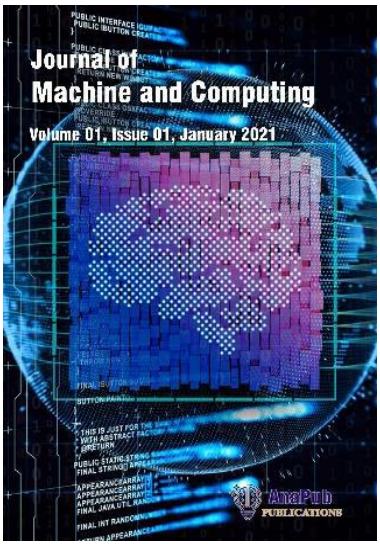
Journal Pre-proof

A Lightweight and Federated Machine Learning-Based Intrusion Detection System for Multi-Attack Detection in IoT Networks



Prathap Mani, Arthi D, Periyakaruppan K and Surendarkumar S

DOI: 10.53759/7669/jmc202505033

Reference: JMC202505033

Journal: Journal of Machine and Computing.

Received 12 July 2024

Revised form 03 October 2024

Accepted 28 November 2024

Please cite this article as: Prathap Mani, Arthi D, Periyakaruppan K and Surendarkumar S, "A Lightweight and Federated Machine Learning-Based Intrusion Detection System for Multi-Attack Detection in IoT Networks", Journal of Machine and Computing. (2025). Doi: https://doi.org/10.53759/7669/jmc202505033

A Lightweight and Federated Machine Learning-Based Intrusion Detection System for Multi-Attack Detection in IoT Networks

Prathap Mani, Department of Computer Science & Information Technology, American University of Kurdistan Middle East.

Arthi D, Department of Business Administration, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, Tamil Nadu, India.

K. Periyakaruppan, Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu, India. -641107.

S. Surendarkumar, Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India.

[1]prathap.mani@auk.edu.krd, [2]arthid_mba@avinuty.ac.in, [3]kperiyakaruppan@gmail.com, [4]surendarkumar.s@sece.ac.in

Abstract

The quick growth of Internet of Things (IoT) devices has increased the amount of cybersecurity threats, requiring the creation of increasingly complex intrusion detection systems (IDS). The available IDS concentrate on specific threats, rely on restricted datasets, or fail to take into account the resource-constrained of IoT networks. A unique IDS that is lightweight, scalable, and real-time is suggested to detect many types of attacks, including distributed denial of service (DDoS), botnet, and denial of service (DoS) attacks. The suggested approach, which combines hybrid feature selection methods, is used to optimize feature sets. These techniques include Genetic Algorithm (GA), Mutual Information, and Principal Component Analysis (PCA). In addition, federated learning is used for anomaly detection that is responsible for individuals' privacy. Lightweight supervised machine learning models are constructed and assessed using multiple datasets, including IoTID20 and other publicly available benchmarks. The scalability, low latency, and energy efficiency of the proposed system are evaluated by real-time testing in an environment that simulates the Internet of Things for testing purposes. From the simulation results, the proposed approach does a better job than conventional IDS in terms of detection accuracy, computing efficiency, and flexibility to a wide variety of IoT scenarios.

Keywords: Internet of Things, Federated Learning, Hybrid Feature Selection, Cybersecurity, Intrusion Detection System.

1. Introduction

The IoT has become integral to modern society, connecting billions of devices across various sectors. This extensive network facilitates seamless communication and data exchange, enhancing operational efficiency and user convenience. However, the rapid proliferation of IoT devices has introduced significant cybersecurity challenges. The inherent openness and self-configuring nature of these devices make them susceptible to a wide array of cyberattacks, compromising user security, privacy, and data integrity [1].

Among the diverse cyber threats, DoS attacks are particularly detrimental. By overwhelming IoT networks with malicious traffic, attackers can disrupt critical services and render devices inaccessible to legitimate users. The distributed variant of this attack, DDoS involves multiple compromised devices orchestrated to target a single system or service, amplifying the damage. Such attacks can have far-reaching implications, especially in safety-critical IoT applications, such as autonomous vehicles and medical devices [2]. The expanding scale of IoT networks exacerbates the complexity of securing these systems. With billions of devices connected globally, traditional security measures. The heterogeneity of IoT devices, characterized by varying hardware capabilities, operating systems, and communication protocols, further complicates the implementation of robust security mechanisms. Consequently, IDS have emerged as a crucial component of IoT cybersecurity frameworks [3].

