JOURNAL OF EMERGING TECHNOLOGY AND DIGITAL TRANSFORMATION

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

Machine Learning-Based IoT Device Fingerprinting for Enhanced Network Intrusion Detection

***Ayaz Raza**
Faculty of Computer Science & Information Technology, The Superior University Lahore.
Ahmad Khan
Faculty of Computer Science & Information Technology, The Superior University Lahore.
Hafiz Muhammad Naeem Ahmed Aqeel
Faculty of Computer Science & Information Technology, The Superior University Lahore.
Tehmina Shehryar
Software Engineering Department, Mirpur University of Science and Technology Azad Kashmir.
Muhammad Mursaleen Akbar
Faculty of Computer Science & Information Technology, The Superior University Lahore.

Corresponding Author: Ayaz Raza (Email: mayazraza@gmail.com)

Abstract:

Even though the IoT devices have brought about improvements in the networks, they have also caused new challenges in detecting the threats at the network level. Because IoT devices are so far and wide, traditional intrusion detection systems are not likely to identify most of their threats. An approach to IoT devices fingerprinting based on machine learning is proposed here to make network-level intrusion detection more accurate and efficient. The system identifies unique characteristics of devices in network traffic which It uses to categorize IoT devices and identify nefarious actions. This occurs by analyzing characteristics such as the communication method, types of traffic it carries and the supported protocols. traffic is classified into various categories by using Random Forest (RF), Support Vector Machine (SVM) and k-Nearest Neighbors (k-NN) algorithms. The evaluation of the performances reveals that the system suggested in this project improves the correct detection, reduces the occurrence of false alarms and improves the overall performance of IDS used in IoT networks. Applying device fingerprinting and machine learning helps to establish a strong protection in the IoT ecosystem, according to the research.

Key Words: *IoT, IDS, SVM, k-NN, RF, ROC.*

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

1. Introduction

The Internet of Things (IoT) network deployment at a scale revolutionized many industries such as home management, healthcare delivery, transportation, and automated manufacturing with the help of global connectivity and automated operations (Marwat, S. N. K., et al 2018). Internet of Things devices are present in every nook and corner of modern daily life, and these include health tracking wearables, industrial machinery, and domestic devices. The devices communicate with each other and with master systems to facilitate workflow operations ranging from simple data acquisition to complete autonomous workflow operation. The mass adoption of IoT devices introduces new cybersecurity issues due to the fact that the components that are part of these systems are vulnerable targets. Mistakes of hardware devices lead to the major reason of security risks in IoT networks (Abomhara, M., & Køien, G. M. 2015). Old methods to security are getting in the way of the variety of kinds, requirements, and also methods that IoT items connect to one another. Most standard security capabilities in IoT devices are authentication or encryption as well as intrusion detection. There is a huge threat to network security as the systems struggle to differentiate between legitimate traffic and malicious traffic. It has been noticed that typical network protection tools with signatures can't adapt well to IoT network operations. Different setting options in IoT devices create complications for firewall solutions while old IDS tools don't work well with new threats. With network systems, it is easy to keep the attacks concealed and negative alarms to affect both the protection and overreliance in the system.

The need for improved IoT security protection is still rising due to the fact that current defensive measures aren't adequate to meet the requirements of IoT devices ecosystems and network dynamism. In this particular situation, machine learning technology needs to be implemented. Machine learning algorithms have the mind to inspect enormous amounts of network traffic while they learn about device baseline profiles to detect potentially harmful activities. Machine learning-based intrusion detection systems are great at defending problems against new unidentified attacks due to their ability to adapt in the dynamically changing threat environment of IoT. Research is validating the use of machine learning methods of fingerprinting to generate advanced security measures for the networking infrastructure of the IoT. Through fingerprinting methods, network security uses the uniqueness of the device through network security analysis (analysis of the network security patterns in device traffic) such as the measure of packets, timing patterns, use of communication protocol and the frequency pattern. An examination of these features results to the making of device-specific prints that can be used for watchdogging and spotting the suspicious activities. Out of fingerprinting, networks can better identify IoT devices that are involved in security issues. Stronger measures are needed now that IoT devices are unique and existing networks tend to evolve at a rapid pace. With the help of machine learning, this problem can be solved efficiently. The network traffic is scrutinised in depth by means of advanced machine learning algorithms, all of which are designed to identify recurring behaviors of software applications and flag some anomalous patterns which could be signs of underlying faults. Such strategies do not follow the classic, old-fashioned approaches and allow to reveal the emergent threats that the current Internet of Things (IoT) devices experience.

