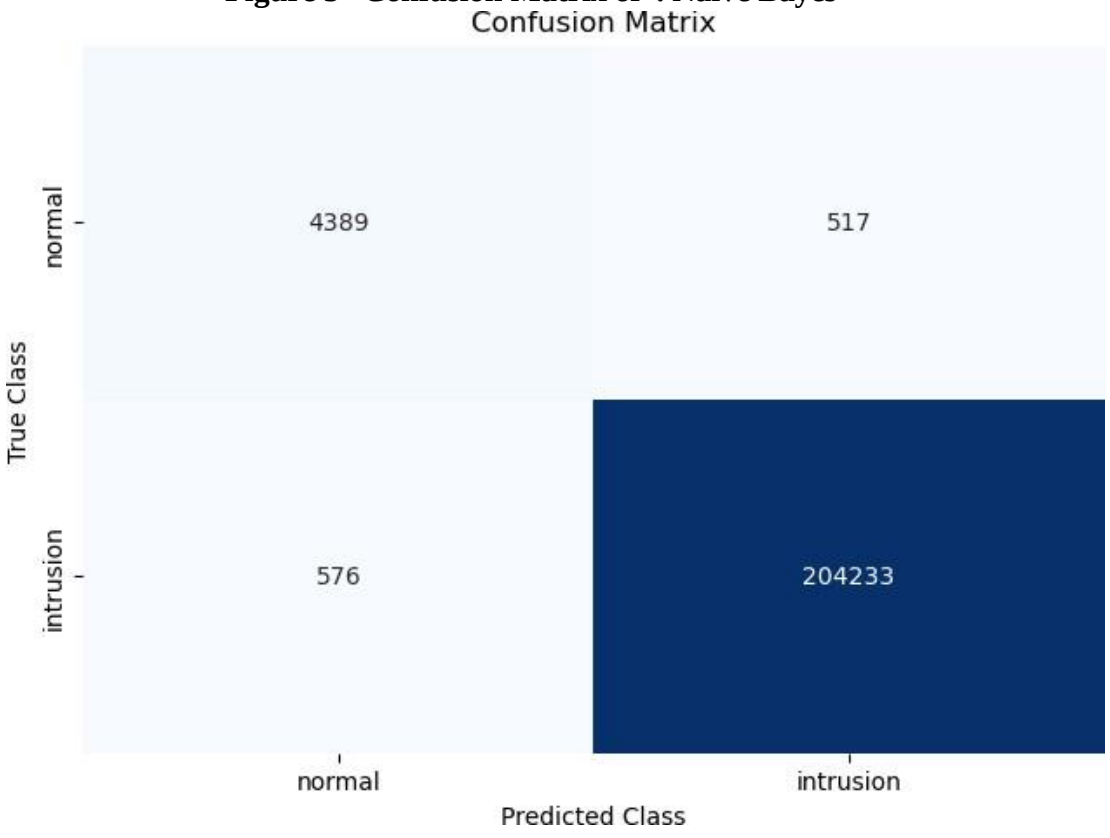


Figure 6 Confusion Matrix of Xgb

The small edge that the hybrid ensemble achieves does not come from leaning on one heavyweight model but rather from mixing different learning approaches. Analyzing precision and recall in more detail, the intrusion detection scenario is always able to differentiate between malicious and normal traffic, achieving strong results in both aspects. The confusion matrix further verifies that most normal and attack examples are properly classified, except for a few ambiguous instances. Compared with traditional classifier methods, the hybrid ensemble method has several distinguishing aspects. It demonstrates the model's ability to separate classes elegantly by showing off its talent for drawing complex decision boundaries in the imbalanced IoT network flows through the collective intelligence of its ensemble members. Second, the model is quite efficient, especially for use in real-world applications. For one, the bagging method is assuring for parallel processing, while the boosting model utilizes less resource-intensive classifiers for minimal efficiency losses. Moreover, the efficiency is guaranteed as the model scales up with the growing data sets; its responses are still quite speedy, making it more suitable for the realms of smart cities where the internet of things is concerned. Nevertheless, the model is only validated on a single smart city IoT dataset in which the models were manually tuned, which might imply a potential difference in model behavior with the changing conditions of the dataset or the overall network flows. It is also worth mentioning how the model focuses solely on the features at the network flow level, indicating its potential for altered IoT detection accuracy once the host features are incorporated for completeness.

Conclusion

In this paper, a hybrid intrusion detection system framework based on the ensemble approach has been designed particularly to meet the security demands of the smart city environment in IoT applications. By combining the adaptive learning of AdaBoost with the bagged decision trees that reduce the variance, the crafted framework exhibits efficient intrusion detection, high accuracy, and fewer false alarms. The experimental results confirm the effectiveness of the framework in detecting both prominent and subtle intrusion patterns while demonstrating sufficient computation efficiency.