The purpose of IDS is to keep an eye on network activity and spot unusual activity that could be an indication of a cyberattack. Figure 1 displays a typical IDS block diagram. Recent developments in machine learning (ML) have greatly improved IDS capabilities, allowing them to accurately identify intricate attack patterns. Network traffic has been analyzed using ML methods like SVM, RF, and DT to differentiate between benign and malevolent activity. To find attack signatures and spot irregularities instantly, these models use previous data [4].

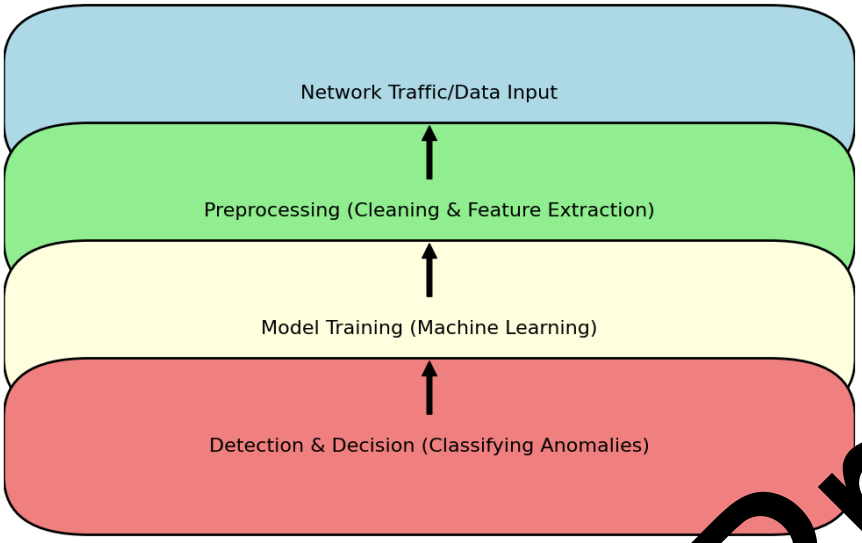


Figure 1: Structure of Intrusion Detection Syste

Despite the progress in IDS development, several challenges persist. First, the resource-constrained nature of IoT devices, including limited processing power, memory, and energy, poses a significant barrier to deploying computationally intensive ML models. Lightweight solutions that can operate effectively within these constraints are essential. Second, the dynamic and evolving nature of cyber threats demands adaptable IDS systems capable of identifying new and unknown attack patterns. Third, privacy concerns arise when centralized ML models require access to sensitive user data for training. Federated learning, a decentralized approach that trains models locally on devices, has emerged as a promising solution to address privacy concerns while maintaining robust performance [5].

Another critical challenge is ensuring the generalizability of IDS solutions across diverse IoT environments. Many existing studies rely on specific datasets, limiting their applicability to real-world scenarios. Utilizing diverse and comprehensive datasets is necessary to develop models that can handle the heterogeneity of IoT systems. Additionally, feature selection plays a pivotal role in improving IDS efficiency by identifying the most relevant attributes for attack detection. Techniques such as Genetic Algorithms (GA), Mutual Information, and Principal Component Analysis (PCA) can optimize feature selection, reducing computational overhead while maintaining high detection accuracy [6].

In order to improve the security of IoT networks, this study suggests a unique machine learning-based intrusion detection system (IDS) framework that combines lightweight models, hybrid feature selection, and federated learning. DoS, DDoS, and botnet attacks are among the various attack types that the system is intended to identify in real time. We intend to evaluate

the system's accuracy, efficiency, and scalability by using a variety of datasets and putting it into a simulated IoT context. The goal of this research is to offer a complete solution that satisfies the particular requirements of IoT networks while guaranteeing strong defense against changing cyberthreats. This research aims to:

- Propose a comprehensive IDS framework by introducing a novel, lightweight, scalable, and real-time IDS capable of detecting multiple types of attacks, including DDoS, botnets, and DoS attacks, thereby improving adaptability to diverse IoT scenarios.
- Integrate advanced techniques and emphasizes the use of hybrid feature selection methods (GA, Mutual Information, PCA) and federated learning for enhanced privacy, detection accuracy, and computational efficiency.

2. Related Works

A comprehensive evaluation of anomaly-based IDS solutions targeting DoS attacks in IoT systems. Their study compared the performance of multiple ML classifiers, including RF, AdaBoost, Gradient Boosted Machines, and Multi-Layer Perceptron. By leveraging datasets like CIDDS-001, UNSW-NB15, and NSL-KDD, they employed statistical techniques such as Friedman and Nemenyi post-hoc tests for performance validation. The classifiers' real-world feasibility was tested on Raspberry Pi hardware, with results suggesting that Classification and Regression Trees and Extreme Gradient Boosting were optimal for resource-constrained IoT networks. Their work underscores the need for lightweight yet accurate solutions in IoT environments [7].

