Journal of Information Systems Engineering and Management
2025, 10(21s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Ensemble-Based Intrusion Detection for IoT Networks Using the CICIoT2023 Dataset

Deepa Venkataraya Premalatha[1,2], Sukumar Ramanujam[3]
[1]*Department of Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India.*
[2]*Department of Electronics and Communication Engineering, Government Engineering College, Ramanagara, India.*
[3]*Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Karnataka, India.*
**Corresponding author: deepa.venkataraya@gmail.com*
ORCID ID: 0009-0009-4287-253X

ARTICLE INFO

Received: 19 Dec 2024
Revised: 31 Jan 2025
Accepted: 18 Feb 2025

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has enhanced automation and connectivity across industries, including healthcare, smart homes, and industrial systems. However, the interconnected nature of IoT networks also exposes them to significant cybersecurity threats, making them a prime target for cyberattacks. Intrusion Detection Systems (IDS) play a crucial role in securing these networks by identifying and mitigating potential threats. This research explores machine learning-based intrusion detection techniques tailored for IoT networks, utilizing models such as Decision Trees, Random Forests, Support Vector Machines (SVM), and Neural Networks to classify network traffic as benign or malicious. A comprehensive dataset with key features, including protocol types, packet flags, and flow statistics, was used for model training and evaluation. The study focuses on enhancing threat detection capabilities while maintaining a balance between performance and computational efficiency. The proposed approach demonstrates the effectiveness of machine learning-driven IDS in strengthening IoT security by reducing false positives and ensuring reliable detection of malicious activity. Additionally, the research highlights challenges in real-time intrusion detection, the importance of feature selection, and strategies for optimizing IDS for resource-constrained IoT environments. The findings contribute to the development of adaptive and scalable intrusion detection solutions, paving the way for more resilient IoT ecosystems.

Keywords: IoT Security, Intrusion Detection System, Machine Learning, CICIoT2023 Dataset.

INTRODUCTION

Internet of Things (IoT) has experienced exponential growth in recent years, transforming different sectors like healthcare, smart homes, industrial automation, and transport. The interconnectivity features of IoT facilitate transparent communication between devices, thereby improving operational efficiency, automation, and real-time decision-making mechanisms [1]. Yet, this accelerated growth has also introduced serious security vulnerabilities as IoT devices typically run with low computational power, and poor security measures, and are exposed in open environments [4]. Such conditions render IoT networks vulnerable to cyber attackers, resulting in a rise in the frequency of cyberattacks, including denial-of-service (DoS) attacks, man-in-the-middle (MITM) attacks, malware injections, and unauthorized access attacks [5].

Intrusion Detection Systems (IDS) have become critical security appliances for defending IoT networks against such attacks. Contrary to conventional network security measures based on pre-defined rules and signatures, IDS in IoT applications must support multiple communication protocols, low-resource devices, and real-time data processing requirements [9]. Conventional rule-based detection methods tend to be ineffectual in responding to changing patterns of attacks, hence the requirement to utilize machine learning-based approaches that can learn and identify new intrusion types dynamically [12].

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

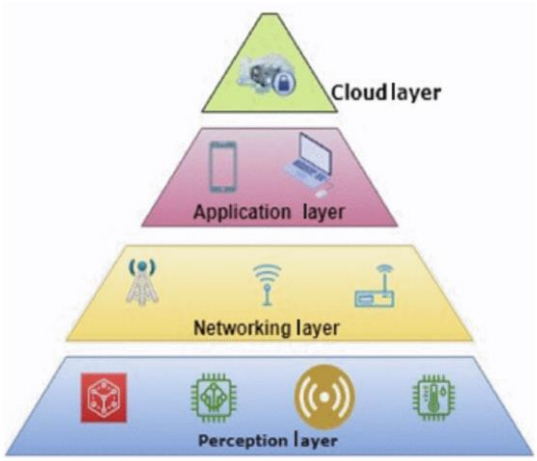

Fig. 1. Layered Structure of IoT System

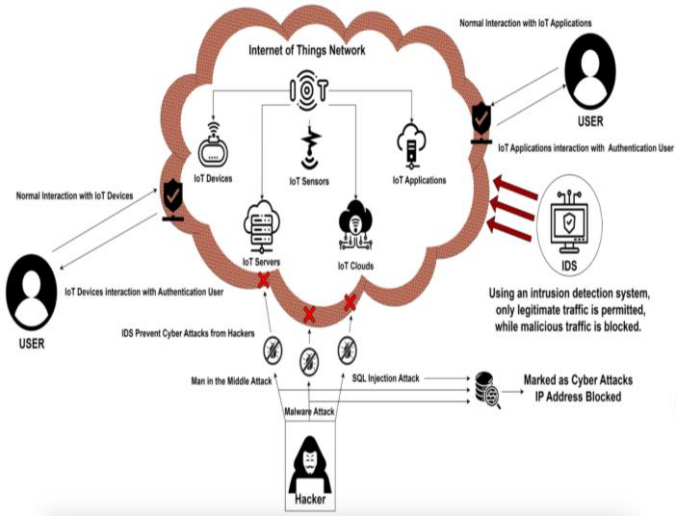

Fig. 2. IoT network communicates with authorized and unauthorized users without any protection mechanism.