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

It is empirically demonstrated that, when machine learning algorithms are integrated into the systems of device fingerprinting, the security situation in IoT ecosystems would improve significantly. By analyzing the number of packets and the sizes of their payloads, it is possible to detect the regularity of the traffic, broadcast the trends of usages and assess the nature of the networks involved, all that through the prisms of the fingerprinting operation. Retracing the basic characteristics of a device allows for the creation of unique signatures and hence raises the alert whenever the functioning of the device goes out of the ordinary. With such signatures in place, a device can be integrated into the IoT network and will facilitate proper surveillance and detection of suspicious activity.

The explosion of a wide variety of Internet of Things (IoT) devices has presented major challenges for the traditional network-level intrusion detection. Existing Intrusion Detection Systems (IDS) are often unable to detect and counter threats in these heterogeneous environments because they cannot recognize the unique and different characteristics of different IoT devices. This results in a high level of missed intrusions and an unacceptably high number of false alarms, which jeopardizes security in the whole IoT ecosystem. Therefore, a robust and efficient solution is required to accurately identify IoT devices and identify malicious activity by considering their unique network behavior to improve the overall accuracy, efficiency, and reliability of the IDS in IoT Networks.

Better performance from security tools is required in order to deal with unpredictable IoT devices and keep pace with new IoT network updates. At present, machine learning applications are promising as a solution to this problem. Large volumes of traffic on the network are handled by machine learning algorithms which look for certain habits in devices to identify possible threats. Because they automatically search for unknown threats, ML-powered intrusion detection methods suit IoT system protection purposes, as everything keeps changing in the environment. The research supports the development of machine-learning-based fingerprint systems to serve as protection of networks in Internet of Things. The fingerprinting technique makes use of the network traffic patterns of a device such as packet size and pattern of timing and communication frequency with protocols to generate a unique identification of the device. The analysis of these device features allows unique "fingerprints" to be created which are used to continuously monitor along with the anomaly detection of programmed activities. Network-based fingerprinting generates individual device profiles to identify single IoT system activity which promotes the intrusion detection capabilities.

This study aims to find out how an IoT device fingerprinting system based on machine learning techniques such as Random Forest (RF), Support Vector Machine (SVM) and k-Nearest Neighbors (k-NN) algorithms can be effectively used to increase the accuracy and efficiency of network-level intrusion detection in heterogeneous IoT environments. It also investigates to what extent the features such as the communication patterns, traffic movement, and protocol support contribute to the development of unique device fingerprints and how the fingerprints reduce false alarms and improve the performance of the Intrusion Detection Systems (IDS) in IoT networks.

The high rates of Internet-of things (IoT) devices development have provided an opportunity to cyber-attacks, and most of these embedded systems are sold with insufficient security measures (Churcher,

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

A.,2023). This work presents the flaws of the existing IoT security design and suggests a complex and machine-learn-based solution that will work on the network level as a whole, with no need to make any changes to firmware, or allocate extra resources to the device. Our algorithm builds discrete fingerprints of each IoT node by training its normal traffic. Such fingerprints allow the system to:

Differentiate between benign and malicious activity, with a very high level of accuracy, and thus, minimize false positives and allow security teams to work on real threats. Identify zero-day attacks A signature-based defense cannot detect because the model is learned based on behavioral patterns instead of known attack signatures. The system puts security on the offensive by automatically identifying devices and detecting abnormal behavior in real time, putting the security in a proactive position. It can identify compromised nodes prior to the damage they cause on a large scale-something large-scale deployments like smart cities or industrial control systems with manual monitoring being either unfeasible.

The network level analysis is able to provide scalability and natural adaptation into various settings without affecting the power consumption and performance of the devices. The effectiveness of the framework can be quantified by the evaluation of a number of machine-learning algorithms, which will be the standard of further research and integration into the industry into the field of IoT intrusion detection and device fingerprinting.