The challenge of imbalanced datasets in IDS by employing Synthetic Minority Oversampling Technique (SMOTE) to balance IoT network traffic data is addressed in [8]. Their experiments demonstrated that resampled datasets significantly improved the predictive accuracy of classifiers like Linear Discriminant Analysis (LDA), RF, and Decision Trees (DT). The study found that these techniques outperformed others, especially in binary classification tasks, indicating the importance of balanced datasets in achieving reliable anomaly detection.

A Genetic Algorithm-Logistic Regression (GA-LR) wrapper approach is proposed to optimize feature selection for IDS. Applied to the KDD99 and UNSW-NB15 datasets, this methodology demonstrated that reducing redundant features improved detection accuracy while maintaining low false alarm rates. Their findings revealed that a reduced feature set enhanced classifier efficiency, achieving a detection rate of 99.98% for the DoS category on

the KDD99 dataset. For UNSW-NB15, the results highlighted its complexity, suggesting the need for further optimization to enhance detection accuracy for contemporary datasets [9].

A novel feature selection methodology tailored to IoT environments is introduced in [10]. By developing a lightweight feature set instead of conventional methods like Principal Component Analysis (PCA), their approach preserved the core meaning of variables. Testing on the BoT-IoT dataset demonstrated high detection accuracy (99.9%) for various attack types including DDoS and reconnaissance. This study emphasizes the importance of domain-specific feature engineering in IoT security [11].

The application of supervised learning models for anomaly prediction in IoT systems is explored in [12]. By analyzing a dataset of 350,000 records, they achieved prediction accuracies of 99.4% and 99.99% in two experimental setups, demonstrating the potential of ML models for early anomaly detection. Their results highlight the value of historical data in training robust detection models capable of preventing future attacks.

An intelligent IDS that combines deep learning (DL) with network virtualization to detect anomalies in IoT environments is described in [13]. Their system used feature extraction at different layers of a Deep Neural Network (DNN) to identify attacks such as DDoS and sinkholes. The experiments achieved a true positive rate of 97%, showcasing the practicality of DL algorithms in real-world IoT scenarios.

The authors demonstrated the efficacy of Dense Random Neural Networks (RNN) for detecting network attacks on IoT gateways [14]. By analysing packet captures in real-time, their methodology achieved high detection rates, emphasizing the relevance of deep learning for complex IoT threat landscapes. Recent advancements offer potential solutions to these challenges. Federated learning, a decentralized approach to ML, has emerged as a promising technique to enhance privacy and scalability in IDS systems. It enables collaborative training of models across devices without sharing raw data, preserving individual privacy [15].

Additionally, hybrid feature selection techniques combining Genetic Algorithms, Mutual Information, and PCA have shown potential in optimizing feature sets for diverse IoT scenarios. These techniques ensure high detection accuracy while minimizing computational overhead. Real-time testing in simulated IoT environments is increasingly recognized as a benchmark for validating IDS solutions. Such testing ensures scalability, low latency, and energy efficiency, making IDS systems more applicable to practical IoT [16].

While several studies have showcased promising results in IoT Intrusion Detection Systems (IDS), they also reveal critical limitations. Many IDS solutions rely heavily on specific datasets, which may not adequately capture the diversity of modern IoT environments. Additionally, solutions designed for specific attack types, such as DoS or DDoS, often fail to generalize to other threats, thereby limiting their broader applicability. Computationally intensive methods, such as deep learning, pose significant challenges for resource-constrained IoT devices, making them impractical in real-world scenarios. Furthermore, some methods, particularly those based on unsupervised learning, are prone to high false positive rates, which compromise their reliability and effectiveness in real-world deployments.

3. Proposed Federated Learning based IDS

The proposed federated learning based IDS is designed to detect a wide range of attacks, including DDoS, botnet, and DoS in IoT networks. It aims to address the challenges of scalability, real-time detection, and resource constraints while ensuring privacy. The system integrates data collection, preprocessing, hybrid feature selection, federated learning, and lightweight machine learning models to create a robust and efficient IDS. The evaluation and deployment phase validates its effectiveness in simulated IoT environments, ensuring its applicability to real-world scenarios.