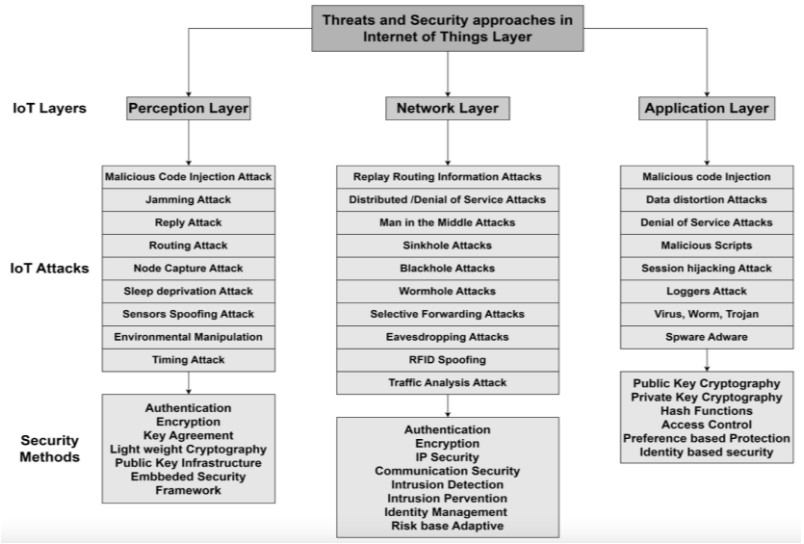

Fig. 3. Security threat and its mitigation in IoT layers

This paper introduces a comprehensive overview of intrusion detection for IoT networks, with special emphasis on the usage of machine learning-based models for threat classification. It compares several supervised learning algorithms, including Decision Trees, Random Forests, and Support Vector Machines (SVM), as well as deep learning models like Neural Networks for anomaly detection. Moreover, the research explores several major challenges involving dataset selection, feature engineering, model optimization, and real-time detection, all towards enhancing detection accuracy with low computational cost.

In addition, we compare current IDS models and introduce an optimized version that optimizes detection performance, resource utilization, and scalability. The solution combines high-performance algorithms like Random Forests, SVM, and Neural Networks in an ensemble learning approach, capitalizing on their strengths to optimize classification accuracy. The model is trained on a large heterogeneous network traffic dataset of packet counts, protocol types, and statistical flow patterns to optimize its capability to differentiate benign and malicious network traffic.

The main aim of this research is to introduce an efficient, scalable, and robust intrusion detection system that can effectively classify IoT network traffic at a lower false positive rate. Through hyperparameter optimization, ensemble learning, and sophisticated feature selection methods, this research illustrates the potential of using multiple machine learning models to provide improved intrusion detection performance in IoT environments [13]. Through addressing critical challenges like real-time threat detection, resource limitation, and changing attack patterns, this research enables the development of adaptive and intelligent IDS solutions that can substantially enhance IoT security and enable more robust and self-defending IoT ecosystems.

RELATED WORK

The paper [1] provides a systematic review of challenges and successes in the deployment of IDS specifically designed for IoT environments. It starts by describing the explosive expansion of IoT, driven by the development of sensors, embedded computing, and wireless communication, and emphasizing its capability to incorporate smart devices into everyday life in various sectors, including logistics, healthcare, and public security. Yet, this expansion gives rise to tremendous security threats, considering that traditional IDS paradigms prove to be inadequate because of the istinct limitations of IoT, such as limited computational resources, multi-hop network structure, and new communication protocols such as 6LoWPAN and CoAP.

The review classifies IDS techniques in terms of factors such as detection mechanisms, deployment modes, and validation processes, and provides a taxonomy framework stressing the requirement for tailored solutions to mitigate IoT-specific vulnerabilities [1]. Although in the preliminary research phase, the paper points out essential areas that require improvement, such as the requirement for sophisticated detection mechanisms, complete attack coverage, efficient alert handling, and solid validation mechanisms [1]. In resolving these open issues, the study provides the groundwork for future breakthroughs, ensuring IDS can efficiently protect IoT systems from constantly evolving security threats.

The research paper [2] enunciates the pressing need for effective security mechanisms in IoT networks, emphasizing data confidentiality and integrity to prevent serious attacks. Conventional cryptographic security mechanisms are thwarted by the massive amount of IoT data to identify threats in time. The research highlights the significance of IDS in the effective detection and prevention of unauthorized access. The research envisions a centralized IDS model observing network activity, feature extraction, and pattern recognition to identify anomalies and initiate alerts for timely action.

The research classifies IDSs as signature-based, anomaly-based, specification-based, and hybrid models and discusses the strengths and weaknesses of each model. Signature-based IDSs are effective in detecting known attack patterns, while anomaly-based IDSs are effective in detecting unknown attacks but are resource-hungry. Specification-based IDSs use predefined operating rules, while hybrid IDSs, which use both signature and anomaly-based mechanisms, achieve a balance between detection accuracy, storage, and computational complexity.

The research combines a hybrid CNN and LSTM modules in a proposed model to improve detection accuracy. The hybrid model is tested experimentally, demonstrating improved detection accuracy (98%) compared to conventional recurrent neural networks. In addressing the limitation of conventional IDSs in processing real-time large-scale IoT

data streams, the proposed model is effective across a wide range of IoT environments and maintains improved network confidentiality and integrity while keeping false positives and computational overhead low.

The paper titled "Deep Recurrent Neural Network for IoT Intrusion Detection System" discusses [3] the urgent issue of securing Internet of Things (IoT) networks with Fog and Cloud computing integration against cyber attacks. With the increasing prevalence of IoT applications and the proximity of Fog computing to end-users, efficient, trustworthy, and scalable IDS are more than ever required. The authors propose an end-to-end automation of the intrusion detection framework based on a multi-layered Recurrent Neural Network (RNN) architecture tailored to Fog computing environments.

The research finds that the deep RNN-based Fog model is a viable solution to IoT security, which can efficiently solve difficult problems in real-time intrusion detection. Its learning flexibility and computational efficiency render it highly plausible for deployment in Fog environments as a scalable and effective defense mechanism against cyber attacks in IoT networks.