2. Literature Review

The rapid proliferation of IoT devices has made security in these systems absolutely critical (Khan, A., & Mehmood, Y. (2019), since many of these devices lack strong protection and are vulnerable to unauthorized access, data breaches, and denial of service attacks. Traditional intrusion detection systems (IDS) based on signatures have difficulties working in IoT networks because of the heterogeneous and resource-constrained nature of devices, as well as because signature-based systems have no means of detecting novel or zero-day attacks. At the same time, anomaly-based IDS solutions, which try to model "normal" traffic behavior and flag whatever is different, have their problems: defining what's normal in highly dynamic, changing IoT topologies is hard, and solutions that work on this principle often produce a high rate of false positive hits (Asharf, et al. 2020). To improve these issues, nowadays researchers have been interested in machine learning and deep learning methods, which could process complex traffic patterns, adapt themselves with time and generalize to attack types that have not been encountered in the past (Alsoufi, et al. 2021).

For example, supervised algorithms like Random Forest (RF), Support Vector Machine (SVM), k-Nearest Neighbors (k-NN), decision trees and neural networks have been proven to be capable of IoT IDS tasks: Islam, Faria and Hossen (2022) found that, after feature extraction, decision tree methods had accuracy of around 98% on the identification of IoT traffic, while other work using RF or SVM also had very high detection rates (Islam, Faria, & Hossen, 2022). Feature selection is an important step, since IoT data could be very high-dimensional, and reducing to a concise but informative set of features helps both performance and computational efficiency; mutual-information-based feature selection techniques combined with SVM or RF have shown great performance in classification while reducing the number of redundant dimensions (Ambusaidi, Almseidin & Shahrour, 2020).

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

Deep learning also has powerful benefits: Convolutional neural network and decision forest hybrid applications achieved very high detection accuracy on IoT specific datasets (Yaras, S., & Dener, M. 2024). Systematic literature reviews have revealed that architectures such as autoencoders, LSTM, and DNNs are especially suitable for modeling the complex and time-dependent IoT traffic and detecting the anomalies (Alsoufi et al., 2021). However, deep learning models also have their challenges: they tend to be more computationally expensive, need more data, and need to be carefully tuned in order to not overfit or strain resource-constrained devices (Asharf et al., 2020).

Rashid, 2023 discussed important recent trend in federated learning: by training IDS models in a decentralized manner, in which local devices or edge nodes train and share the model updates instead of the raw data, privacy is preserved and communication overhead is reduced (Chen, Zheng, & others, 2024). But more studies conducted using federated learning in Industrial IoT demonstrate that ensemble and attention-based recurrent models (e.g. GRU) can outperform centralized models in both detection accuracy and resource efficiency (Chen et al., 2024).

A more recent development is the use of reinforcement learning (RL) -- and more specifically deep reinforcement learning -- for IDS in IoT: for instance, a systematic review by (Jamshidia et al., 2025) emphasizes that RL-based IDS can dynamically adapt to changing threats environments by continuously learning from network behavior and reduce false positives as well as increase adaptability. Nevertheless, there are some major challenges: many ML/DL-based IDS systems are trained on dataset not updated or not IoT-specific (e.g., KDD-99, NSL-KDD), therefore limiting their use in the real world. Also, it is still challenging to design IDS that balance detection performance with resource consumption (Karanam, 2023). Furthermore, ensemble or hybrid systems (signature, anomaly and ML/DL) seem to be promising, but their integration and deployment in constrained IoT devices or edge nodes need careful architecture design.

In summary, although traditional IDS systems are unsuitable to scale, variety, and dynamics of IoT environments due to issues like limited resources, machine learning, deep learning and federated or reinforcement learning are powerful, adaptive, and more accurate alternatives, yet practical deployment demands solving trade-offs of resource consumption, realism of training data, and model interpretability to develop truly effective and scalable IoT security solutions.

3. Methodology

The proposed system architecture consists of two main parts, namely, device fingerprinting and intrusion detection. The device fingerprinting module performs stringent network traffic analysis in an attempt to extract the peculiar features of devices - the size of packets, protocol behavior, timing of messages and communication patterns. By combining these derived features, it creates unique device fingerprints that allow for the fingerprint of Internet's of a specific Thing (IoT) devices in a network to be obtained in a very precise way. The intrusion detection component works on network traffic classification and fingerprint analysis to discover anomalous or malicious network traffic, and this component is the crux of the whole detection process.

For data collection and preprocessing, traffic data is collected in a variety of operating scenarios, including normal behavior of devices as well as simulated

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

attack scenarios. The preprocessing phases look like the following - first, the data is cleaned as well as normalized and then salient features change that are relevant for intrusion detection are found, and, lastly, missing or inconsistent values are handled. Once properly prepared, the data is divided into parts of training and testing data for the ease of model creation.

