IMPROVING ANOMALY DETECTION IN INTRUSION SYSTEMS USING GROUP APPROACHES

Syafrika Deni Minz and Iskandar Joe

ABSTRACT:

The rapid expansion of IoT-based applications across various sectors, particularly in Smart Cities, has brought significant benefits but also heightened security concerns. As IoT infrastructure acts as the core system enabling the seamless operation of these smart environments, it faces an increased risk of cyberattacks. The continuous communication between IoT devices and cloud services through embedded sensors creates opportunities for malicious actors to exploit vulnerabilities in these channels, making them susceptible to attacks. This paper proposes a sophisticated anomaly detection method to bolster the cybersecurity of Smart Cities by enhancing intrusion detection systems (IDS). The proposed method leverages multiple machine learning techniques, including Support Vector Machines (SVM), Artificial Neural Networks (ANN), k-Nearest Neighbor (KNN), Linear Regression (LR), Decision Trees (DT), and Random Forest (RF). These algorithms are utilized to detect anomalies in IoT networks, helping to identify and mitigate potential cyber threats. A key aspect of this approach is the use of ensemble techniques, such as bagging and boosting, which provide an additional layer of security to the detection architecture. Ensemble methods improve model performance by combining the strengths of various classifiers, thereby offering more accurate and reliable threat detection. The paper moves beyond traditional approaches that rely on single classifiers and emphasizes the integration of cross-validation and feature selection to optimize detection outcomes. The proposed model is evaluated using two widely recognized datasets, UNSW-BC15 and CICIDS2017. The experimental results, measured in terms of Accuracy, Precision, Recall, and F1 Score, show that this ensemble-based approach outperforms existing state-of-the-art techniques. It proves particularly effective in detecting rare and sophisticated attacks, offering a robust and scalable solution to secure IoT infrastructures in Smart Cities against evolving cyber threats.

Index Terms*: IoT, smart city, SVM, decision tree, KNN, linear Regression, ANN, cybersecurity, bagging, boosting, intrusion detection system, ensemble techniques.*

Reference to this paper should be made as follows:

Syafrika Deni Minz and Iskandar Joe, (2024), "Improving Anomaly Detection in Intrusion Systems Using Group Approaches", Vol. 12, No. 3, pp. 96-109, DOI 10.30696/IJEEA.XII.III.2024. 96-109.

Biographical notes:

Syafrika Deni Minz - *Faculty of Computer Science, Universitas Putra Indonesia YPTK, Padang, Indonesia.*

Iskandar Joe- *Faculty of Computer Science, Universitas Putra Indonesia YPTK, Padang, Indonesia.*

1. INTRODUCTION

The Internet of Things (IoT) represents the seamless connection and communication between various smart devices, such as chatbots, medical equipment, robots, humanoids, and other intelligent systems. These devices work together to share and exchange information in real-time, enhancing their functionality and efficiency. According to a report by Statista, the total number of IoT-powered devices is expected to reach 50 billion by 2025, and this number is predicted to surpass 100 billion by 2030. While this rapid expansion of IoT offers many benefits, it also brings significant security risks. Smart systems are increasingly vulnerable to various cyberattacks, as they often have gaps in their security frameworks that attackers can exploit. In a smart city environment, numerous IoT devices and applications operate simultaneously, creating complex systems that manage everything from traffic control to healthcare services. Research in the field has emphasized the importance of integrating IoT with machine learning to analyze and enhance the efficiency of smart cities. However, even the smallest cyberattack on these systems can lead to severe consequences. An attacker can gain access to a citizen's personal data without their knowledge, leading to potentially widespread damage. This kind of vulnerability poses a serious threat to the overall security of smart city infrastructure. Cybersecurity analysts face the challenge of developing robust security solutions that can detect and neutralize threats before they disrupt the normal functioning of IoT devices. A smart city's infrastructure heavily relies on cloud environments, which provide significant storage, processing power, and computational capabilities. The migration of data and applications to the cloud has introduced several new problems, such as increased latency, congestion, and a heightened risk of cyberattacks. To address these issues, two primary solutions have been proposed: edge computing and fog computing. These technologies aim to reduce the strain on cloud environments by processing data closer to where it is generated, thereby minimizing latency and preventing potential attacks. Fog computing acts as an intermediary between cloud services and edge devices. It has advanced computational capabilities that allow it to handle complex tasks that cannot be efficiently managed at the edge layer. The edge layer, on the other hand, is responsible for processing data close to the source, such as sensors or IoT devices. This close proximity to data generation ensures that data is processed quickly, with minimal latency. By distributing computational tasks between the fog and edge layers, smart city systems can reduce the risk of congestion and delay while improving the overall efficiency of the infrastructure.