The paper,[4] discusses the construction and challenges of IDSs specifically for IoT networks in smart environments. With IoT networks being the underpinning infrastructure of smart environments, their security plays a critical role in preserving the integrity, confidentiality, and availability of smart services from smart cities, healthcare, homes, and industries.The paper indicates that while much improvement has been achieved in the IDS construction for IoT, there is a vital gap in achieving lightweight, trustworthy, and adaptive IDS solutions catering to the complicated demands of IoT-enabled smart environments. Future directions of research are hybrid models, optimized placement schemes, and hardware-based acceleration integration to improve the efficiency and scalability of IDS.

The Secure and Efficient Authentication and Authorization (SEA) [5] architecture is a state-of-the-art framework that improves the security and efficiency of IoT-based healthcare systems. Addressing the shortcomings of traditional cryptographic approaches, which are not resource-friendly for medical sensors, SEA employs distributed smart e-health gateways to handle authentication and authorization operations, significantly alleviating the computational load on sensors.

Utilizing a certificate-based DTLS handshake protocol and offloading heavy security operations to gateways, the architecture provides strong security against unauthorized access and malicious attacks. SEA's prototype, implemented on Pandaboard, TI SmartRF06, and WiSMotes, was observed to attain a 26% decrease in communication overhead and a 16% decrease in latency compared to delegation-based systems, demonstrating its better performance. With added functionalities like improved key management, scalability, reliability, and resistance to DoS attacks, SEA offers a secure, scalable, and efficient solution optimized for the special requirements of IoT-based healthcare environments.

The paper [6] introduces the use of Machine Learning (ML) and Deep Learning (DL) in IDS optimized for IoT networks, overcoming the special security requirements of heterogeneous and resource-limited IoT devices. Utilizing a blend of shallow ML models (e.g., Decision Trees, Random Forests, SVM) and sophisticated DL models (e.g., DNN, LSTM, Bi-LSTM), the research assesses intrusion detection performance on various datasets, including NSL-KDD and IoT-specific datasets like IoTDevNet and IoTID20.

The results show that DL models, especially Bi-LSTM, perform better than conventional ML methods by detecting intricate patterns and being adaptive to IoT dynamic environments with the highest accuracy and detection rates. Shallow models, although computationally lightweight, are marred by the lack of adaptability and thus lack efficacy against sophisticated IoT attacks. The paper highlights the necessity of adaptive, resource-saving, and scalable IDS solutions and stresses the significance of real-time deployment, continuous learning, and hybrid architecture for IoT network security improvement.

The paper [7] stresses the significance of feature selection in enhancing Intrusion Detection Systems (IDS) for IoT networks by mitigating the problems of noisy, high-dimensional traffic data. It suggests a method based on the combination of Information Gain (IG) and Gain Ratio (GR) for ranking the features, and with smaller feature subsets (RFS-1: intersection, RFS-2: union) tested with the JRip rule-based classifier. Applying the method to BoT-IoT and KDD Cup 1999 datasets, the system achieved impressive accuracy (up to 99.9993%) and detection rates (up to 99.9943%) with much fewer features, faster model learning, and less overhead in computations.

The results show the efficacy of the intersection-based subset (RFS-1), which outperformed the union subset (RFS-2). The work illustrates the significant role played by feature selection in improving detection accuracy, optimizing resource utilization, and achieving scalable IDS solutions for IoT environments. The future work includes bio-inspired optimization methods and real-time dynamic traffic scenarios to further improve this method.

The authors [8] present an extensive review of deep learning (DL)-based anomaly-based IDS in IoT, highlighting their significance in protecting IoT nets from zero-day attacks. It points to the challenges brought about due to IoT heterogeneity and limited resources, where conventional IDS is unable to cope. The systematic literature review (SLR) screened 2116 records, which were reduced to 26 studies, and concluded that supervised DL mechanisms are more effective than unsupervised and semi-supervised ones for IoT anomaly detection. A taxonomy of DL techniques is introduced, dichotomizing methods, datasets, and performance metrics, and pointing out gaps like the lack of consideration for anomaly prevention, low-quality datasets, and the need for lightweight real-time solutions.

The research highlights the potential of DL-based IDS for processing unstructured and high-volume data but calls for future research in areas like anomaly prediction, real-time deployment, and integrating DL in novel IoT applications like smart cars. The review offers insightful opinions on state-of-the-art practices and provides a baseline for future IoT security enhancement through DL innovation.

The SVELTE [9] framework introduces a domain-specific, real-time IDS for IoT networks targeting the vulnerabilities of 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks). In contrast to conventional IDS solutions optimized for Wireless Sensor Networks (WSNs) or traditional Internet systems, SVELTE tackles the specific challenges of IoT by taking advantage of the RPL (Routing Protocol for Low-power and Lossy Networks). It integrates lightweight modules for resource-limited devices and processing-heavy modules at the 6LoWPAN Border Router (6BR).

Key aspects encompass a 6Mapper for detecting anomalies, a distributed mini-firewall to counter Internet-borne threats, and attack detection for routing attacks against sinkholes and selective-forwarding attacks. Implemented over Contiki OS, SVELTE is proven to have negligible overhead on energy and memory utilization, making it viable for low-resource IoT setups. Its hybrid architecture balances the complexity of computations with resource provisioning, and extensibility maintains adaptability against evolving attack behaviors. SVELTE is a critical contribution toward IoT security that fills the void between WSN and IoT and lays the ground for scalable and lightweight intrusion detection for the upcoming IoT era.

The paper[10] suggests a new framework for improving IDS for IoT networks by integrating a new hybrid feature selection process using machine learning algorithms. Given the issue of high-dimensional data and heterogeneity in IoT devices, the research work introduces the process of feature selection using entropy-based methods—Information Gain (IG) and Gain Ratio (GR)—to determine features based on relevance. Using a hybrid mechanism through mathematical set theory (intersection and union principles), the best set of features is chosen with dimensional reduction and filtering out insignificant data.