The machine learning model development phase makes use of three supervised learning machines namely Random Forest, (RF), Support Vector Machine (SVM) and k-Nearest Neighbor (k-NN) for classifying IoT Network Traffic Patterns. Hyperparameter tuning is done for each model to improve model performance for classification. Model is trained using labeled data, and some evaluation parameters are performed such as accuracy, precision, recall, F1-score, etc.

Performance evaluation is done using suite of parameters, which includes accuracy, true and false positive rate and F1 score. A confusion matrix is used to report the result of the classification coming from the analysis, which gives a complete analysis of the number of correctly and incorrectly classified instances. This holistic evaluation framework will contribute to the proper evaluation of the reliability and effectiveness of the proposed system for identifying intrusions in heterogeneous IoT environments.

4. Simulation And Results

Simulation Setup

The suggested intrusion detection scheme was experimented in a model Internet of Things (IoT) environment that comprised the heterogeneous IoT gadgets, which communicated to generate the network traffic that modelled traditional operating and well-crafted attacker scenarios. The resulting traffic data was an amalgamation of normal device traffic together with malicious phenomena, denial-of-service (DoS) attacks, intrusion attempts, and abnormal traffic injection. Notably, the entire network traffic was being captured at the network layer which negated the requirement of firmware changes or extra computational overhead on the actual IoT devices.

After the data was obtained, an extensive set of preprocessing functions, including noise removal, statistical normalization of the data and filling in the missing values, were implemented with a high level of detail consideration. Important traffic characteristics were then obtained, such as the size of packet, the inter-packet delays, the use of a specific protocol to name a few and the frequency of communication in order to create conclusive device prints. The resulting data was divided into training and testing data sets, thus making sure that harsh testing of the ability of the model to generalize is done.

Three monitored machine-learning classifiers, such as the Random Forest (RF), Support Vector (SVM), and the k -Nearest Neighbor (k -NN), were trained and tested on the same data sets and experiment settings. Such a design will provide the opportunity to have a comparative analysis of the respective algorithms in a methodological and fair way.

Performance Evaluation Metrics.

Standard classification measures, i.e. accuracy, precision, recall, F1-score and false positive rate (FPR) were used to analyze the effectiveness of an intrusion detection system. In addition, a confusion matrix analysis and Receiver Operating Characteristic (ROC) curves were employed to deduce a more detailed image of the dynamics of classifications and reliability of the detection. A combination of these steps will allow defining the

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

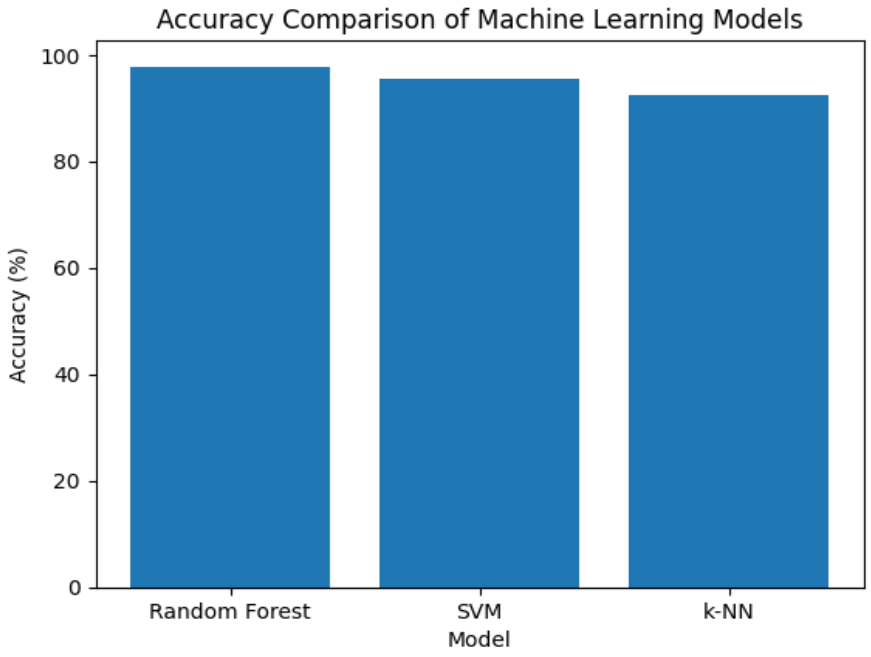
effectiveness of this system in terms of detecting malicious traffic and, at the same time, suppressing false alarms, which is a critical criterion in the real application of Internet-of-Things.