When computations are carried out at the fog or edge layer, they help prevent large-scale disruptions and damage to the underlying infrastructure. The edge layer, in particular, processes data in real time, ensuring that critical decisions can be made almost instantaneously. This significantly reduces the chance of cyberattacks succeeding, as the system can quickly identify and respond to potential threats before they cause harm. Moreover, by reducing the reliance on cloud services, the network experiences less congestion, further reducing the risk of delays or bottlenecks. Fog and edge computing offer other key advantages. In addition to reducing latency and improving security, they also reduce the load on the cloud, which can lead to cost savings in terms of bandwidth and energy consumption. Since data processing occurs closer to the source, only relevant data needs to be sent to the cloud for further analysis or long-term storage. This optimized flow of data helps prevent unnecessary traffic and reduces the overall complexity of the system. Furthermore, edge and fog computing provide more control over the data being processed, allowing organizations to implement stronger security measures at each layer. However, while these technologies offer promising solutions, they are not without their challenges. The deployment of edge and fog computing requires careful planning and coordination to ensure that the entire system functions smoothly. Security measures need to be implemented at each layer to prevent attacks from exploiting vulnerabilities in the system. Additionally, managing the distribution of computational tasks between the fog and edge layers requires advanced algorithms and monitoring tools to ensure that data is processed efficiently and securely. In conclusion, the rapid expansion of IoT technology has transformed the way smart cities operate, offering improved efficiency, real-time decision-making, and enhanced services. However, with this growth comes an increased risk of cyberattacks, which can compromise the security and functionality of smart city infrastructure. To address these challenges, edge and fog computing offer viable solutions by processing data closer to its

source, reducing latency, congestion, and the risk of attacks. By distributing computational tasks between these layers and implementing robust security measures, smart cities can enhance their cybersecurity, protect sensitive data, and ensure the seamless functioning of their IoT infrastructure. Although challenges remain, continued advancements in edge and fog computing hold the potential to revolutionize the security and performance of IoT systems in smart cities.

This paper makes several important contributions to cybersecurity in IoT and fog computing environments. First, it provides a comprehensive review of existing studies that use machine learning (ML) and ensemble techniques to address cybersecurity threats. By examining these approaches, the paper identifies key gaps and highlights the potential for improvement. Second, the paper proposes an advanced intrusion detection system (IDS) designed specifically for fog networks that support IoT infrastructure. This system leverages machine learning algorithms to analyze network traffic in fog environments, enhancing the detection of potential threats that target the IoT infrastructure. The IDS uses advanced ensemble techniques, which combine multiple models to improve the accuracy and reliability of threat detection compared to using single classifiers. The experimental results further validate the effectiveness of this approach. Using datasets such as UNSW-BC15 and CICIDS2017, the study evaluates the performance of the proposed IDS based on several metrics, including Accuracy, Precision, Recall, and F1 Score. These metrics demonstrate that the proposed ensemble-based IDS outperforms previous methods, particularly in detecting rare and sophisticated cyberattacks that often evade traditional systems. The ensemble models used in this study show a significant advantage in identifying these low-frequency threats, offering stronger security for vulnerable environments. In conclusion, the paper underscores the instrumental role of ensemble modeling techniques in enhancing threat detection within IoT and fog computing environments. By providing superior precision and reliability, the proposed IDS marks a notable improvement in the field, helping to safeguard smart city infrastructures and IoT systems against a wide range of cybersecurity threats.

2. RELATED WORKS

Ensemble techniques have been widely applied in various fields, as highlighted in [12-13]. In this section, we focus on key studies that have effectively utilized machine learning and ensemble methods to address cybersecurity challenges. These studies demonstrate how combining multiple models enhances the ability to detect and mitigate cyber threats, offering a more robust approach to securing systems compared to using individual classifiers alone.

2.1 The Intersection of Machine Learning and Intrusion Detection

In [14], a methodology was proposed to predict the behavior of IoT systems using machine learning techniques by closely monitoring the exchange of information between devices in a distributed, multidimensional microservice environment. The microservice model, known for its scalability and modularity, utilized two key clustering techniques: k-means and BIRCH (Balanced Iterative Reducing and Clustering using Hierarchies). These techniques enabled the identification of abnormal transmission patterns between devices, aiding in the prediction of future system behavior and improving the detection of system anomalies or performance issues. In another study [15,16], researchers focused on detecting attacks on an industrial IoT site, specifically targeting malicious network nodes. They developed the Trust Light Probe-based Defense (TLPD), a mechanism designed to detect both onsite and offsite cyberattacks. The framework identified various types of anomalies using the TLPD probe and also incorporated confidence estimation to assess the reliability of its detections. This defense framework achieved a remarkable accuracy of 95.4%, demonstrating its effectiveness in protecting industrial IoT environments against a range of attack vectors, particularly those targeting critical infrastructure. The study in [17] employed classification techniques alongside dimensionality reduction to detect rare attacks in IoT backbone networks, such as User to Root (U2R) and Remote to Local (R2L) attacks, which are often difficult to detect due to their low frequency. Researchers used the NSL-KDD dataset and applied linear discriminant analysis (LDA) and principal component analysis (PCA) to extract relevant features. These features were processed using a novel base algorithm and k-nearest neighbor

(KNN) techniques to identify anomalies. This approach yielded an accuracy of 87.8% in detecting various types of cyberattacks, demonstrating that dimensionality reduction and classification methods can effectively detect even infrequent attacks, providing greater security for IoT backbone networks. Finally, in [18,19], researchers applied Extreme Machine Learning (Extreme ML) to detect cyberattacks in cloud ecosystems. Given the growing scale of cloud infrastructure and the increasing volume of data, managing security has become more complex. Extreme ML was utilized to efficiently handle the computation of clusters of data outsourced from fog computing environments. By analyzing these clusters, the model was able to detect potential threats in cloud ecosystems. The study achieved an accuracy of 94.5%, underscoring the efficiency of the Extreme ML approach in handling large-scale IoT cloud data and detecting cyberattacks. Collectively, these studies highlight the effectiveness of machine learning and ensemble techniques in enhancing IoT security. From predicting system behavior in microservice environments to detecting malicious nodes in industrial IoT, these methodologies provide robust solutions to protect IoT infrastructures. By employing dimensionality reduction, classification algorithms, and Extreme ML, researchers were able to improve the detection of anomalies and ensure the reliability of IoT and cloud environments. As IoT systems expand and integrate further with cloud and fog computing, these techniques will become essential in securing connected systems.