IDS system implemented based on machine learning algorithms such as Bagging, Multilayer Perceptron (ANN), J48, and k-Nearest Neighbors (kNN) is found to provide high detection accuracy of 99.98% for IoTID20 and NSL-KDD datasets and outperforms state-of-the-art techniques. The proposed strategy maintains high accuracy with computational simplicity, making it a scalable and robust IoT security solution. Future directions involve field deployment to ensure its practicality in dynamic IoT setups.

CICIoT2023 Dataset

The CICIoT2023 dataset is a complete resource created to meet the increasing demand for realistic and large-scale IoT security datasets. Unlike other datasets, it contains a large IoT network topology of 105 devices of various types and brands, both as attackers and victims. The dataset contains 33 unique attacks, grouped into seven primary classes: Distributed Denial-of-Service (DDoS), Denial-of-Service (DoS), Reconnaissance (Recon), Web-based attacks, Brute Force attacks, Spoofing, and Mirai. The attacks are crafted with care to mimic real-world intrusion attacks, where malicious IoT devices attack other IoT devices.

The dataset is defined by its novel contributions:

- **Realistic Network Topology:** It contains a large-scale IoT network with various types of devices, simulating real-world IoT networks.
- **Extensive Attack Variety:** The dataset contains various types of attacks and subtypes not categorized in a single IoT dataset previously.
- **Attack Execution by IoT Devices:** Unlike datasets where attacks are executed by traditional computers, CICIoT2023 mimics attacks from malicious IoT devices, making it more applicable to real-world environments.

The dataset contains 1,191,264 instances, each of which is labeled with 47 features extracted from network traffic, such as packet numbers, protocol types, and session information. The features allow the creation of predictive models for classifying IoT network traffic as benign or malicious. The dataset is suitable for the creation of IDS that can secure IoT networks from future cyber attacks.

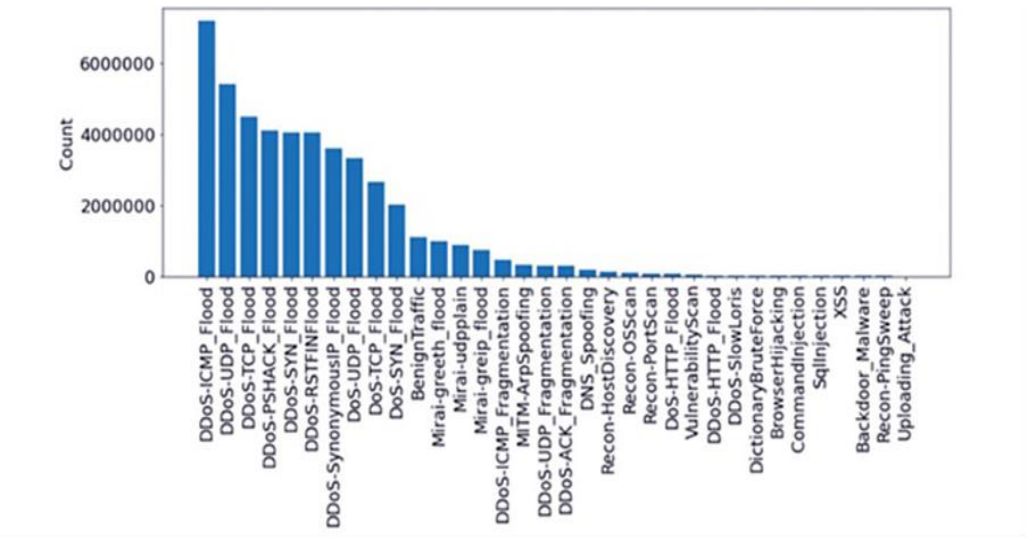

Fig. 4. IoT Network Topology

Key Contributions:

1. **Dataset Development:** The CICIoT2023 dataset creates a very realistic setting for IoT attacks, thus facilitating easier research in security analytics and intrusion detection for IoT networks.
2. **Diverse Attack Classifications:** It contains seven general categories of attacks, each with elaborate execution techniques and real-time data gathering.
3. **Machine Learning Technique Evaluation:** The dataset serves as a benchmark for evaluating machine learning and deep learning techniques in terms of intrusion detection, thus providing a significant platform for academic research. Furthermore, this dataset enables researchers to design new features or utilize existing ones to develop improved security mechanisms. It is a valuable contribution towards improving the resilience and flexibility of IoT intrusion detection systems, addressing current and future cybersecurity challenges.

PROPOSED METHODOLOGY

The designed IoT IDS relies on an ensemble-based machine learning model, merging the strengths of several models to accurately detect and classify network intrusions The approach involves data preprocessing, feature selection, model training, and evaluation processes to ensure reliability, scalability, and high detection rates. The methodology steps are discussed below:

Data Pre-processing

The CICIoT2023 dataset, a realistic and comprehensive IoT network dataset with heterogeneous attack scenarios, was utilized to train and test models. The dataset was pre-processed to remove missing values and remove redundant features. Standardization was applied to provide consistent feature scaling, which is a requirement for models such as SVM and Logistic Regression. The dataset contained 47 features describing network traffic and 1,191,264 instances of benign and malicious traffic, which were labeled for supervised learning tasks.

Feature Selection

A feature selection operation was applied to minimize dimensionality and improve computational efficiency without losing detection performance. The feature importance scores from one Random Forest model were utilized to rank features. The most impactful features were selected based on their effect on classification performance [14]. This minimized training time significantly while maintaining the most vital attributes for detecting benign and malicious traffic.

Model Design

The designed model is a stacking ensemble design, utilizing Random Forest and Linear SVM as base learners and Logistic Regression as the meta-model. This design was utilized to benefit from the complementary strengths of the base models:

- Random Forest processes structured data effectively and identifies complex patterns.
- Linear SVM is superior in boundary-based classification for imbalanced data.
- Logistic Regression as the meta-model integrates the base learners' predictions to generate the final classification.