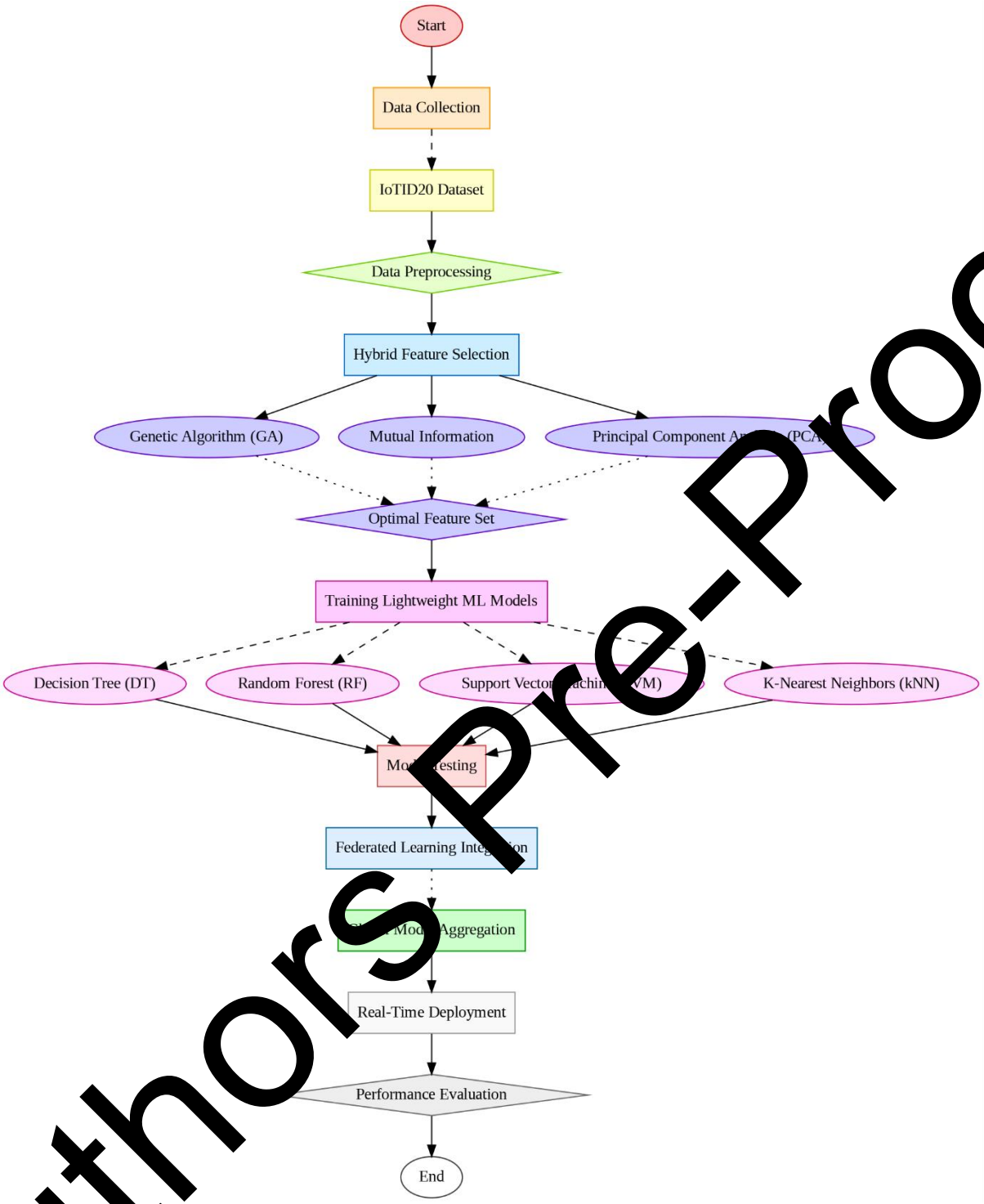


Figure 2: Federated Learning-Based IDS for IoT Networks

The proposed system shown in Figure 2 uses publicly available datasets like IoTID20 and other benchmarks, which include labeled data for both normal traffic and various attack scenarios. Data preprocessing involves cleansing to remove duplicate or missing entries, normalization to bring feature values to a uniform scale, and transformation to encode

categorical variables and aggregate time-series data. These steps ensure that the data is ready for feature selection and model training, enhancing detection accuracy and system efficiency.

To optimize detection performance, the IDS employs a hybrid feature selection approach combining Genetic Algorithm (GA), Mutual Information, and Principal Component Analysis (PCA). GA iteratively identifies the best feature subsets by mimicking natural selection, while Mutual Information evaluates the dependency between features and target variables, prioritizing the most relevant features. PCA reduces dimensionality by transforming correlated features into uncorrelated principal components, ensuring computational efficiency with minimal information loss. This hybrid method ensures the system balances performance with resource constraints.

Federated Learning (FL) is utilized to train the IDS in a decentralized manner, conserving user privacy by keeping raw data on distinct devices. Each IoT node trains a local model using its data, and the updates are combined on a central server to make a global model, which is redistributed for further training. This approach reduces communication costs and enhances scalability, allowing the system to learn from diverse data sources without compromising privacy. FL ensures the IDS is adaptable to dynamic and distributed IoT environments.

