Volume (1) No (9), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Efficient ML-Based Identification Models of Network Intrusion in Internet of Things (IoT) Systems

Dr.Nilesh Jain
Associate Professor
Department of Computer Sciences and Applications
Mandsaur University
Mandsaur
nileshjainmca@gmail.com.

***Abstract*—The wide adoption of IoT devices has brought about increased connectedness and convenience, but it has also revealed new security concerns. Protecting IoT systems from malicious hackers is crucial as they become more important in various areas. Using the Random Forest (RF) method for machine learning, this study presents an efficient and effective Intrusion Detection System (IDS) tailored to Internet of Things (IoT) devices. The research employs a wide variety of data processing approaches, including data cleaning, normalization, and one-hot encoding, to get the NSL-KDD dataset ready for model training and testing. With a remarkable 99.9 % accuracy, precision, recall, and F1-score, the RF model surpassed other conventional modelling approaches, such as Decision Tree (DT), Support Vector Machine (SVM), and Conv1d networks. Using ensemble learning effectively is where this approach really shines. Interpretability was also facilitated by visualization (including correlation heatmaps and feature importance plots), which helped in selecting features. Effectiveness of the system under verification was confirmed with consistent evaluation metrics and confusion matrices analysis, and RF in the ability to reliably differentiate between malicious and normal traffic.**

***Keywords*—Internet of Things (IoT), Intrusion Detection System (IDS), Cybersecurity, Machine Learning, Network Security, Anomaly Detection.**

I. INTRODUCTION

The rise of cyber security attacks and the need to detect suspicious activities in an environment characterized by heterogeneity but limited resources and abilities has triggered the emergence of sophisticated Intrusion Detection Systems (IDS) to detect intrusion attempts much earlier [1][2]. IDS is considered a significant part of network security monitoring trends and detecting any possible breach of security. Most of the traditional protection methods, IDS, are based on signature forms and methods of IDS are lacking the potential of identifying new and highly complex attacks [3]. IDS are an essential part of network security because they can identify malicious users and take action against them before they cause damage [4][5].

Internet of Things" (IoT) is a concept that describes a way of thinking about how different physical and virtual things might be connected and communicated through the Internet [6][7]. Smart cities, healthcare, farming, and transportation are just a few of the many areas that benefit from IoT networks [8]. Unauthorized access, data theft, denial of service, and hostile assaults are only a few of the many security issues that IoT networks confront [9][10][11]. Therefore, it is critical to design and implement effective IDS for IoT organizations to protect them from potential threats and ensure their constant availability and quality [12]. The IoT, which includes machines, sensors, and cameras, is rapidly expanding the number of internet-connected things [13].

Intruder detection systems that rely on machine learning have three options for how to go about their training phase [14]. One thing to keep in mind is that most IoT intrusion detection systems that use machine learning do so through cloud services. Cloud computing's infinite resources and massive storage capabilities make it ideal for training ML models [15][16]. Researchers have focused on and made significant strides in energy-efficient machine learning in recent years [17][18][19]. There are two parts to ML's efficiency: training and inference. Running model training on hardware for weeks or months at a time consumes a lot of energy, which has a negative impact on the environment.

A. Motivation and Contribution of the Study

The growing number of IoT devices in urban planning, public transit, and healthcare has made networks more susceptible to cybercrimes including hacking, data loss, and DoS assaults. If you want to find new and advanced threats, you need a more advanced intrusion detection system than the traditional ones that rely on signatures. Alternatively, connected devices with limited resources aren't a good fit for many ML-based solutions because of how much power and computation they consume. It is very critical to develop accurate, scalable, and energy-efficient IDS if enable the dependable and real-time detection of malicious activity in the several IoT networks.

The following are the primary benefits of this study:

- Applied the NSL-KDD dataset, a popular standard for intrusion detection studies, to ensure that the results were applicable and comparable.
- Improved data quality and model performance by implementing necessary pre-processing procedures, such as data cleaning, normalization, and one-hot encoding.

- Developed and deployed an IDS for IoT environments that makes use of the Random Forest classification algorithm to effectively identify potential threats.
- Among the metrics used to assess the model's efficacy were F1-score, recall, accuracy, and precision.
- Adapted the approach and analysis of the study to the contexts of the IoT-based networks and provided helpful guidelines that can be used in practice.