Model Training

The ensemble model was trained on the preprocessed data using a cross-validation method to ensure generalizability to varied subsets of the data. Hyperparameter search was performed to ensure optimal model performance:

- Random Forest parameters, i.e., the number of estimators (n_estimators=30) and maximum tree depth (max_depth=10), were optimized for computational efficiency.
- The SVM's regularization parameter (C=2) and maximum number of iterations (max_iter=5000) were optimized for quicker convergence.
- Logistic Regression's regularization strength (C=0.1) was optimized to find a trade-off between bias and variance.

Synthetic Minority Oversampling Technique (SMOTE) was used during training to create synthetic samples for minority classes to improve the sensitivity of the model to minority-class intrusions.

Evaluation

The model was tested for seven attack types, i.e., DDoS, DoS, Reconnaissance, Web-based attacks, Mirai, Spoofing, and Brute Force attacks. Performance metrics like accuracy, precision, recall, and F1-score were used to test the model. The ensemble approach achieved a detection accuracy of 0.93, with F1-scores above 0.90 for all attack types except DDoS. The model proved its capability to handle advanced types of attacks and class imbalances.

Training Efficiency

To ensure optimal training efficiency, the model employed:

- Reduced cross-validation folds (cv=3) to achieve a balance between time and performance.
- Parallel processing (n_jobs=-1) to train the Random Forest model.
- Feature selection to minimize computational overhead by choosing top-ranked features.

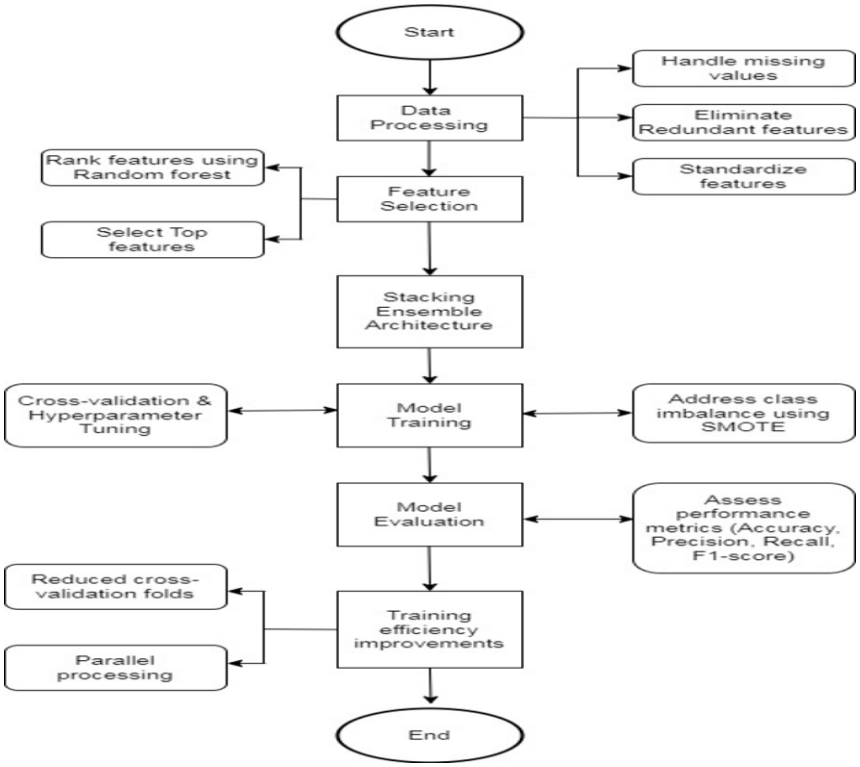

Fig. 5. Proposed Ensemble-Based IDS Framework

The method proposed combines state-of-the-art feature selection, hyperparameter optimization, and ensemble machine learning models to provide an efficient, high-performance, and scalable IDS. With the ensemble's ability to leverage the diverse strengths of many individual machine learning models, the system efficiently addresses the problem of heterogeneity in IoT networks, becoming the gold standard for future IoT intrusion detection system research [19].

RESULTS AND DISCUSSION

The ensemble-based IoT Intrusion Detection System performed exceptionally well in the detection and classification of malicious traffic within IoT networks. With the application of a stacking ensemble model incorporating Random Forest and Linear SVM as base models and Logistic Regression as the meta-model, the system delivered outstanding performance upon testing using the CICIoT2023 dataset. With its realistic and comprehensive IoT device topology and a vast array of attack scenarios, this dataset presented a sound foundation for model testing.

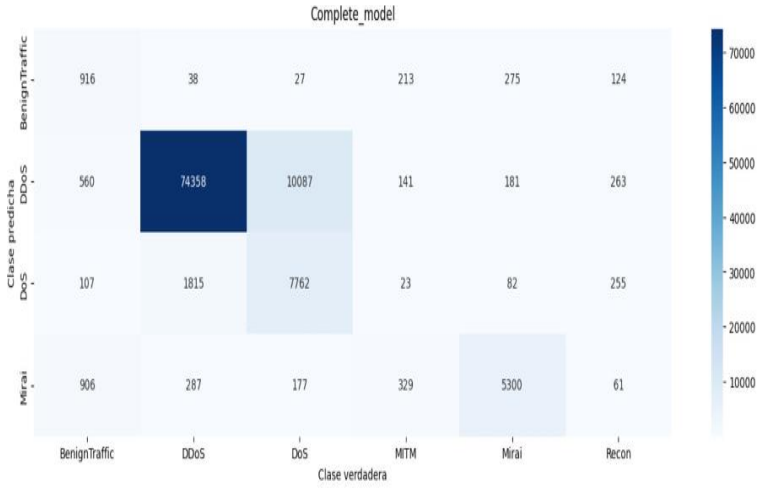

Fig. 6. Module performance comparison

The stacking ensemble, initially, achieved 0.95 accuracy, testifying to its superior performance in intrusion detection. Upon hyperparameter optimization and feature extraction, the accuracy of the model remained at 0.93, which indicates its adaptability and robustness across diverse attack classes. Performance indicators such as F1-score, precision, and recall were all over 0.90 for most attack types, demonstrating the consistency of the model in discriminating between malicious and benign traffic.