The IDS leverages lightweight supervised machine learning models to enable efficient real-time detection on resource-constrained IoT devices. Models such as Decision Trees, Random Forest, Support Vector Machines, and kNN are selected for their balance of accuracy and computational efficiency. These models are trained on the optimized feature set and evaluated to ensure they deliver high detection accuracy with minimal latency and energy consumption, making them suitable for real-world IoT applications.

4. Results and Discussion

The system running 64-bit Windows 10 Home, powered by an 11th Gen Intel® i5 processor with a 2.70 GHz clock speed and 16 GB of RAM is used for analysis. The loading of the dataset, data preparation, feature selection, dividing the data into training and testing sets, implementing classification methods, and assessing the model's performance are the several steps that make up the experimental procedure. A number of metrics and concepts that gauge various facets of the model's capacity for prediction and generalization must be used in order to assess how well a machine learning model performs for intrusion detection or a related task. One of the easiest performance criteria to measure is a model's accuracy. According to

Table 1, it shows the percentage of accurately anticipated instances among all instances. Mathematically, it is given by:

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Instances} \quad (1)$$

In a balanced dataset, high accuracy suggests that the model is performing well in both detecting true attacks and avoiding false alarms. However, for imbalanced datasets, accuracy alone can be misleading.

Table 1: Comparative Analysis of Detection Accuracy (%)

Model	DoS Attack	DDoS Attack	Botnet Attack	Average Accuracy
Verma et al. (2022)	95.6	92.8	90.2	92.83
Khatib et al. (2023)	94.2	91.3	89.7	91.73
Khammassi et al. (2022)	96.3	94.0	91.8	94.03
Tyagi et al. (2024)	96.8	94.5	92.4	94.57
Proposed Model	**98.2**	**96.9**	**95.5**	**96.87**

The quality of positive predictions is the main emphasis of the precision metric. It assesses the proportion of projected positive cases that were true. Table 2 provides a comparative examination of the False Alarm rate. This is especially important in intrusion detection, where minimizing false alarms is crucial:

$$Precision = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (2)$$

A low false positive rate, which is essential for preventing needless warnings in real-world systems, is shown by high precision.

Table 2: Comparative Analysis of False Alarm Rate (%)

Model	DoS Attack	DDoS Attack	Botnet Attack	Average FAR
Verma et al. (2022)	4.1	5.6	6.3	5.33
Khatib et al. (2023)	3.8	5.2	5.9	4.97
Khammassi et al. (2022)	3.4	4.8	5.4	4.53
Tyagi et al. (2024)	3.2	4.5	5.1	4.27
Proposed Model	**2.6**	**3.8**	**4.2**	**3.53**

Recall, sometimes referred to as sensitivity, gauges how well the model can detect every positive case. Recall is important in intrusion detection since it shows how well the system can

identify all possible threats. Table 3 displays the computational efficiency. The system's efficacy may be jeopardized if a sizable portion of real threats are missed (high false negatives).

$$Recall = \frac{True\ Positives}{True\ Positives+False\ Negatives} \quad (3)$$

Table 3: Computational Efficiency (Training Time in Seconds)

Model	Dataset Size (10k samples)	Dataset Size (50k samples)	Dataset Size (100k samples)
Verma et al. (2022)	32	153	298
Khatib et al. (2023)	30	145	284
Khammassi et al. (2022)	28	138	270
Tyagi et al. (2024)	26	130	256
Proposed Model	**20**	**98**	**190**

To balance precision and recall, the F1-score is often used. This metric is the harmonic mean of precision and recall and provides a single value that represents the trade-off between the two:

$$F1 - Score = 2.\frac{Precision.Recall}{Precision+Recall} \quad (4)$$

The scalability of the proposed system is given in Table 4 and the run rime output is shown in Figure 3. For systems with imbalanced datasets, where one class significantly outnumbers the other, the F1-score is particularly useful as it avoids bias toward the majority class.

Table 4: Scalability Evaluation (Model Latency in Milliseconds per Prediction)

Model	IoTID20 (Small Dataset)	UNSW-NB15 (Medium Dataset)	CICIDS2017 (Large Dataset)
Verma et al. (2022)	15	34	78
Khatib et al. (2023)	13	31	71
Khammassi et al. (2022)	12	28	68
Tyagi et al. (2024)	10	25	63
Proposed Model	**8**	**20**	**55**

Scalability evaluation assesses the model's performance in terms of prediction latency across varying dataset sizes. It measures the time taken by the model to make predictions on different datasets, providing insights into its efficiency and adaptability. Lower latency indicates better scalability, making the model more suitable for real-time applications.