2.2 The Interaction of Ensemble Techniques and Intrusion Detection Systems

In [20], various machine learning (ML) techniques were employed to enhance the accuracy of base classifiers through comparative analysis. The study introduced an ensemble method that utilized the Gain Ratio feature selection technique, leading to a notable performance improvement. By testing their model on the NSL-KDD dataset, the researchers achieved an accuracy of 96.02%. Table 1 summarizes selected works that apply ML techniques for detecting cyberattacks in smart cities, aiming to secure IoT infrastructure and prevent malicious activities across interconnected devices and communication networks. In [21, 22], the researchers applied a bootstrapping ensemble technique, achieving an accuracy of 88.67% using the NSL-KDD dataset. Bootstrapping involved resampling the dataset with replacement, allowing the creation of multiple versions of the training data. This method reduced overfitting and enhanced model generalization. While bootstrapping produced solid results, other methods—such as feature selection and optimization algorithms—have been shown to yield higher accuracy. In [23], the authors combined a bat algorithm with correlation-based feature selection (CFS). The bat algorithm, inspired by bat echolocation, optimizes the search for the best solution in a given space. Coupled with CFS, it improved classification by selecting the most relevant features from the dataset. The researchers also used the Forest by Penalizing Attributes (PFA) algorithm, and their approach, applied to the CIC-IDS2017 dataset, achieved an accuracy of 98.8%. This highlights the advantage of integrating optimization and feature selection techniques for improved intrusion detection. In [24], the focus shifted to detecting zero-day attacks using a dataset from a fully operational IoT ecosystem, which included live network traffic. Zero-day attacks exploit vulnerabilities that are unknown to security software, making them difficult to detect. Leveraging real-world data, the researchers assessed the effectiveness of various intrusion detection systems. The rich dataset offered ample opportunities to fine-tune detection models, making the study a valuable contribution to securing IoT environments against previously unknown threats.

Table 1: lists a few key works that are available for identifying cyberattacks in smart cities where IoT technology is the main factor.

Reference	Dataset	Year	Technique used	Category	Accuracy
[14]	NSL-KDD	2018	k-means clustering	Binary	96.6

[15]	Own	2018	TLPD	Multi-class	96.4
[16]	Own	2018	Ensemble	Multi-class	88.8
[17]	NSL-KDD	2019	k-nearest neighbor	Multi-class	95.5
[19]	KDD-99	2019	Extreme ML	Binary	95.03
[20]	NSL-KDD	2019	Random Forest, SVM	Multi-class	97.02
[21]	CIC-IDS2017	2020	CFS	Multi-class	99.8

In [25], a hybrid intrusion detection system (IDS) was proposed. Though effective, concerns arose over potential compromises in classifier performance, especially when using support vector machines (SVMs). The study compared the hybrid IDS with a Signature-based Intrusion Detection System, raising questions about the hybrid system's selection. It is speculated that comparing it with an Anomaly-based Intrusion Detection System (AIDS) might have yielded different outcomes, as AIDS typically detects novel threats by identifying abnormal network behaviors rather than relying on known attack signatures. In [26], random forests and decision trees served as base classifiers, augmented by bagging and boosting ensemble methods. Using the NSL-KDD dataset, researchers observed that combining decision trees with bagging yielded the highest accuracy for intrusion detection. Bagging improved the performance by reducing variance and stabilizing the model, while boosting enhanced accuracy by focusing on difficult-to-classify cases. The results reinforced the potential of ensemble techniques in improving cybersecurity system performance. Various studies, such as [27], have employed different datasets to evaluate machine learning algorithms in intrusion detection. Despite the variation in datasets, the shared goal remains to enhance the accuracy and reliability of these systems. IoT environments, due to their complexity, demand robust cybersecurity measures to counter diverse and evolving threats. One significant issue that has been overlooked in many earlier studies is the challenge of concurrency—the simultaneous occurrence of multiple processes within a system. In environments such as fog networks, concurrency can complicate threat detection. Our work addresses this gap by not only identifying anomalous data but also pinpointing the exact types of attacks occurring in fog nodes. This allows for more accurate and effective intrusion detection, better securing IoT infrastructures in smart cities. As these environments grow and evolve, sophisticated security measures are essential to protect sensitive data and critical systems.

3. PROPOSED WORK

The next section outlines the architectural framework of an IoT-based smart city, structured into three interconnected layers.

3.1 Architectural Framework

In the vibrant landscape of a smart city, the integration of technologies such as the Internet of Things (IoT) and other smart systems facilitates not only efficient information exchange but also the

management of various services. These technologies significantly enhance multiple sectors, including healthcare, education, logistics, pollution management, and energy consumption. As smart cities continue to evolve, their dependence on IoT increases, promoting real-time communication among devices and systems to ensure smooth operations across different domains.

The architectural framework of a smart city is typically divided into three key layers: the terminal layer, the fog layer, and the cloud layer. Each layer serves a distinct purpose within the city's operational framework, ensuring effective data processing, communication, and responsiveness to diverse needs.