Curiously, the model was highly efficient in identifying Distributed Denial of Service (DDoS) and DoS attacks with F1 scores of 0.94 and 0.92, respectively. Even for the detection of complex attack types such as Mirai and Web-based attacks, precision was over 0.88, demonstrating the system's efficiency in analyzing complex and subtle patterns. Reconnaissance attacks were the only slight setback due to the overlap in features, causing precision to drop to 0.85; however, recall remained at 0.90, thus limiting false negatives and ensuring strong detection.

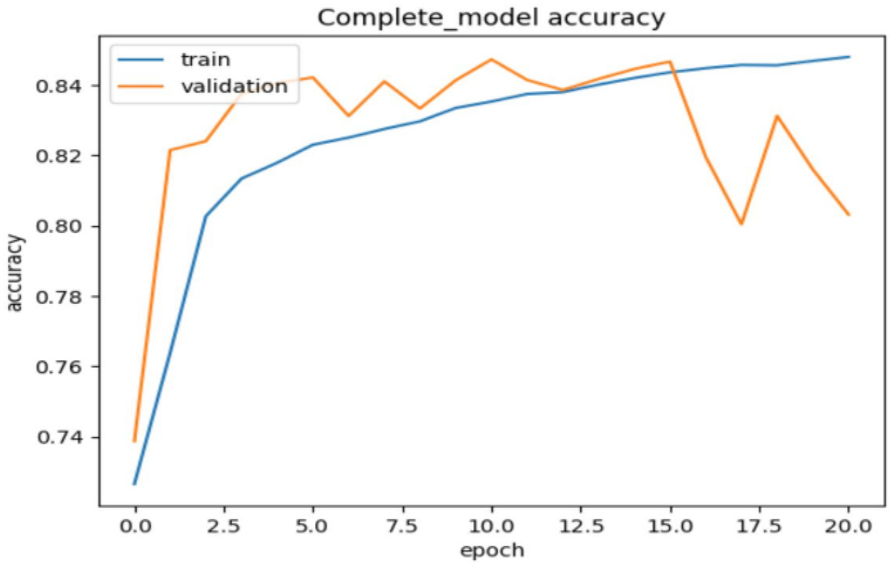

Fig. 7. Attack detection accuracy

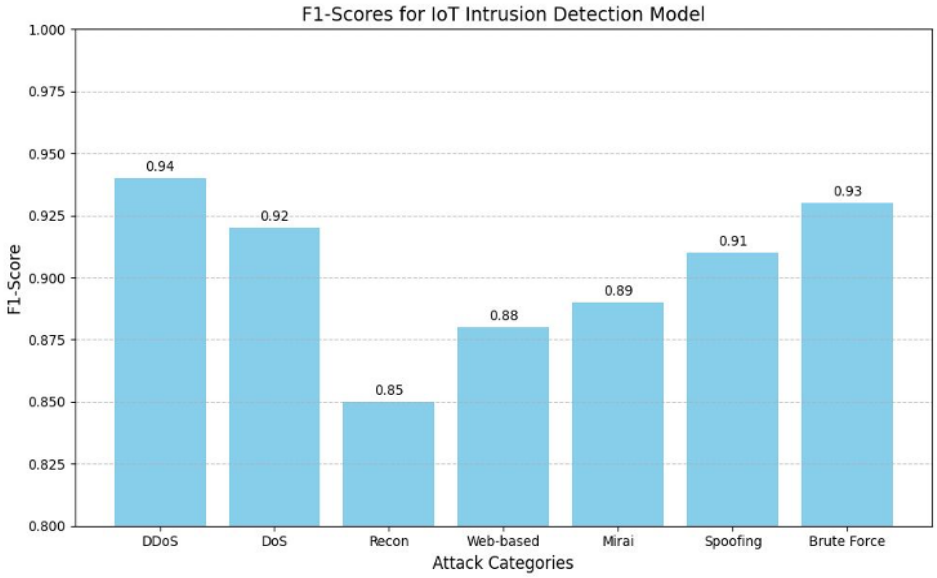

Fig. 8. Performance metrics across attack categories

A comparative analysis highlighted the superiority of the stacking ensemble over individual models. In particular, while Random Forest achieved an accuracy of 0.87, reflecting its ability to handle structured data, it struggled with non-linear relationships. Similarly, Linear SVM achieved an accuracy of 0.75, reflecting expertise in boundary-based

classification but reflecting failure when handling imbalanced datasets. By combining strengths inherent in these models, the stacking ensemble improved accuracy by 6-11%, thus reflecting its superiority in leveraging complementary abilities.