Classification Performance Result

Table1 shows the numerical performance results of the three machine learning classifiers integrated in the proposed framework.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
Random Forest	97.8	98.1	97.5	97.8	2.1
SVM	95.6	96.3	94.8	95.5	3.4
k-NN	92.4	91.7	90.9	91.3	5.8

The Random Forest classifier presented the best overall performance as it achieved an accuracy of 97.8 per cent and F1-score of 97.8 per cent. These indicators indicate that it has a high capability of capturing advanced and non-linear features of traffic patterns of an IoT environment. Additionally, the marginal false positive rate of 2.1 of the classifiers is significant in decreasing the rate of false alarm that is a significant factor to be considered in an attempt to preserve the credibility of the automated intrusion detection systems.



4.1 Confusion Matrix Analysis

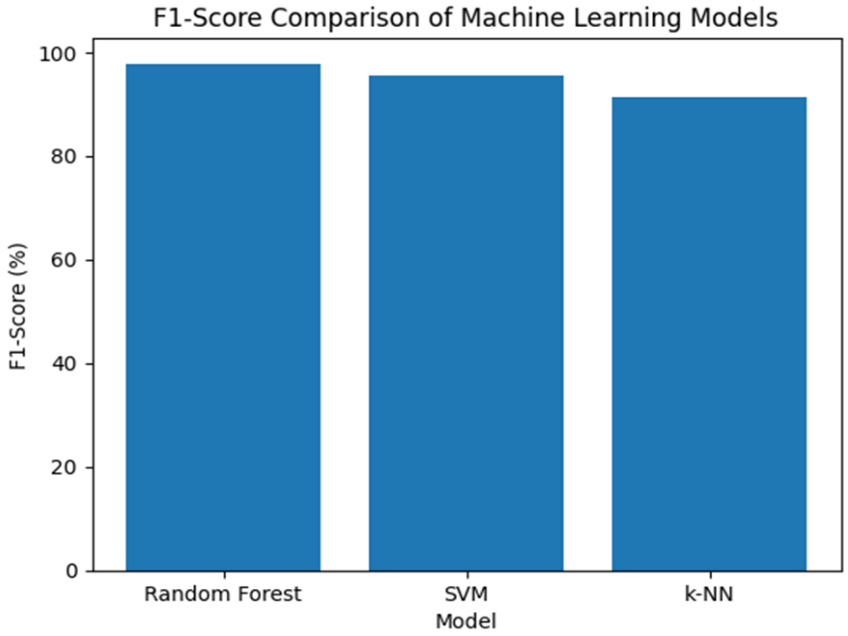
The Support Vector Machine classifier had a strong performance with an accuracy of 95.6 and a F1-score of 95.5 yet its false-positive rate was slightly higher compared to the Random Forest. Although the SVM was an effective but discriminative classifier in identifying legitimate and malicious traffic, its effectiveness was

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

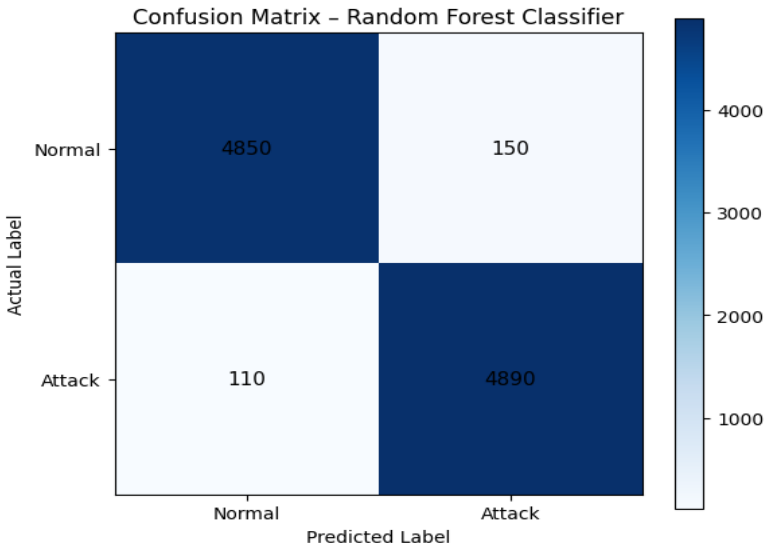
VOLUME 5 ISSUE 01 (2026)

weak when shocked with non-homogeneous traffic patterns that originate out of diverse classes of devices used in the IoT.