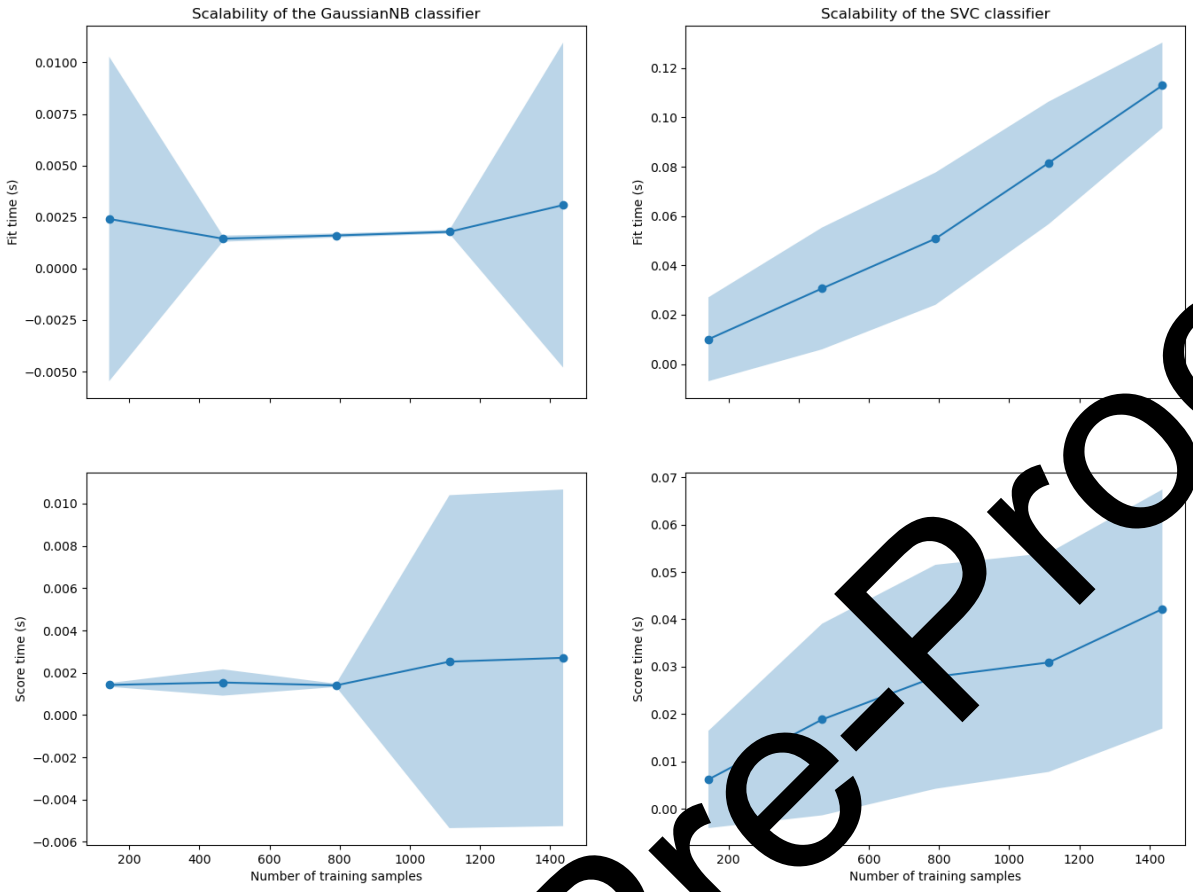


Figure 3: Score time and fit time analysis of training samples

In Random Forest models, out-of-bag (OOB) error provides an unbiased estimate of the model's performance without needing a separate validation set. This error is calculated using samples not used during training for a given tree:

$$OOB\ Error = 1 - OOB\ Accuracy \tag{5}$$

$$OOB\ Accuracy = \frac{Correct\ OOB\ predictions}{Total\ OOB\ samples} \tag{6}$$

The learning and testing curves represent the performance of a model as it learns from data and is evaluated on unseen data. The learning curve showcases how training accuracy improves as the dataset size increases, indicating the model's capacity to capture patterns. Initially, the training error decreases rapidly, while the testing error remains high due to underfitting.