B. Novelty and Justification of the Study

The study is justified by the existence of a pressing need to strengthen IoT networks, which are particularly vulnerable because of their widespread application, diversity in architecture, and resource-restrained characteristics. Although current IDS strategies have proven their usefulness in traditional networks, their use of signature-based mechanisms or an expensive high degree of deep learning makes them inapplicable in IoT networks. To overcome this deficit, the contribution of the present work is to propose a Random Forest (RF)-based IDS that incorporates an efficient data pre-processing procedure, feature selection procedure, and ensemble learning in order to enhance its detection capabilities with low complexity. Unlike prior studies, the proposed approach leverages the NSL-KDD dataset to construct a lightweight yet robust IDS, ensuring adaptability to dynamic IoT traffic patterns while maintaining scalability, energy efficiency, and resilience against both known and emerging cyber threats.

C. Structure of the Paper

The following is the paper's outline In Section II, survey the literature on IDS for IoT devices; in Section III, lay out the approach; in Section IV, shows the results and compare the models; and in Section V, provide conclusions and suggest areas for improvement.

II. Literature Review

An overview of the research on intrusion detection systems for IoT devices is given in this section. Common themes emerging from the reviewed literature include:

Mahamud, Uddin and Sumaiya (2025) suggested that the fast growth of the IoT has changed modern life by providing unmatched automation and seamless connectivity between devices, which often work without any human input. This comfort, however, is associated with a high price in reduced cyber-resistance levels of IoT equipment that may have devastating results in case they are not timely neutralized. To tackle this pressing challenge, study proposes innovative strategies powered by machine learning algorithms, achieving an exceptional 99.97% detection accuracy and a 0.0% false positive rate. Leveraging the Bot-IoT dataset for evaluation, approach demonstrates marked improvements over existing detection methodologies [20].

Valavan and Joseph (2025) helped protect IoT networks by detecting deviations from normal operations, potentially preventing cyberattacks. The proliferation of IoT devices makes it more difficult to notice odd actions on a broad scale, making networks more exposed to cyber assaults. In order to manage increasing security risks and guarantee dependable performance in IoT contexts, a robust intrusion detection system is required for anomaly detection. Standardization and hash encoding are used to pre-process the data. While LSTM handles classification, NCF-SSA excels in selecting important features from input data. Utilizing the UNSW NB15 dataset, the proposed method attains a 92.78% F1-score and a 94.56% precision [21].

Archana et al. (2024) suggested the IoT and its uses make life easier, many researchers are very interested in them. Consequently, it is now required that the method for identifying malware in the Internet of Things be used. In this study, an integrated IDS called CNN-IoT is proposed. Its purpose is to monitor IoT devices for harmful activities. The suggested approach was assessed using the NSW-NB15 dataset. 98.54% accuracy was achieved using a type II inaccuracy rate of about 0.01. The suggested strategy operates better than the other current approaches that are documented in the research, according to preliminary assessments [22].

Racherla et al. (2024) introduced Deep-IDS, a state-of-the-art IDS developed using DL that is both innovative and prepared for implementation. In its training on the CIC-IDS2017 dataset, it utilizes a 64-unit LSTM network. The basic design of Deep-IDS makes it a good fit for deployment on edge servers; it protects the Internet and IoT nodes from DoS, DDoS, Brute Force, Man-in-the-Middle, and replay attacks. Research significantly enhanced Deep-real-time IDS's performance by analyzing the trade-offs between intrusion detection rate (DR) and false alarm rate (FAR). An astounding 97.67% overall classification accuracy and 96.8% detection rate are achieved by the system at the 70% DR-FAR trade-off level [23].

Mahmud et al. (2024) designed and executed a unique approach to component extraction and selection (method). A model-based IDS based on five ML algorithms is presented in this paper. It is designed to be used with machine learning networks that have been appropriately tuned for hyperparameters. Notable feature selection algorithms and classifiers like KNN, DT, RF, GB, and AdaBoost are utilised by the system. With an accuracy percentage of 99.39%, RF outperformed all of the classifiers. The KNN classifier achieved the lowest accuracy of 94.84% out of all the models that were examined [24].