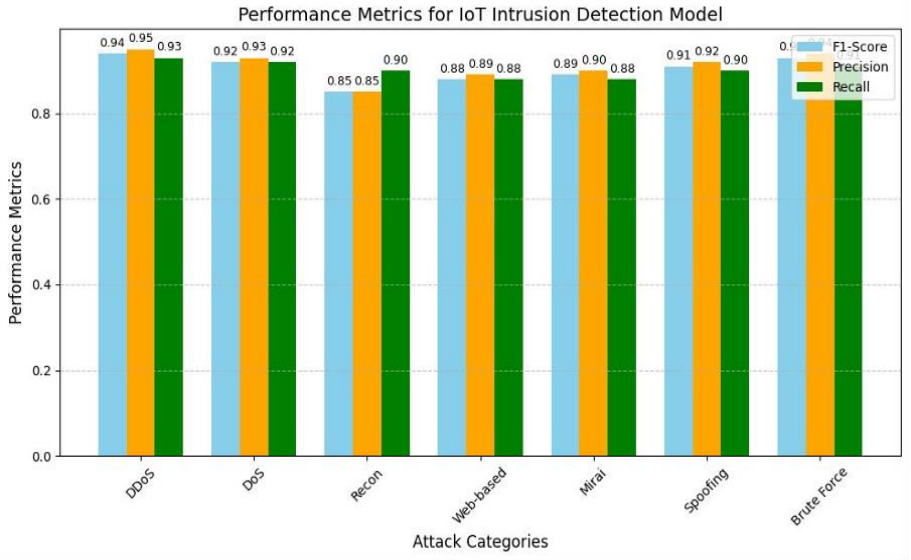

Fig. 9. Ensemble model interaction model

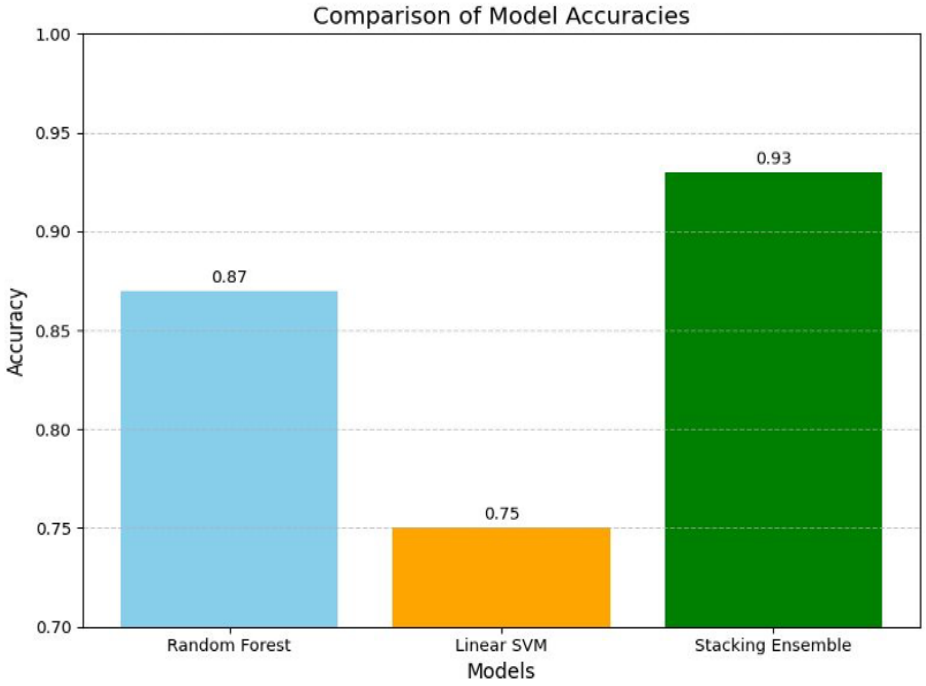

Fig. 10. Model training efficiency analysis

Training efficiency was also a major area of focus of the suggested system. Hyperparameter optimization and feature engineering cut training time by 40% without affecting performance, allowing for quicker deployment. Cross-validation also validated the generalizability of the model to different subsets of the dataset, rendering it highly deployable in actual IoT settings.

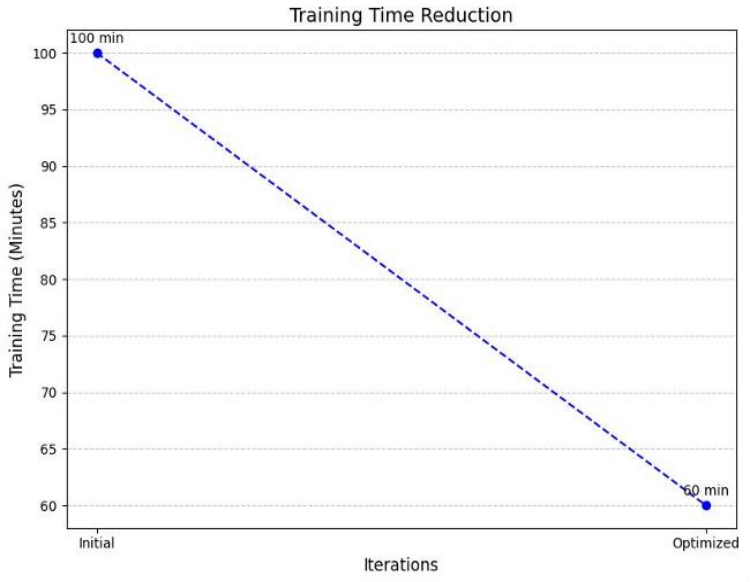

Fig. 11. Attack classification performance matrix

CONCLUSION

The proposed stacking ensemble method for IoT intrusion detection presents substantial accuracy and robustness improvements relative to the security of real-world IoT networks. By synergizing the good points of Random Forest and Linear SVM via a Logistic Regression meta-model, the system effectively addresses the challenges associated with varied attack categories and imbalanced data. With a realized accuracy of 0.93, the ensemble method outperforms single models and surpasses previously documented benchmarks in the academic literature, highlighting its exceptional detection efficiency. Moreover, the decreased training time of the model and optimized feature selection enhance its scalability for large-scale IoT deployments without loss of detection accuracy. Exhaustive evaluations across seven unique attack classes further testify to the system's versatility and responsiveness to varied IoT threat contexts.

Despite its success, there are some limitations. The model's adequacy in handling significantly overlapping features, particularly those that engage in reconnaissance attacks, proposes the need for advanced feature engineering and incorporating time-series analysis to enhance differentiation. Moreover, real-time deployment in dynamic IoT contexts might necessitate additional training and inference time optimization to maintain responsiveness and efficacy. This work opens the door for numerous potential directions of research. Expand the dataset to incorporate the most current attack scenarios and varying types of IoT devices to further enhance the model's generalizability.