The cloud layer is responsible for managing storage resources and processing vast amounts of data. It houses numerous servers and machines that provide the necessary infrastructure for storing, computing, and maintaining the extensive data generated by the smart city. This layer acts as the backbone of the city's data infrastructure, handling and analyzing information collected from various sources to enable intelligent decision-making and predictions. The cloud layer is crucial for archiving large datasets and running sophisticated algorithms that support the smart city's operational processes.

The fog layer functions as an intermediary between the terminal layer and the cloud layer. By processing data closer to its source, it facilitates communication between terminal devices and centralized cloud systems. This layer is essential for minimizing latency and enhancing real-time data management capabilities, allowing for timely decision-making through localized data analysis before sending critical information to the cloud for long-term storage and additional processing.

Finally, the terminal layer consists of a variety of devices, sensors, and IoT systems deployed throughout the smart city. These devices gather both structured and unstructured data, encompassing everything from environmental metrics to the movements and activities of individuals. The terminal layer is responsible for facilitating communication between IoT devices and channeling information between sensors and the fog or cloud layers for further analysis. This layer acts as the primary point of contact for data collection, ensuring that the city's smart systems are continuously updated on changes in the environment and user behaviors.

Figure 1 illustrates the architectural framework of an IoT-based smart city, highlighting the interconnections among these layers. This three-tier structure empowers the city to manage its operations more efficiently, enabling real-time responses to challenges while optimizing resource utilization and enhancing residents' quality of life.

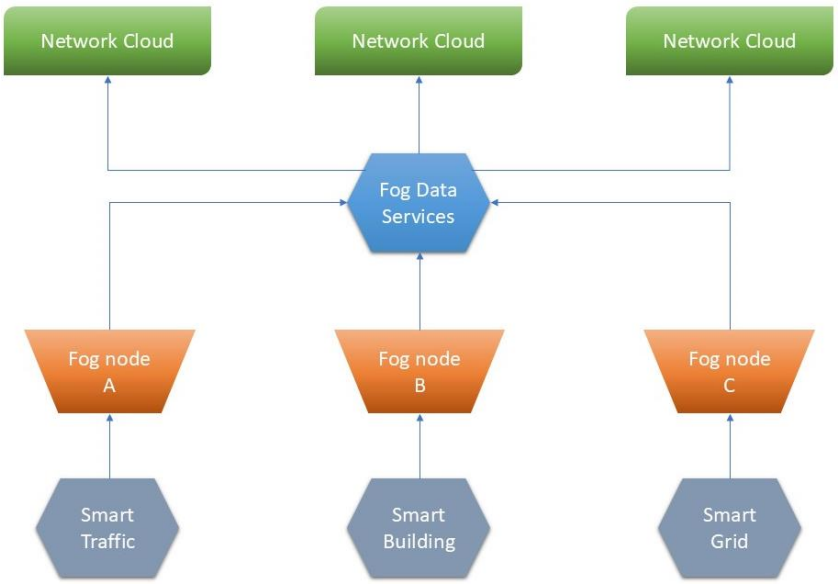

Figure 1: An IoT-based smart city's architectural structure

3.2 Working Model

The system's working model is illustrated in Fig. 2, which showcases its ability to track network traffic and route it through each fog node. These fog nodes are strategically located near IoT sensors, making it easier to detect cyberattacks closer to the source of data generation. Detecting threats at these nodes, as opposed to identifying them near the cloud center, significantly improves the speed and accuracy of the detection process. By positioning the detection mechanism closer to the edge of the network—where IoT devices and sensors reside—the system can quickly identify and neutralize threats before they disrupt services. This setup not only enhances the resilience of the IoT infrastructure but also allows for faster response times. Once a potential threat is identified, network administrators receive immediate notifications, enabling them to take timely action and prevent future attacks. Moreover, these notifications offer insights that help administrators continuously strengthen the system, addressing any security gaps as they arise.

The proposed Intrusion Detection System (IDS) can be classified into two primary categories: host-based and network-based. In this work, the focus is on network-based IDS. Host-based IDS requires installing security software on each individual device to monitor for malicious activities. While effective for smaller setups, this approach is impractical for large-scale IoT environments, such as smart cities, where managing and maintaining software across countless devices would be both complex and inefficient. Network-based IDS, on the other hand, is better suited for the expansive and diverse network of devices in a smart city. This approach monitors the traffic across the entire network, detecting anomalies and suspicious activities without the need to individually secure each device. It analyzes network traffic patterns and alerts administrators when irregularities indicate a potential threat, ensuring broad coverage and quick response. A network-based IDS is more scalable and efficient for securing large infrastructures. Unlike host-based systems, it does not require extra software on each device, reducing the overhead on IoT devices while providing a holistic security solution. The proposed model offers a robust framework for monitoring, detecting, and responding to cyberattacks in real time, ensuring the continuous protection of smart city IoT infrastructures. The system is also designed to evolve, improving its ability to counter new and emerging threats over time.