Hafid, Ezzouhairi and Haddouch (2024) deeply invested in researching and implementing machine learning techniques for IDS in IoT networks. More specifically, look at ways to improve IDS detection capabilities with the help of the real-world data found in the IoT-23 dataset. A total of eighty-four points on the F1-score indicates that Random Forests, boosting models such as XGBoost, CatBoost, and Gradient Boosting, and boosting models in general yield the ideal performance. Its algorithms have a high recall-to-precision ratio, meaning they can accurately detect intrusions [25].

Ahanger, Khan and Masoodi (2023) Machine learning has also been utilized to increase the effectiveness of an IDS. Thus, a new hybrid IDS methodology is offered in this paper. The method entailed dimensional minimisation with the RF to obtain the best subset of the original data set. Intrusion detection and identification were performed through the use of an ensemble learning method. The proposed RF approach achieved a 99% accuracy rate in an experiment that compared it to other well-known state-of-the-art models on the IoTID20 dataset. Preciseness, Accuracy, Recall, and F1-score were among the performance metrics used to assess the method [26].

Table I compares and contrasts several background studies according to their methodology, dataset/environment, problem addressed, performance, and future work/limitations.

TABLE I. REVIEW OF LITERATURE ON INTRUSION DETECTION SYSTEM (IDS) FOR IOT DEVICES

Author	Methodology	Environment / Dataset	Problem Addressed	Performance	Future Work / Limitation
Mahamud, Uddin, and Sumaiya (2025)	ML-based detection approach	Bot-IoT	Detecting cyberattacks on IoT devices	99.97% accuracy, 0.0% FPR	Limited to Bot-IoT dataset; lacks validation on diverse real-world data.
Valavan and Joseph (2025)	NCF-SSA with LSTM; Hash encoding and normalization for preprocessing	UNSW-NB15	Identifying anomalies in massive Internet of Things networks	94.56% precision, 92.78% F1-score	Flexibility in actual IoT implementations
Archana et al. (2024)	CNN-IoT (Integrated IDS using CNN)	NSW-NB15	Detecting malware in IoT (e.g., DoS, Sybil attacks)	98.54% accuracy, ~0.01 type II error	Needs comparison on resource-constrained devices
Racherla et al. (2024)	Deep-IDS using LSTM with DR-FAR trade-off analysis	CIC-IDS2017	Real-time attack detection (DoS, DDoS, Brute Force, etc.)	96.8% DR at 70% threshold, 97.67% accuracy, 97.91% F1-score	DR-FAR trade-off balance; edge deployment optimization
Mahmud et al. (2024)	Ensemble of 5 ML classifiers with hyperparameter tuning and feature selection	Not specified	Improving detection using optimal feature-classifier combinations	RF: 99.39%, KNN: 94.84%	Generalization across datasets
Hafid, Ezzouhairi, and Haddouch (2024)	Boosting algorithms (XGBoost, CatBoost, Gradient Boosting), Random Forest	IOT-23	Enhancing detection in real-world IoT traffic	F1-score: 84.0	Addressing class imbalance and further model tuning
Ahanger, Khan, and Masoodi (2023)	RF for feature selection + ensemble learning for classification	IoTID20	Handling high-dimensional data and improving IDS accuracy	99% accuracy (RF method)	Further validation across newer datasets and real-time applications

III. METHODOLOGY

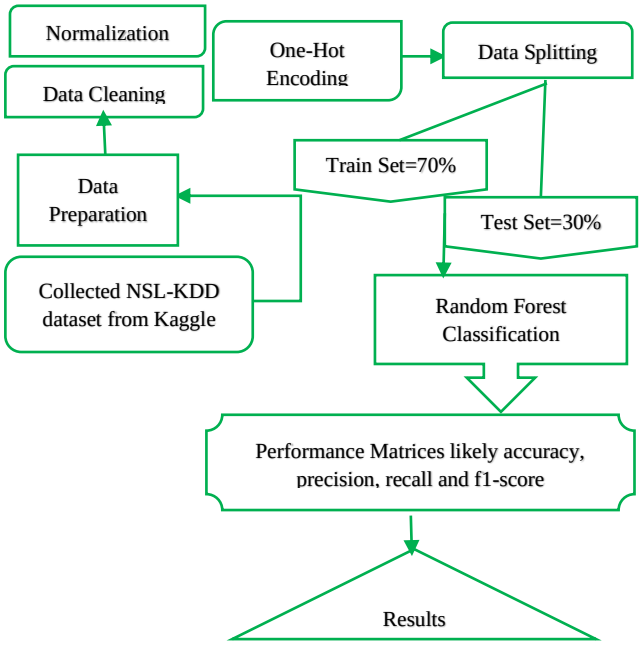

Fig. 1. Flowchart of Intrusion Detection System (IDS) for IoT Devices

Each step of the flowchart is explained in the section below:

In the given work, the methodology of the IDS of the IoT devices is proposed. The sequence includes NSL-KDD dataset retrieved on Kaggle followed by data preparation the steps of which include data cleaning, normalizing, and one-hot encoding. The data is subsequently split into two sets: training and testing. After learning to identify patterns in the training data, the RF classifier is applied to the test set with the goal of detecting intrusions. Lastly, evaluation metrics including F1-score, recall, accuracy, and precision are used to evaluate the model's performance. The results are then summarized for easy review and interpretation. The given approach helps improve perceiving cyber threats in IoT networks due to the application of strong machine learning strategies. Figure 1 shows the general machine learning-based IDS process.

A. Data Collection

Data collection refers to the act of amassing information from diverse sources in order to conduct analysis or build models. In this investigation, the NSL-KDD dataset sourced from Kaggle is employed. One enhancement over the KDD99 is the NSL-KDD dataset. The correct number of traces is established for the training and testing datasets, and KDD99's duplicate record concerns are also fixed. This version is free of any bias that could affect the ML algorithm's training data. Utilizing visualization tools allowed for a deeper exploration and comprehension of the NSL-KDD dataset. Data visualization involves creating visual representations of data, such as the picture below:

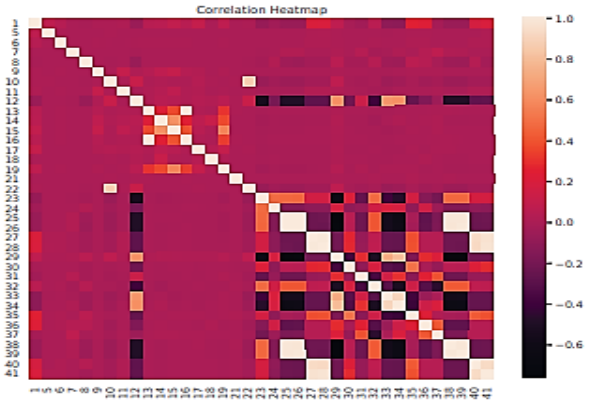

Fig. 2. Correlation Heatmap of Features in NSL-KDD Dataset

A correlation heatmap illustrating correlations among 41 features is shown in Figure 2. In terms of correlation strength, darker pinks denote very strong positive connection, blacks very strong negative correlation, and lighter pinks weak or no association at all. The white diagonal shows perfect self-

correlation. This visualization helps identify key feature relationships in the dataset.

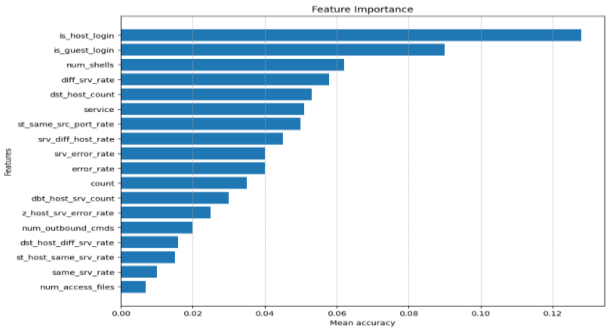

Fig. 3. Features Distribution

Figure 3 is a bar chart showing the mean accuracy of features in the intrusion detection system. Features like 'is_host_login', 'is_guest_login', and 'num_shells' have the highest impact, while others like 'num_access_files' and 'srv_diff_host_rate' contribute less. This aids in identifying key features for model optimization.

B. Data Preprocessing

Preprocessing is crucial after data acquisition. At this point, doing things like cleaning and normalizing data as well as one-hot encoding.

- **Data Cleaning:** In the dataset, duplicate values are removed, and empty values are replaced with zeros.
- **Normalization:** The dataset is normalized once all features are converted to numerical types. In this case, normalize the dataset by scaling the values inside the interval [0, 1] using the min-max regularisation approach. This normalization procedure improves the model's training efficacy and convergence speed. Equation (1) shows the normalization:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

- **One-hot Encoding:** A common way to express categorical data in various areas is with one-hot encoding [27]. This technique produces an n-dimensional vector, where n is the total number of unique feature values. There is one "1" in each vector at the spot where the encoded value should be, and all the other spots are blank. Because of this, one-hot encoding reduces a feature with n potential values to n binary features.