The modularity of this framework facilitates scalability and seamless integration with different smart cities' systems. The experimental verification of this solution justifies the proposed strategy; however, it could be further evaluated using various heterogeneous datasets in dynamic conditions of traffic flow. The applicability of this solution could be further explored using techniques such as decentralized learning approaches for enhanced privacy and adaptability in a distributed IoT environment. The potential of this hybrid solution could be further disclosed using techniques such as a hybrid of this solution and deep learning and context-aware approaches to withstand increasingly sophisticated attacks to introduce intelligent intrusion detection systems of the future smart cities scenario. The solution contributes to the enhancement of classification performance while providing robustness and stability using a well-organized ensemble strategy. The proposed solution represents a balanced, applicable solution for intrusion detection systems of dynamic IoT environments, using techniques such as feature reduction and variance-controlled adaptive boosting techniques.

References

[1] Akif, M. A., Butun, I., Williams, A., & Mahgoub, I. (2025). *Hybrid machine learning models for intrusion detection in IoT: Leveraging a real-world IoT dataset.* arXiv:2502.12382. https://arxiv.org/abs/2502.12382

[2] Alhowaide, A. (2021). *Ensemble Detection Model for IoT IDS.* Internet of Things, 16, 100435. https://doi.org/10.1016/j.iot.2021.100435

[3] Almotairi, A. (2024). *Enhancing intrusion detection in IoT networks using a heterogeneous machine learning stack classifier model.* International Journal on Information and Communication Technologies, 16(2), Article 2321381. https://doi.org/10.1080/21642583.2024.2321381

[4] Alotaibi, Y., & Ilyas, M. (2023). *Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security.* Sensors, 23(12), 5568. https://doi.org/10.3390/s23125568

[5] Amouri, A., Al Rahhal, M. M., Bazi, Y., Butun, I., & Mahgoub, I. (2024). *Enhancing intrusion detection in IoT environments: An advanced ensemble approach using Kolmogorov-Arnold Networks.* arXiv:2408.15886. https://arxiv.org/abs/2408.15886

[6] Chatterjee, S., & Hanawal, M. K. (2021). *Federated learning for intrusion detection in IoT security: A hybrid ensemble approach.* arXiv:2106.15349. https://arxiv.org/abs/2106.15349

[7] *Olanrewaju-George, B., & Pranggono, B. (2025). Federated learning-based intrusion detection system for the Internet of Things using unsupervised and supervised deep learning models. Cyber Security and Applications, 3, 100068. https://doi.org/10.1016/j.csa.2024.100068*

[8] Hammood, B. A. K., & Sadiq, A. T. (2023). *Ensemble machine learning approach for IoT intrusion detection systems.* Iraqi Journal for Computers and Informatics, 49(2). https://doi.org/10.25195/ijci.v49i2.458

[9] Alashjaee, A.M., Alqahtani, F. Enhanced intrusion detection system IoT network security model by feed forward neural network and machine learning. *Sci Rep* 15, 36085 (2025). https://doi.org/10.1038/s41598-025-20047-0

[10] Khan, M. A., et al. (2021). *Voting Classifier-based Intrusion Detection for IoT Networks.* arXiv:2104.10015. https://arxiv.org/abs/2104.10015

[11] Lazzarini, R., Tianfield, H., & Charissis, V. (2023). *A stacking ensemble of deep learning models for IoT intrusion detection.* Knowledge-Based Systems, 260, 110941. https://doi.org/10.1016/j.knosys.2023.110941

[12] Talukder, M.A., Islam, M.M., Uddin, M.A. *et al.* Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *J Big Data* 11, 33 (2024). https://doi.org/10.1186/s40537-024-00886-w

[13] Maidamwar, I. P., Lokulwar, P. P., & Kumar, K. (2023). *Ensemble Learning Approach for Classification of Network Intrusion Detection in IoT Environment.* International Journal of Computer Network and Information Security, 15(3), 30–46. https://doi.org/10.5815/ijcnis.2023.03.03

[14] Premalatha, D. V., & Ramanujam, S. (2025). *Ensemble-based intrusion detection for IoT networks using the CICIoT2023 dataset*. Journal of Information Systems Engineering and Management, 10(21s). https://www.jisem-journal.com/

[15] Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). *A Survey on Intrusion Detection System in IoT Networks.* Computer Safety, Reliability, and Security, 100082. https://doi.org/10.1016/j.csa.2024.100082

[16] Saba, T. S., et al. (2022). *Anomaly-based intrusion detection system for IoT networks using CNN.* Elsevier Scientific Journals. https://doi.org/10.1016/j.compeleceng.2022.1001100

[17] Sanju, P. (2023). *Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks.* Journal of Enterprise Research, 100122. https://doi.org/10.1016/j.jer.2023.100122

[18] Tiwari, V. K., Kaur, G., Sharma, N. R., Srivastava, P., Rao, S. G., & Parveen, N. (2025). *Enhancing Cloud and IoT Security Using Deep Learning-Based Intrusion Detection Systems with Blockchain and Federated Learning.* Journal of Information Systems Engineering and Management, 10(25s), Article 4019. https://jisem-journal.com/index.php/journal/article/view/4019

[19] Yin, J., Shi, Y., Deng, W., Yin, C., Wang, T., Song, Y., Li, T., & Li, Y. (2023). *Internet of Things Intrusion Detection System Based on Convolutional Neural Network.* Computers, Materials & Continua, 77(3), 3763–3787. https://doi.org/10.32604/cmc.2023.035077

[20] Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). *A survey on intrusion detection system in IoT networks.* Cyber Security and Applications, 3(1), 100082. https://doi.org/10.1016/j.csa.2024.100082