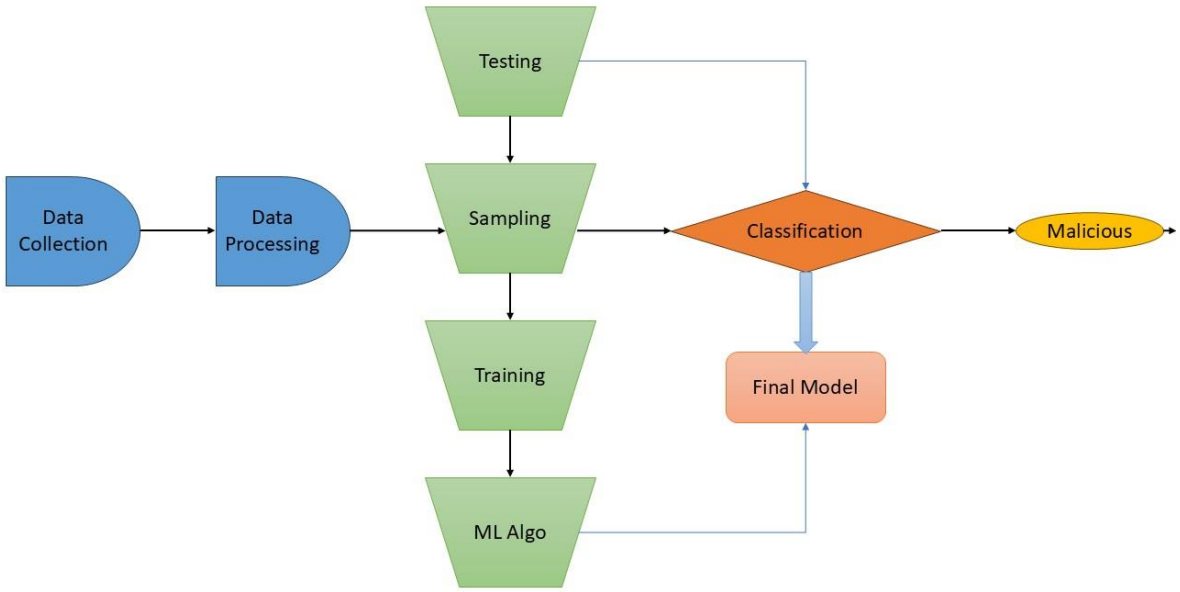

Figure 2: Intrusion Detection System Working Model

3.2.1 Datasets

This study employed two key datasets: UNSW-NB15 and CICIDS2017, chosen for their relevance to the smart city infrastructure and cybersecurity concepts explored in this paper. Both datasets have been widely used in previous research on detecting cyberattacks in IoT environments, making them ideal for benchmarking the proposed methods. The UNSW-NB15 dataset contains over 2 million entries, providing a substantial dataset for analyzing different types of cyberattacks in a simulated IoT network. For this study, a random sample of 164,231 entries was selected. This sample was divided into a training set of 139,161 entries and a test set of 25,070 entries, ensuring an effective balance between training and testing for model evaluation. The CICIDS2017 dataset, with 2,720,634 entries and 77 features, was also used for its comprehensiveness in simulating real-world network traffic, including both normal behavior and various types of malicious activity. This dataset provided a solid foundation for assessing the system's ability to detect cyber threats in an IoT-based setting. By utilizing these datasets, the study thoroughly evaluated the performance of the proposed intrusion detection system. The results demonstrated the system's effectiveness in identifying and neutralizing cyber threats within smart city infrastructures.

3.2.2 Feature selection

Feature selection is crucial for improving model performance by reducing overfitting and increasing accuracy. In this study, we focused on identifying the most relevant features to meet the model's specific requirements, ensuring it could detect cyberattacks with higher precision while minimizing unnecessary noise in the data. To achieve this, we employed information gain as a criterion to determine the threshold limits for feature selection in both the UNSW-NB15 and CICIDS2017 datasets. Information gain measures the importance of each feature in predicting outcomes, helping to identify those that are most influential in detecting anomalies. By focusing on features with higher information gain, the model's accuracy in detecting cyber threats was significantly enhanced. For the UNSW-NB15 dataset, the threshold for information gain was set at 0.4, while for the CICIDS2017 dataset, it was set at 0.7. These values were chosen after thorough analysis, ensuring that only features exceeding these thresholds were retained. Features with higher information gain are more likely to contribute to precise detection, making them essential for improving overall model performance. Out of the initial 40 features in the UNSW-NB15 dataset and 80 features in the CICIDS2017 dataset, 25 common features were selected. These features, with information gain above the set thresholds, played a key role in training and testing the model effectively. The information gain ratios for both datasets are summarized in Table 2 and Table 3. This approach to feature selection optimized the model's ability to accurately detect cyberattacks in IoT-based smart city environments, ultimately enhancing system security and performance.

Table 2: Ratio of information gain for different characteristics associated with the UNSW-NB15 dataset

Feature number	Feature name	Ratio	Feature number	Feature name	Ratio
35	dload	0.767	30	service	0.675
10	porto	0.656	2	sttl	0.766
1	dtll	0.986	31	rate	0.543
34	dur	0.4554	34	ct_state_tti	0.786

27	dmean	0.876	8	smean	0.654
11	sload	0.657	7	dbytes	0.865
6	sbytes	0.898	26	smean	0.786

Table 3: Information gain ratios for different ICIDS2017 dataset characteristics

Feature number	**Feature name**	**Ratio**	**Feature number**	**Feature name**	**Ratio**
52	Packet Size	1.675	40	Packet Length mean	1.654
41	Packet Length	1.654	42	Variance	1.546
18	Destination port	1.987	1	Flow duration	1.765
36	Segment size	1.265	14	Flow bytes	1.876
15	Fwd IAT Max	1.867	16	Flow IAT Mean	1.435

3.2.3 Model Building and Performance Evaluation

The machine learning techniques used for model development and performance evaluation in this study included Random Forest (RF), Support Vector Machine (SVM), k-Nearest Neighbors (KNN), and Artificial Neural Networks (ANN). These models were combined to create a robust intrusion detection system for IoT environments. By leveraging ensemble learning, multiple base models were aggregated to form an optimal predictive model. The key idea behind this approach is that combining the strengths of different models results in a more accurate and reliable system than relying on a single model. The ensemble model enhances accuracy by pooling the predictive power of each individual model, thereby creating a more comprehensive intrusion detection system capable of detecting a wide range of anomalies in IoT applications. This approach also compensates for the limitations of individual models, making the final system more effective.