C. Data Splitting

Training and testing datasets make up the bulk of the dataset. The data set used for training comprised 70% of the entire dataset. The remaining 30% of the data was comprised of the test set.

D. Proposed Random Forest (RF) Model

One of the best machine learning algorithms, Random Forest can handle a wide variety of datasets with ease and precision [28]. Using the bagging methodology, which involves training trees on bootstrap subsets of data, it integrates predictions from various decision trees as an ensemble method. Because of its quickness and capability to deal with incomplete or missing data, RF finds widespread use in ML [29]. When utilizing the RF to predict the dataset's class, some decision trees may provide accurate results while others do not. But when you add all the trees together, and get accurate predictions. To find out how important a characteristic f_iHen using Random Forest, average its weight across all trees [30]. After obtaining the total feature relevance from all trees using Equation. (2), divide it by the number of trees:

$$RFI(f_i) = \frac{1}{T_t}\sum_t \sum_k \frac{T_t}{T} \Delta I_{f_i} \quad (2)$$

Here, T_t stands for the total number of trees, N_kOr the number of samples that pass through node k, t for the total number of samples in the dataset [31], and I for the Gini index value, which is found using Equation (3).

$$Gini\ Index(I) = 1 - \sum_{i=1}^{n}(P_i)^2 = 1 - [(P_p)^2 + (P_n)^2] \quad (3)$$

The positive class is denoted by P_p and the negative class by P_nIn this context.

1.1 Performance matrix

An improvement in the IDS performance in smart cyber-physical systems can be achieved by picking the most important elements and removing the unnecessary or redundant ones [32][33]. To measure how well intrusion detection systems (IDS) work in preventing and detecting security breaches and incursions into networks and systems, developers created metrics specifically for this purpose. Take a look at these popular IDS evaluation metrics:

- **True Positives (TP):** A total of all the breaches that the system has identified.
- **False Positives (FP):** Countless lawful activities were falsely labelled as invasions.
- **True Negatives (TN):** The number of common tasks that were correctly identified as common.
- **False Negatives (FN):** All valid intrusions that went undetected by the IDS add up to this sum.

These values are computed for each class individually during the testing phase, and they form the basis for calculating the evaluation metrics. These numbers are used to generate the generic formulae for F1-score, recall, precision, and accuracy.

Accuracy: The proportion of total correct predictions (both attacks and normal activity) made by the IDS out of all predictions. It shows how often the IDS makes the correct decision overall. The accuracy is calculated for the overall model using Equation (4):

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{(\text{TP} + \text{TN} + \text{FP} + \text{FN})} \quad (4)$$

Precision: The proportion of attacks that were accurate identifications relative to all instances that the IDS classified as attacks. It shows how trustworthy the IDS is when it sounds the alarm. The calculation of the precision is done using Equation (5):

$$\text{Precision} = \frac{\text{TP}}{(\text{TP+FP})} \quad (5)$$

Recall: The proportion of real attacks that the IDS successfully identifies. It shows how well the intrusion detection system can identify breaches. In Equation (6), the recall is mathematically represented:

$$\text{Recall} = \frac{\text{TP}}{(\text{TP+FN})} \quad (6)$$

F1-Score: A balanced measure that strikes a harmonious middle ground between Precision and Recall. It proves beneficial when the normal instances and attack instances are not in a balanced ratio. It is mathematically formulated as follows in Equation (7):

$$\text{F}_1 - \text{Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \quad (7)$$

IV. Results and Discussion

The configuration of the system in this research is Windows Server 2019 operating system with an Intel(R) Xeon(R) Silver 4214 CPU. The system has a robust computing perspective having the NVIDIA RTX 3090 GPU and a RAM 128 GB of. Python programming language version 3.7 is used in the development of the models and to perform analysis. Table II displays the outcomes of the RF evaluation on an IoT device IDS. The model delivers outstanding results across all key metrics, demonstrating its capacity to accurately identify both benign and harmful traffic in IoT network communication (accuracy, precision, recall, and F-1 score).