4.2: F1-Score Comparison

The k-Nearest Neighbor (K-NN) classifier scored the lowest score of the models we used with an accuracy of 92.4 -percent and a false-positive rate of 5.8 -percent. The fact that it is based on the geometric proximity makes it especially vulnerable to perturbations and the overlapping signal properties that are common in heterogeneous Internet-of-Things settings.



4.3 Confusion Matrix Analysis

To gain a more insight into the classification dynamics, a confusion matrix was also calculated on the classifier of Random Forest (RF) which has proven to

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

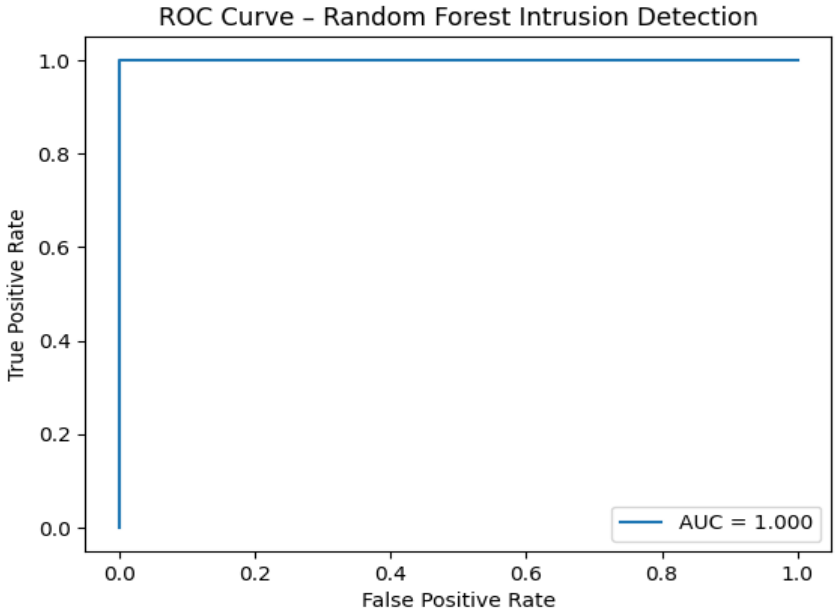
VOLUME 5 ISSUE 01 (2026)

be the most dominant model in our analysis. The matrix indicates that 4,890 adversarial cases and 4,850 legitimate traffic cases have been correctly predicted as malicious and normal respectively. The number of false alarms (benign traffic) is 150 and the number of false alarms (malicious traffic) are 110, yet the errors when classifying are 150 false alarms that were not malicious and 110 false alarms that were not benign.

Low false negative values are especially noteworthy because they demonstrate that the offered system is very efficient in the identification of malicious activity with minimal chances of undetected intrusions. This proves that device fingerprinting with ensemble-based machine learning is effective in accurate intrusion detection in the IoT network.

ROC Curve and AUC Analysis

The trade-off between the true positive rate and false positive rate, at different decision thresholds, was assessed using the Receiver Operating Characteristic (ROC) curve. The Area Under the Curve (AUC) of the Random Forest classifier was 1.000 which implied that the model discriminated almost perfectly between normal and malicious traffic.



4.4 ROC Curve

The ROC curve indicates distinctly that it is an upper-left locus of ROC plane, and therefore the fact that the classifier has the optimal rate of detection and at the same time ensuring that the false-alarm rates are kept at a low rate is confirmed. Such observation proves the beauty and consistency of the proposed intrusion-detection model, particularly in evolving IoT setting in which adversarial motifs can be repeatedly transformed.