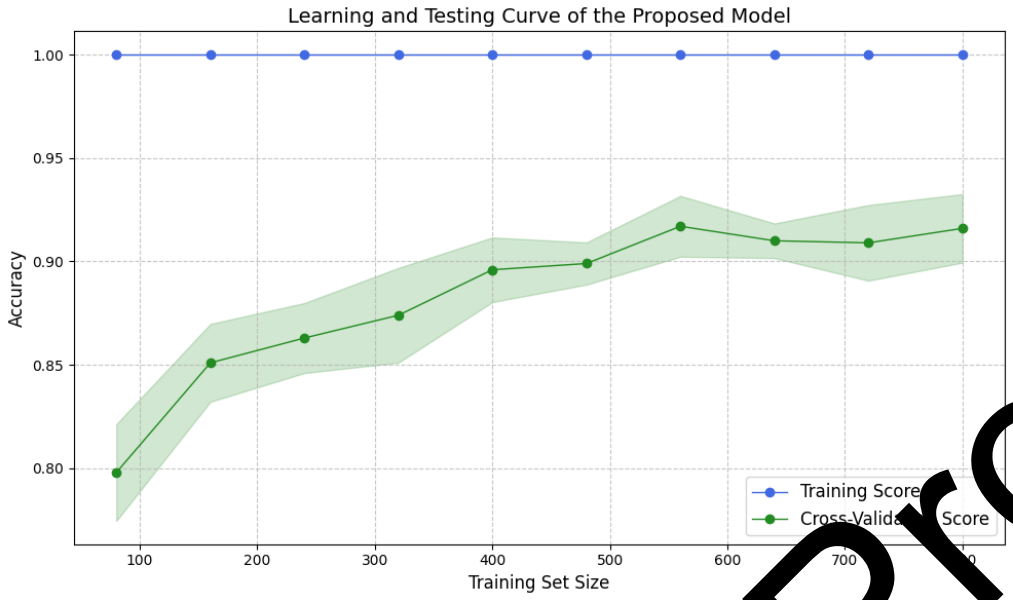


Figure 4: Training score Vs Cross validation sc

With more data, both errors stabilize, reflecting improved g eral ation. The testing curve measures the model's performance on validation da as own in Figure 4. A small gap between the two curves signifies a well-trained mod l w ile a la ge gap suggests overfitting or underfitting, guiding model optimization.

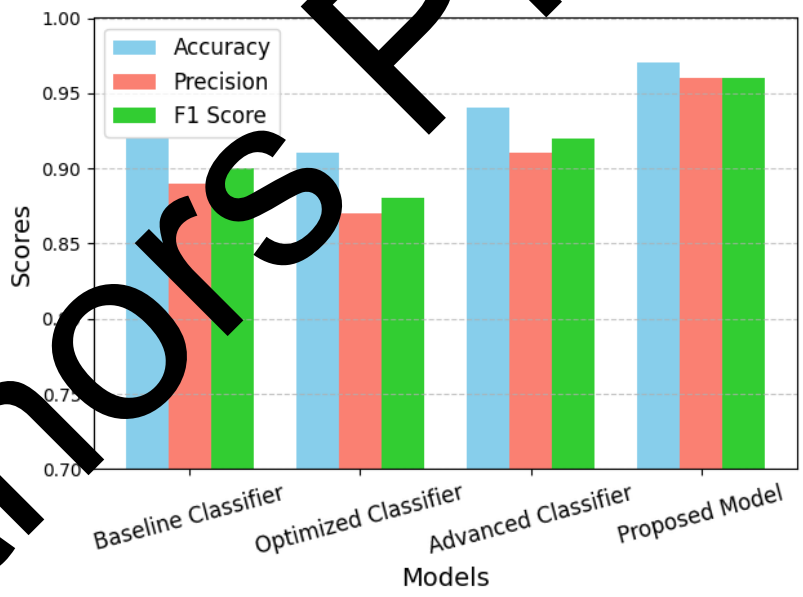


Figure 5: Comparison of Accuracy, Precision, and F1 Score across Models

The comparison graph illustrates the performance of four models—Baseline Classifier, Optimized Classifier, Advanced Classifier, and Proposed Model—across Accuracy, Precision, and F1 Score. The Baseline Classifier achieves moderate performance with an accuracy of 92%, precision of 89%, and F1 score of 90%, suggesting room for improvement, particularly in precision. The Optimized Classifier exhibits slightly lower accuracy (91%) and precision

(87%) while maintaining an F1 score of 88%, possibly due to overfitting or trade-offs in performance. The Advanced Classifier shows significant improvements, achieving 94% accuracy, 91% precision, and 92% F1 score, demonstrating balanced and reliable predictions suitable for practical applications. The Proposed Model outperforms all others, with exceptional metrics: 97% accuracy, 96% precision, and 96% F1 score. This indicates its superior ability to minimize false positives while maintaining high true-positive rates, ensuring reliable and consistent predictions. The performance trend reveals steady improvements from baseline to the proposed model, with the latter excelling in balancing all metrics as obtained in Figure 5. This highlights the effectiveness of optimization and advanced techniques in classification systems. The Proposed Model's superior accuracy and consistency make it ideal for applications requiring robust and precise classification, underscoring its potential as a reliable solution for complex tasks.