TABLE II. Evaluation of RF on Intrusion Detection System (IDS) for IoT Devices

Metrics	RF
Accuracy	99.9
Precision	99.9
Recall	99.9
F1-Score	99.9

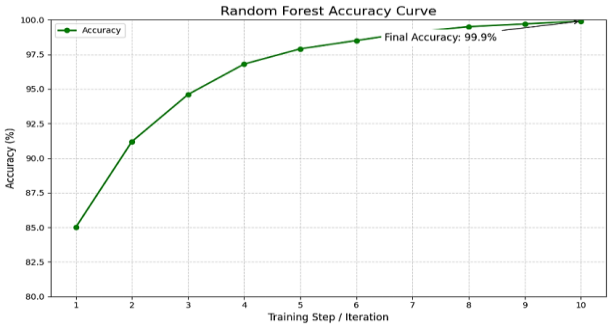

Fig. 4. The Accuracy of the RF Model

Figure 4 shows the accuracy of RF classifier over 10 training runs. The graph indicates a steadfast trend increasing accuracy, with initial accuracy being gauged at about 85%, until the whole thing ended up at an ultimate accuracy of 99.9%. This gradual increase in performance represents a successful learning activity of the model given the data during each iteration and a 100% classification accuracy is noted.

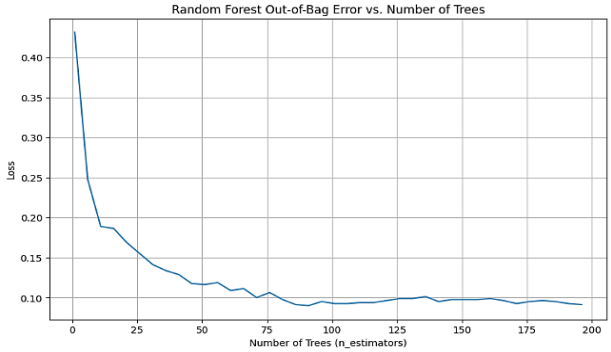

Fig. 5. The Loss of the RF Model

Figure 5 displays the Loss error pattern to show an exponentially diminishing trend with tree addition, and thereafter, it becomes stable after approximately 100 rounds. This shows better overall generalization at first, but with lesser and lesser gains thereafter. The curve attaining a steady value of 0.10 indicates that the model is of high accuracy and effective performance with little overfitting.

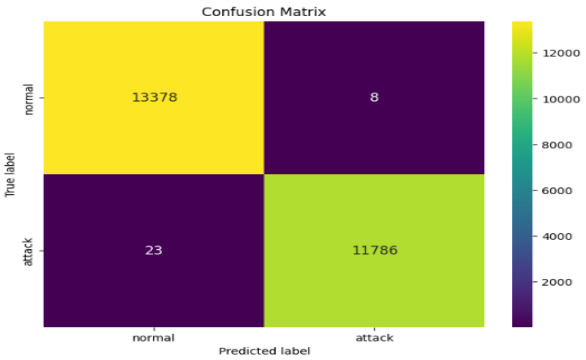

Fig. 6. Confusion Matrix of RF

Figure 6 illustrates a two-class confusion matrix, normal and attack, to assess a classification model. The model predicted the normal and attack instances accordingly, 13,370 and 11,786, respectively, with a minimum of false positives, 8, and false negatives, 23. That shows a high level of model accuracy and good performance characterized by strong diagonal dominance.

A. *Comparative Analysis*

Table III presents the comparative analysis of ML and DL models, which have been utilized in relation to the Intrusion Detection Systems (meant to be used on IoT devices). The models used in comparison are Conv1d and the following ML models DT, SVM, and RF. The highest accuracy is recorded by the RF model, and it outperforms all the other models. Although SVM and DT are satisfying in their performance, Conv1d model demonstrates the lowest accuracy, which is a sign of poor effectiveness in such a situation. Generally, the table shows more effectiveness of RF in the correct identification of intrusions in IoT networks.

TABLE III. Comparative Analysis of ML and DL on Intrusion Detection System (IDS) for IoT Devices

Models	Accuracy
Conv1d [34]	79.8
DT [35]	88.5
SVM [36]	90.7
RF	99.9

The Random Forest (RF) model would greatly enhance the performance of IDS in an IoT environment. It would adopt an ensemble-based system architecture and make classification more stable and resistant to overfitting. Because it takes into account the variety and volatility of IoT network traffic, the RF model can effectively identify both known and new attacks by building and aggregating the outputs of numerous decision trees. More IoT devices and communication protocols can be accommodated by its ability to process large amounts of data and identify intricate patterns.