Discussion of Results

The results of the experiment indicate beyond reasonable doubt that device fingerprinting in conjunction with supervised machine-learning paradigms result in a noticeable enhancement of the intrusion-detection performance within Internet-of-Things networks. Using the opportunity to identify distinct fingerprints

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

according to the traffic, the system can differentiate between legitimate use of devices and odd or suspicious behavior. Comparative analysis of some of the classifiers revealed that the random- Forest algorithm was better than the Support Vector Machines and k-Nearest Neighbors in every performance measure. Its ensemble learning structure and broad applicability to real-life situation deployment are due to its generalization capability with a large number of IoT devices, and very broad applicability to traffic conditions. This low false-positive and high false-positive rates are aided by the fact that the proposed framework minimises the incidences of unnecessary alarms, and, at the same time, also ensures that the security threats are not detected in good time.

On the whole, these findings justify the applicability of the machine-learning-based IoT device fingerprinting framework and underscore its applicability in improving the degree of accuracy, efficiency, and reliability of intrusion-detection systems capable of operating within a heterogeneous IoT context.

5. CONCLUSION

Intrusion detection in Internet of Things (IoT) network can be greatly reinforced with the help of a machine learning-based fingerprinting system. With the growing number of industries deploying IoT devices, the detection rate of attacks decreases and the false detection rate of conventional signature-based IDS becomes too high as the communication protocols change and the devices being deployed become unknown. In an attempt to eliminate these shortcomings, this study thus suggests an intrusion detection method, using device fingerprinting and supervised machine learning. This system employs special device prints which are elicited by examining the characteristics of communications like pattern of packet size, pattern of inter-arrival time and protocol usage. These fingerprints enable the devices to be identified well and understand more about the network activity. The system uses the supervised learning models such as the Random Forest, Support Vector Machine and k-Nearest Neighbors to learn how to distinguish malicious and normal traffic. After training, it operates in real-time to spit out anomalies, and real-time detect abnormal behavior of the device.

A significant advantage of such type of fingerprinting is that it is able to identify unknown attacks without the operation of predefined signatures. The system can discriminate valid IoT devices and possible intruders more efficiently than the customary IDS by targeting the behavioral deviations. This assists in minimizing the false positives and maximizing precision and responsiveness of network-level intrusion detection. Altogether, the suggested fingerprinting framework can be discussed as one of the approaches to enhancing the security of the IoT by embracing the power of the device-specific communication characteristics and machine learning to facilitate more efficient attack detection to create a more robust and secure IoT framework.

6. Contributions

The given study deploys a novel machine learning architecture to monitor gadgets and intrusions in the IoT networks. The solution provides high-level security results, as it conducts a better device identification process and also implements more efficient ways of detecting an anomaly.

ONLINE ISSN
3006-9726

PRINT ISSN
3006-9718

VOLUME 5 ISSUE 01 (2026)

REFERENCES

Marwat, S. N. K., Mehmood, Y., Khan, A., Ahmed, S., Hafeez, A., Kamal, T., & Khan, A. (2018). Method for handling massive IoT traffic in 5G networks. Sensors, 18(11), 3966.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), 65-88.

Khan, A., & Mehmood, Y. (2019). Resource Management for Machine Type Communication and Internet of Things in Mobile Networks. *Journal of Engineering and Applied Sciences*, *38*(2), 31-42.

Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). *Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review*. *Applied Sciences, 11*(18), 8383. https://doi.org/10.3390/app11188383

Ambusaidi, M. A., Almseidin, M., Reddy, M., Rahman, M., & Shahrour, I. (2020). IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method. *Applied Sciences, 12*(10), 5015. https://doi.org/10.3390/app12105015

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics, 9*(7), 1177. https://doi.org/10.3390/electronics9071177

Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., ... & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. Sensors, 21(2), 446.

Rashid, M. M., Khan, S. U., Eusufzai, F., Redwan, M. A., Sabuj, S. R., & Elsharief, M. (2023). A federated learning-based approach for improving intrusion detection in industrial internet of things networks. Network, 3(1), 158-179.

Jamshidia, S., Nikanjama, A., Nafia, K. W., Khomha, F., & Rastab, R. (2025). Application of Deep Reinforcement Learning for Intrusion Detection in Internet of Things: A Systematic Review. *arXiv*. https://arxiv.org/abs/2504.14436

Karanam, V. (2023). Is there a Trojan! Literature Survey and Critical Evaluation of the Latest ML Based Modern Intrusion Detection Systems in IoT Environments. *arXiv*. https://arxiv.org/abs/2310.10778

Yaras, S., & Dener, M. (2024). IoT-based intrusion detection system using new hybrid deep learning algorithm. Electronics, 13(6), 1053.