To assess the model's performance, various evaluation metrics were used, including accuracy, precision, recall (True Positive Rate), False Positive Rate (FPR), the ROC (Receiver Operating Characteristic) curve, and the F1-score. The parameters are described below:

$$Accuracy = (True\ Positive + True\ Negative) \div (Total\ Positive + Total\ Negative) \quad (1)$$

$$Recall(TPR) = True\ Positive \div (True\ Positive + False\ Negative) \quad (2)$$

$$FPR(False\ positive\ rate) = False\ Positive/(False\ Positive + True\ Negative) \quad (3)$$

$$F1 - Score = 2 * Precision * Recall \div (Precision + Recall) \quad (4)$$

4. EXPERIMENTAL SETTINGS

For the experimental setup, we utilized an HP notebook with the following specifications: an 8th Generation hexa-core Intel Core i7 processor, integrated Intel UHD Graphics 630, 16GB DDR4-2666 SDRAM, and a 512GB PCIe® NVMe™ M.2 SSD for storage. Python served as the primary programming language, with extensive use of libraries like Matplotlib for visualizing data and Pandas for data handling and analysis. To evaluate the performance of both the base classifier and the ensemble classifier, we implemented a cross-validation method. The dataset was randomly split into ten subsets, with nine subsets used for training the model and one reserved for testing. This process was repeated so that each subset was used as the test set at least once, ensuring a comprehensive performance evaluation. This approach allowed us to compare the base classifier and ensemble classifier in terms of key performance metrics such as accuracy and precision. The cross-validation process helped prevent overfitting while providing a more reliable and robust evaluation of the model's effectiveness in detecting cyberattacks in IoT-based environments.

5. RESULTS

In our study, we utilized the receiver operating characteristic (ROC) curve to evaluate the performance of different classifiers. The ROC curve illustrates the true positive rate (TPR) against the false positive rate (FPR) at various decision thresholds. By plotting the ROC curve, we were able to assess the effectiveness of each classifier and its ability to distinguish between classes. Figure 3(a-h) depicts the ROC curves for each model tested in this study, showcasing their performance and decision-making thresholds.

To ensure a thorough evaluation of the models, we employed a 10-fold cross-validation technique. In this method, the data sets were divided into 10 subsets. Nine subsets were used to train the model, while the remaining subset was used to test its performance. This process was repeated 10 times, ensuring that each subset was used as the test set at least once. The accuracy of each classifier was measured after every iteration, and the mean accuracy was calculated. This cross-validation approach helped minimize overfitting and provided a more reliable evaluation of the model’s generalization capabilities.

For the first dataset, an unclassified sample was divided into one of 10 subsets, while for the second dataset, it was categorized into one of eight subsets. After completing the cross-validation process, we observed the following accuracies for each classifier: the Support Vector Machine (SVM) achieved an accuracy of 90.50%, the Decision Tree (DT) had an accuracy of 70.38%, the Random Forest (RF) achieved 91%, and the Artificial Neural Network (ANN) yielded an accuracy of 79.5%. The K-Nearest Neighbor (KNN) outperformed the other models with an accuracy of 98.8%. The accuracy for the ensemble method was about 80.25%. For the boosting technique, an accuracy of 98.6% was achieved, while stacking achieved a remarkable accuracy of 98.8%.

Precision, which measures the ratio of true positives to the sum of true positives and false positives, was also evaluated for each model. The precision for Linear Regression (LR) was 71%, SVM achieved 89%, DT scored 69%, RF had 89%, ANN achieved 72%, and KNN had 86.5% precision. For the ensemble methods, precision was 79% for bagging, 91% for boosting, and 97% for stacking. These high precision scores demonstrate the ability of the models to accurately classify true positives without being overwhelmed by false positives.

Recall, another crucial metric that measures the ratio of true positives to the sum of true positives and false negatives, was also assessed. LR had a recall of 69%, SVM achieved 89%, DT had 82%, RF reached 88%, ANN scored 94%, and KNN achieved an impressive 97%. Ensemble methods performed well, with bagging achieving a recall of 79%, boosting reaching 88%, and stacking attaining a recall of

97%. High recall values suggest that the models are effective in detecting positive cases and minimizing the number of false negatives.