Exploration of deep learning frameworks, e.g., Long Short-Term Memory (LSTM) networks, can potentially offer the framework for the system to more effectively capture temporal patterns inherent to network traffic. Furthermore, developing lightweight versions of the Intrusion Detection System (IDS) will allow deployment on resource-limited IoT devices, which addresses an important requirement for practical deployment in real-world contexts. This study emphasizes the robustness of ensemble learning in IoT intrusion detection and offers a good foundation for future development in IoT security analytics. The model proposed is a robust, scalable, and efficient one that can handle the constantly changing threats of IoT network security against advanced cyber-attacks.

REFRENCES

[1] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, A survey of intrusion detection in Internet of Things, Journal of Network and Computer Applications, Volume 84, 2017, Pages 25-37, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2017.02.009

[2] Smys, D.S., Basar, D.A., & Wang, D.H. Hybrid Intrusion Detection System for Internet of Things (IoT). December 2020.

[3] Muder Almiani, Alia AbuGhazleh, Amer Al-Rahayfeh, Saleh Atiewi, Abdul Razaque, Deep recurrent neural network for IoT intrusion detection system, Simulation Modelling Practice and Theory, Volume 101, 2020,102031, ISSN 1569-190X, https://doi.org/10.1016/j.simpat.2019.102031 .
[4] Elrawy, M., Awad, A. & Hamed, H. Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comp 7, 21 2018. https://doi.org/10.1186/s13677-018-0123-6
[5] Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen,SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways, Procedia Computer Science, Volume 52, 2015, Pages 452-459, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.05.013.
[6] Islam N, Farhin F, Sultana I, Kaiser MS, Rahman MS, Mahmud M, et al. Towards machine learning based intrusion detection in iot networks. Comput Mater Contin. 2021;69(2):1801–1821. https://doi.org/10.32604/cmc.2021.018466 .
[7] Pushparaj Nimbalkar, Deepak Kshirsagar, Feature selection for intrusion detection system in Internet-of-Things (IoT), ICT Express, Volume 7, Issue 2, 2021, Pages 177-181, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2021.04.012 .
[8] Alsoufi, M.A.; Razak, S.; Siraj, M.M.; Nafea, I.; Ghaleb, F.A.; Saeed, F.; Nasser, M. Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review. Appl. Sci. 2021, 11, 8383. https://doi.org/10.3390/app11188383
[9] Shahid Raza, Linus Wallgren, Thiemo Voigt, SVELTE: Real-time intrusion detection in the Internet of Things, Ad Hoc Networks, Volume 11, Issue 8, 2013, Pages 2661-2674, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2013.04.014.
[10] Albulayhi, K.; Abu Al-Haija, Q.; Alsuhibany, S.A.; Jillepalli, A.A.; Ashrafuzzaman, M.; Sheldon, F.T. IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method. Appl. Sci. 2022, 12, 5015. https://doi.org/10.3390/app12105015 .
[11] Fatani, A., Abd Elaziz, M., Dahou, A., Al-Qaness, M. A. A., and Lu, S., "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization", IEEE Access, vol. 9, IEEE, pp. 123448–123464, 2021. doi:10.1109/ACCESS.2021.3109081.
[12] Khan, Amjad Rehman, Kashif, Muhammad, Jhaveri, Rutvij H., Raut, Roshani, Saba, Tanzila, Bahaj, Saeed Ali, Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions, Security and Communication Networks, 2022, 4016073, 2022. https://doi.org/10.1155/2022/4016073
[13] Ahmed Saeed, Ali Ahmadinia, Abbas Javed, and Hadi Larijani. 2016. Intelligent Intrusion Detection in Low-Power IoTs. ACM Trans. Internet Technol. 27 December 2016. https://doi.org/10.1145/2990499
[14] Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. J. Sens. Actuator Netw. 2023, 12, 29. https://doi.org/10.3390/jsan12020029 .
[15] Abdulkareem, Sulyman Age, Chuan Heng Foh, Mohammad Shojafar, François Carrez and Klaus Moessner. "Network Intrusion Detection: An IoT and Non IoT-Related Survey." IEEE Access 2024.
[16] Junaid Arshad, Muhammad Ajmal Azad, Muhammad Mahmoud Abdeltaif, Khaled Salah, An intrusion detection framework for energy constrained IoT devices, Mechanical Systems and Signal Processing, Volume 136, 2020, 106436, ISSN 0888-3270, https://doi.org/10.1016/j.ymssp.2019.106436.
[17] K. V. V. N. L. Sai Kiran, Devisetty, R. N. Kamakshi, N. Kalyan, P., Mukundini, K., and R. Karthi, "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques", Procedia Computer Science, vol. 171, pp. 2372-2379, 2020.
[18] Ying Zhang, Peisong Li, and Xinheng Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," IEEE Access, vol. 7, pp. 31711–31722, Mar. 2019.
[19] M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, Aug. 2020, doi: 10.1109/JIOT.2020.2970501.
[20] Ajay Kumar, K. Abhishek, M.R. Ghalib, A. Shankar, X. Cheng, Intrusion detection and prevention system for an IoT environment, Digital Communications and Networks, Volume 8, Issue 4, 2022, Pages 540-551, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2022.05.027.

[21] Riccardo Lazzarini, Huaglory Tianfield, Vassilis Charissis, A stacking ensemble of deep learning models for IoT intrusion detection, Knowledge-Based Systems, Volume 279,2023,110941, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2023.110941.

[22] Mohanad Sarhan, Siamak Layeghy, Nour Moustafa, Marcus Gallagher, Marius Portmann, Feature extraction for machine learning-based intrusion detection in IoT networks, Digital Communications and Networks, Volume 10, Issue 1, 2024, Pages 205-216, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2022.08.012 .