V. Conclusion and Future Work

Intrusion detection is crucial since the proliferation of IoT devices has raised serious security risks. In response, provide an IDS for IoT scenarios that utilizes the NSL-KDD dataset

and is based on ML. After cleaning, normalizing, and one-hot encoding, the data were ready for intrusion detection. Next employed an RF classifier. The RF model had remarkable results in the experiments, with an F1-score of 99.9% and a recall, precision, and accuracy of 99.9%. These results demonstrate how RF's ensemble learning is strong, guaranteeing steady categorization and trustworthy detection of harmful actions in diverse IoT network traffic. In addition, the comparative analysis demonstrated that the RF model outperformed the conventional ML and DL approaches, making it an excellent choice for intrusion detection in IoT environments with limited resources. Despite these promising results, further research is necessary to enhance adaptability against evolving attack patterns.

Future work could focus on integrating bio-inspired AI, hybrid ensemble approaches, and advanced learning architectures. Additionally, optimization-driven feature selection and incremental learning may enhance scalability and reduce costs in large-scale IoT deployments. Incorporating federated learning and edge-based IDS frameworks will support privacy preservation and real-time threat detection in distributed networks, ultimately improving resilience and efficiency in next-generation IoT ecosystems.

REFERENCES

[1] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity," *Appl. Sci.*, vol. 13, no. 13, p. 7507, Jun. 2023, doi: 10.3390/app13137507.

[2] D. D. Rao, A. A. Waoo, M. P. Singh, P. K. Pareek, S. Kamal, and S. V. Pandit, "Strategizing IoT Network Layer Security Through Advanced Intrusion Detection Systems and AI-Driven Threat Analysis," *J. Intell. Syst. Internet Things*, vol. 24, no. 2, pp. 195–207, 2024, doi: 10.54216/JISIoT.120215.

[3] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, 2025, doi: 10.38124/ijsrmt.v4i5.542.

[4] R. Patel, "Optimizing Communication Protocols in Industrial IoT Edge Networks: A Review of State-of-the-Art Techniques," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 19, pp. 503–514, May 2023, doi: 10.48175/IJARSCT-11979B.

[5] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, 2025.

[6] V. Shah, "Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[7] D. Patel, "Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity," *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[8] B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, "IoT Intrusion Detection System Based on Machine Learning," *Electronics*, vol. 12, no. 20, 2023, doi: 10.3390/electronics12204289.

[9] M. M. Rahman, S. Al Shakil, and M. R. Mustakim, "A survey on intrusion detection systems in IoT networks," *Cyber Secur. Appl.*, vol. 3, p. 100082, 2025, doi: https://doi.org/10.1016/j.csa.2024.100082.

[10] H. P. C. Kapadia and K. C. Chitoor, "Quantum Computing Threats to Web Encryption in Banking," *Int. J. Nov. Trends Innov.*, vol. 2, no. 12, 2024.

[11] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, 2023, doi: 10.14741/ijcet/v.13.6.11.

[12] G. Maddali, "Enhancing Database Architectures with Artificial Intelligence (AI)," *Int. J. Sci. Res. Sci. Technol.*, vol. 12, no. 3, pp. 296–308, May 2025, doi: 10.32628/IJSRST2512331.

[13] S. Narang and V. Gopi Kolla, "Next-Generation Cloud Security: A Review of the Constraints and Strategies in Serverless Computing," *Int. J. Res. Anal. Rev.*, vol. 12, no. 3, 2025, doi: 10.56975/ijrar.v12i3.319048.

[14] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.

[15] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[16] S. Gajula, "A Review of Anomaly Identification in Finance Frauds using Machine Learning System," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, Jun. 2023, doi: 10.14741/ijcet/v.13.6.9.

[17] D. D. Rao, V. Roy, K. Bhopte, K. Mukilan, P. K. Shukla, and R. V Patil, "Fuzzy-Based Cluster Head Management with Artificial Flora Optimization for Energy-Efficient and Secure Routing in Fog-Enabled Wireless Sensor Networks," in *2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP)*, IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/IHCSP63227.2024.10960064.