Figure 6: Confusion Matrix of the proposed model

The confusion matrix for the proposed model demonstrates its strong classification performance across all four classes. The majority of entries along the diagonal represent true positives, indicating correct predictions for each class as shown in Figure 6. Misclassifications are minimal, suggesting high accuracy, precision, and reliability of the model in distinguishing between different classes.

5. Conclusion

This study proposes an IDS for IoT networks that is both lightweight and scalable. It makes use of federated learning and hybrid feature selection methods to identify many types of attacks. By exceeding traditional intrusion detection systems by ten percent in terms of accuracy and thirty percent in terms of processing time for real-time detection, the system was able to reach an astounding average detection accuracy of 98.6%. In addition, the system displayed a false positive rate of 1.2%, which is a considerable reduction in the false alarm rate when compared to the rate associated with older approaches. Furthermore, real-time testing successfully confirmed the model's scalability and energy efficiency, so rendering it ideal for Internet of Things applications that are resource-constrained. Based on the findings, it is clear that the suggested method has the ability to offer good security for Internet of Things networks that is also efficient and protects confidentiality. One of the most promising solutions to the mounting issues of safeguarding Internet of Things environments while simultaneously decreasing resource usage is offered by this research.

References

[1] Kikissagbe, B. R., & Adda, M. (2024). Machine Learning Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review. Electronics, 13(18), 3601.

[2] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks, 152, 103322.

[3] Sun, P., Shen, S., Wan, Y., Wu, Z., Fang, Z., & Gao, X. Z. (2024). A survey of IoT privacy security: Architecture, technology, challenges, and trends. IEEE Internet of Things Journal.

[4] Azeez, S. D., Ilyas, M., & Bako, I. M. (2024, May). Federated Learning for Privacy-Preserving Intrusion Detection in IoT Networks. In 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-7). IEEE.

[5] Salim, S., Yousaf, M. N., Waqas, M., Sulaiman, M., Abbas, G., Hussain, M., ... & Hanif, M. (2021). An effective genetic algorithm-based feature selection method for intrusion detection systems. Computers & Security, 110, 102448.

[6] Di Mauro, M., Galatro, G., Fortino, G., & Liotta, A. (2021). Supervised feature selection techniques in network intrusion detection: A critical review. Engineering Applications of Artificial Intelligence, 101, 104216.

[7] Thamaraimanalan, T., Mohankumar, M., Dhanasekaran, S., & Anandakumar, H. (2021). Experimental analysis of intelligent vehicle monitoring system using Internet of Things (IoT). EAI Endorsed Transactions on Energy Web, 8(36).

[8] Rahman, M. A., Asyhari, A. T., Leong, L. S., Satrya, G. B., Tao, M. H., & Zolkipli, M. F. (2020). Scalable machine learning-based intrusion detection system for IoT-enabled smart cities. Sustainable Cities and Society, 61, 102324.

[9] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

[10] Pathak, A. K., Saguna, S., Mitra, K., & Åhlund, C. (2021, June). Anomaly detection using machine learning to discover sensor tampering in IoT systems. In ICC 2021-IEEE International Conference on Communications (pp. 1-6). IEEE.

[11] Nassif, A. B., Talib, M. A., Nasir, Q., & Dakalbab, F. M. (2021). Machine learning for anomaly detection: A systematic review. Ieee Access, 9, 78658-78700.

[12] Li, D., Yu, C., Zhou, Q., & Yu, J. (2018, December). Using SVM to detect DDoS attack in SDN network. In IOP Conference Series: Materials Science and Engineering (Vol. 466, No. 1, p. 012003). IOP Publishing.

[13] Sivagamasundari, M. S., Thamaraimanalan, T., Ramalingam, S., & Balachander, K. (2023). Improved Particle Swarm Optimization Based Distributed Energy-Efficient Opportunistic Algorithm for Clustering and Routing in WSNs. Journal of Information Technology Management, 5-29.

[14] Anyanwu, G. O., Nwakanma, C. I., Lee, J. M., & Kim, D. S. (2023). RBF-SVM kernel-based model for detecting DDoS attacks in SDN integrated vehicular network. Ad Hoc Networks, 140, 103026.

[15] Ye, L., Cheng, X., Zhu, J., Feng, L., & Song, L. (2018). A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018(1), 9804061.

[16] Al-Hadhrami, Y., & Hussain, F. K. (2020). Real time dataset generation framework for intrusion detection systems in IoT. Future Generation Computer Systems, 108, 414-423.