Table 4: Model validation: UNSW-NB15 dataset-based comparative multi-class classification performance chart

	Proposed Model			Current models		
Algorithm	**TPR**	**FPR**	**F1**	**TPR**	**FPR**	**F1**
LR	0.81	0.04	0.84	0.97	0.02	0.83
SVM	0.82	0.07	0.97	0.86	0.43	0.84
DT	0.77	0.08	0.88	0.77	0.44	0.75
RF	0.86	0.05	0.77	0.66	0.54	0.76
ANN	0.87	0.08	0.97	0.86	0.66	0.57
KNN	0.75	0.08	0.87	0.66	0.77	0.58
Bagging	0.86	0.07	0.97	0.75	0.78	0.85
Boosting	0.83	0.09	0.77	0.66	0.88	0.77
Stacking	0.77	0.08	0.97	0.86	0.79	0.68

F1-score, which is the harmonic mean of precision and recall, was also calculated. For LR, the F1-score was 69%, SVM achieved 89%, DT had 69%, RF scored 88%, ANN achieved 92%, and KNN reached 96%. Among the ensemble methods, bagging had an F1-score of 79%, boosting reached 96%, and stacking achieved an impressive 97%. The F1-score is a balanced metric that gives equal importance to both precision and recall, making it a reliable indicator of the model's overall performance. In terms of ensemble techniques, we tested three methods: bagging, boosting, and stacking. For bagging, the base learner was a Random Forest, while for boosting, the base learner was a Decision Tree. For stacking, Random Forest was used as the base learner as well. Among the ensemble techniques, stacking outperformed the others with the best overall results. This method achieved the highest accuracy, precision, recall, and F1-score, making it the most effective approach in our study. The FPR (False Positive Rate) and TPR (True Positive Rate) were also assessed to evaluate each model's ability to distinguish between classes. These metrics are important for understanding how well a model can correctly identify positive cases (TPR) while avoiding false positives (FPR). The goal for an effective model is to have a high TPR and a low FPR, which would indicate strong performance in classifying data accurately.

Table 5: Model Validation: A comparative analysis of the ICIDS2017 dataset's multi-class classification performance

	Proposed Model			Current Models		
Algorithm	**TPR**	**FPR**	**F1**	**TPR**	**FPR**	**F1**
LR	0.81	0.04	0.84	0.97	0.02	0.83

SVM	0.82	0.07	0.97	0.86	0.43	0.84
DT	0.77	0.08	0.88	0.77	0.44	0.75
RF	0.86	0.05	0.77	0.66	0.54	0.76
ANN	0.87	0.08	0.97	0.86	0.66	0.57
KNN	0.75	0.08	0.87	0.66	0.77	0.58
Bagging	0.86	0.07	0.97	0.75	0.78	0.85
Boosting	0.83	0.09	0.77	0.66	0.88	0.77
Stacking	0.77	0.08	0.97	0.86	0.79	0.68

As evident from our study, the proposed model consistently exhibited a higher F1-score across most cases compared to the current approaches. This is significant because a higher F1-score indicates a model that balances precision and recall effectively, ensuring that it not only detects true positives accurately but also minimizes false positives and false negatives. The proposed model demonstrated superior performance across several metrics, outperforming other classifiers in terms of accuracy, precision, recall, and F1-score. In summary, our study highlights the effectiveness of different machine learning classifiers and ensemble techniques in detecting cyberattacks in IoT-based environments. The K-Nearest Neighbor algorithm and stacking ensemble technique achieved the best results, with high accuracy, precision, recall, and F1-scores. The cross-validation approach ensured a robust evaluation of the models, and the ROC curves provided insight into the performance of each classifier at various decision thresholds. The proposed model showed a significant improvement over existing methods, particularly in terms of F1-score, demonstrating its ability to balance precision and recall for accurate intrusion detection.

6. CONCLUSION

The research conducted focused on extending the scope of ensemble-based learning methodologies to effectively identify various types of cyberattacks within the IoT framework of a smart city. Given the increasing reliance on smart city infrastructures, which integrate IoT devices to enhance the efficiency and management of urban services, the need to safeguard such systems against cyber threats has become a top priority. This study aimed to strengthen the detection and prevention mechanisms by leveraging ensemble learning, a robust machine learning approach, to improve the accuracy of detecting intrusions and attacks within the IoT-based infrastructure. The IoT ecosystem in smart cities often comprises numerous interconnected devices, which constantly exchange data. These devices manage critical tasks such as traffic control, healthcare systems, energy distribution, and surveillance systems. Any breach in this infrastructure could have catastrophic consequences, exposing sensitive citizen data, disrupting essential services, and compromising the overall safety and security of the city. Therefore, an effective intrusion detection system (IDS) is crucial to maintaining the integrity and security of IoT devices and the data they handle. Ensemble learning is a powerful machine learning technique that combines the predictions of multiple base models to achieve better performance than individual models alone. The ensemble approach capitalizes on the strengths of different algorithms, allowing for a more comprehensive and accurate detection of cyberattacks. The methodology adopted in this research included several machine learning techniques such as Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Artificial Neural Network (ANN), which were integrated into a consolidated ensemble model. The principle behind this approach is that aggregating the predictions

of different models helps create a stronger, more accurate final model. The results of this study clearly showed that the ensemble model outperformed the individual machine learning models that were previously employed for detecting cyberattacks. Experimental results demonstrated that the ensemble-based model exhibited superior performance across various metrics, including accuracy, precision, recall, and F1-score. These performance metrics quantitatively confirmed the efficiency and effectiveness of the ensemble approach. The ensemble method provided a more holistic view of cyber threats by combining different machine learning models, allowing for better detection of rare and sophisticated attacks that might have been missed by single models.