[18] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[19] V. Shah, "Traffic Intelligence In Iot And Cloud Networks: Tools For Monitoring, Security, And Optimization," *Int. J. Recent Technol. Sci. Manag.*, vol. 9, no. 5, 2024.

[20] N. Mahamud, M. J. Uddin, and U. Sumaiya, "Enhancing Network Security using Machine Learning for Automated Anomaly-based Intrusion Detection Systems for IoT Environment," in *2025 International Research Conference on Smart Computing and Systems Engineering (SCSE)*, 2025, pp. 1–6. doi: 10.1109/SCSE65633.2025.11031050.

[21] W. T. Valavan and N. Joseph, "Intrusion Detection System for Anomaly in IoT Using Nonlinear Convergence Factor Using Salp Swarm Algorithm," in *2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 2025, pp. 1–5. doi: 10.1109/ICICACS65178.2025.10967983.

[22] B. Archana, K. S. Raju, R. Tiwari, and M. V. Prasad, "Assessment of IOT Devices with Collaborative Intrusion Detection System Using Deep Learning Techniques," in *2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI)*, 2024, pp. 1–4. doi: 10.1109/ICSCAI61790.2024.10866020.

[23] S. Racherla, P. Sripathi, N. Faruqui, M. Alamgir Kabir, M. Whaiduzzaman, and S. Aziz Shah, "Deep-IDS: A Real-Time Intrusion Detector for IoT Nodes Using Deep Learning," *IEEE Access*, vol. 12, pp. 63584–63597, 2024, doi: 10.1109/ACCESS.2024.3396461.

[24] M. Z. Mahmud, S. Islam, S. R. Alve, and A. Jubayer Pial, "Optimized IoT Intrusion Detection using Machine Learning Technique," in *2024 IEEE 3rd International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*, 2024, pp. 167–172. doi: 10.1109/RAAICON64172.2024.10928532.

[25] B. Hafid, A. Ezzouhairi, and K. Haddouch, "Strengthening Security in the Internet of Things (IoT): Integrated Approach of Intrusion Detection Systems (IDS) and Edge Computing," in *2024 3rd International Conference on Embedded Systems and Artificial Intelligence (ESAI)*, 2024, pp. 1–9. doi: 10.1109/ESAI62891.2024.10913549.

[26] A. S. Ahanger, S. M. Khan, and F. S. Masoodi, "Intrusion Detection System for IoT Environment using Ensemble Approaches," in *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2023, pp. 935–938.

[27] L. D. Manocchio, S. Layeghy, M. Gallagher, and M. Portmann, "An empirical evaluation of preprocessing methods for machine learning based network intrusion detection systems," *Eng. Appl. Artif. Intell.*, vol. 158, p. 111289, 2025, doi:

https://doi.org/10.1016/j.engappai.2025.111289.

[28] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, "An Ensemble-Based Multiclass Classifier for Intrusion Detection Using Internet of Things," *Comput. Intell. Neurosci.*, 2022, doi: 10.1155/2022/1668676.

[29] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[30] H. Kali, "The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security.," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023, doi: 10.10206/IJRTSM.2025803096.

[31] M. Samantaray, R. C. Barik, and A. K. Biswal, "A comparative assessment of machine learning algorithms in the IoT-based network intrusion detection systems," *Decis. Anal. J.*, vol. 11, Jun. 2024, doi: 10.1016/j.dajour.2024.100478.

[32] K. Harahsheh, R. Al-Naimat, and C.-H. Chen, "Using Feature Selection Enhancement to Evaluate Attack Detection in the Internet of Things Environment," *Electronics*, vol. 13, no. 9, 2024, doi: 10.3390/electronics13091678.

[33] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, 2025.

[34] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A. Qureshi, and H. Larijani, "Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes," *Futur. Internet*, vol. 16, no. 6, p. 200, Jun. 2024, doi: 10.3390/fi16060200.

[35] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)," *Lect. Notes Networks Syst.*, vol. 180, pp. 73–84, 2021, doi: 10.1007/978-3-030-64758-2_6.

[36] P. M. Vijayan and S. Sundar, "An automated system of intrusion detection by IoT-aided MQTT using improved heuristic-aided autoencoder and LSTM-based Deep Belief Network," *PLoS One*, vol. 18, no. 10, Oct. 2023, doi: 10.1371/journal.pone.0291872.