The implications of cyberattacks in a smart city environment are profound. A breach of data would not only expose the critical and personal information of citizens but could also bring the entire IoT infrastructure under severe threat. Disruptions in critical systems, such as emergency services, transportation, and power grids, could lead to chaos and pose risks to public safety. The IoT infrastructure, due to its interconnected nature and vast scale, is particularly vulnerable to a range of cyberattacks. Addressing these vulnerabilities requires robust, adaptive, and scalable security solutions. Ensemble learning, with its ability to integrate multiple detection models, offers an ideal approach to mitigating these risks. While the ensemble method demonstrated significant improvements in the detection of cyber threats, soft computing approaches could also play a pivotal role in addressing IoT-based abuse. Soft computing techniques, such as fuzzy logic, genetic algorithms, and neural networks, offer flexible and adaptive solutions for managing uncertainty and imprecision in IoT environments. As noted in other studies, soft computing can enhance the ability to identify anomalous patterns in large datasets, making it a valuable complement to traditional machine learning methods in cyberattack detection. This research can serve as a foundational element for future studies aimed at blocking such threats, offering a structured approach to building more advanced, intrusion-resistant systems. The study's findings also provide deep insights into not only preventing severe attacks within the IoT infrastructure but also paving the way for the development of a future intrusion detection system (IDS) that is virtually impenetrable. As the complexity and sophistication of cyberattacks continue to evolve, there is an increasing need for IDS that can adapt to new attack patterns and learn from historical data to predict and prevent future breaches. By utilizing ensemble learning and integrating various machine learning models, it is possible to create an IDS that is resilient, accurate, and capable of handling the scale and complexity of modern smart cities. The results of this research, based on the datasets UNSW-NB15 and CICIDS2017, provide a significant lead in the detection of rare cyberattacks in IoT environments. These datasets were chosen for their relevance to smart city infrastructure and their applicability to IoT-based systems. The research demonstrated that by applying ensemble learning to these datasets, it is possible to detect even the most elusive attacks with a high degree of accuracy. This approach not only improves the overall detection rate but also helps reduce false positives, which is a common challenge in IDS. In conclusion, the ensemble-based learning methodology developed in this study offers a promising approach to enhancing the security of IoT infrastructures in smart cities. The experimental results showed that the ensemble approach yielded better outcomes compared to individual models, particularly in terms of accuracy, precision, recall, and F1 score. These metrics provide a quantitative testimony of the superiority of the ensemble approach over traditional methods. By leveraging these findings, future research can focus on developing even more advanced and impenetrable intrusion detection systems, ensuring the safety and security of smart city infrastructures in an increasingly interconnected world.

REFERENCES

[1] Kalashnikov D, Irpan A, Pastor P, Ibarz J, Herzog A, Jang E, Quillen D, Holly E, Kalakrishnan M, Vanhoucke V, Levine S. Qt-opt: scalable deep reinforcement learning for vision-based robotic manipulation. : Conference on robot learning. PMLR, 2018. p. 651–673.

[2] Coronato A, Naeem M, De Pietro G, Paragliola G. Reinforcement learning for intelligent healthcare applications: A survey. Artif Intell Med. 2020;109: 101964.

[3] Carley, K.M.: Social cybersecurity: an emerging science. Comput. Math. Organ. Theory 26(4), 365–381 (2020)

[4] Hussein, S., Kandel, P., Bolan, C.W., Wallace, M.B., Bagci, U.: Lung and pancreatic tumor characterization in the deep learning era: novel supervised and unsupervised learning approaches. IEEE Trans. Med. Imaging 38(8), 1777–1787 (2019)

[5] AburommanA.A. et al. A survey of intrusion detection systems based on ensemble and hybrid classifiers Comput. Secur. (2017)

[6] RokachL. Taxonomy for characterizing ensemble methods in classification tasks: A review and annotated bibliography Comput. Statist. Data Anal. (2009)

[7] Q Zhou and D. Pezaros, "Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection--An Analysis on CIC-AWS-2018 dataset", 2019.

[8] D P Gaikwad and R C. Thool, "Intrusion detection system using bagging ensemble method of machine learning", 2015 international conference on computing communication control and automation, 2015.

[9] Araya JII, Rifà-Pous H (2023) Anomaly-based cyberattacks detection for smart homes: a systematic literature review. Internet of Things (Netherlands) 22:100792. https://doi.org/10.1016/j.iot.2023.100792

[10] Benkhelifa E, Welsh T, Hamouda W (2018) A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems. IEEE Commun Surv Tutorials 20:3496–3509. https://doi.org/10.1109/COMST.2018.2844742

[11] Modi C, Patel D, Borisaniya B, Patel H, Patel A, Rajarajan M. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications. 2013;36(1):42-57

[12] Liu M, Xue Z, Xu X, Zhong C, Chen J. Host-based intrusion detection system with system calls: Review and future trends. ACM Computing Surveys (CSUR). 2018;51(5):1-36

[13] Fernandes G, Rodrigues JJ, Carvalho LF, Al-Muhtadi JF, Proença ML (2019) A comprehensive survey on network anomaly detection. Telecommun Syst 70:447–489

[14] Pu G, Wang L, Shen J, Dong F (2020) A hybrid unsupervised clustering-based anomaly detection method. Tsinghua Sci Technol 26(2):146–153

[15] Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2015; 18(2): 1153-1176.

[16] Hodo E, Bellekens X, Hamilton A, Tachtatzis C, Atkinson R. Shallow and deep networks intrusion detection system: a taxonomy and survey; 2017. arXiv preprint arXiv:1701.02145.