AMERICAN ACADEMIC PUBLISHER

International journal of IoT (ISSN: 2692-5184)

Volume 05, Issue 01, 2025, pages 146-158
Published Date: -17-06-2025
Doi: -https://doi.org/10.55640/ijiot-05-01-08

Machine Learning-Based Framework for Detecting Unauthorized IoT Devices

Venkata Srinivas Kompally
Northeastern University, Boston, MA, United States of America

Preethi Gajawada
Sreenidhi Institute of Science and Technology, Hyderabad, India

ABSTRACT

The widespread adoption of Internet of Things (IoT) devices across homes and enterprises has introduced significant security risks, especially when unauthorized or compromised devices gain access to sensitive networks. This paper proposes a machine learning-based framework to detect unauthorized IoT devices in real-time using features extracted from TCP/IP traffic. We utilize a Random Forest classifier trained on labeled network traffic from authorized devices. The proposed approach detects device types not on a pre-established whitelist, achieving an average of 96% accuracy in identifying unauthorized devices based on a 20-session window classification. The framework generalizes across different vendors, supports real-time alerting, and is resilient against adversarial attacks.

Keywords: IoT security, unauthorized devices, machine learning, TCP/IP traffic, Random Forest, network traffic analysis, device detection, real-time detection, classification accuracy, adversarial resilience, vendor agnostic, anomaly detection, smart devices

1. INTRODUCTION

The world of modern businesses has completely changed with the new automation of tasks and devices within the firm owing to the advent of IoT, or the Internet of Things. (Ashton, 2017) Originally coined by Ashton, the Internet of Things (IoT) conceptually represents a global network of interconnected devices acting as humanity's nervous system. However, this rapid growth in device interconnectivity also invites many new cyber attack opportunities due to weak security measures, inconsistence in updating patches, unreliable default settings, and the wide use of different protocols set by different vendors. (Mercer, 2023) The scale of IoT adoption continues to expand, with predictions suggesting that approximately 50 billion IoT devices will be operational soon.

Due to the 'Bring Your Own IoT' policy (where employees are encouraged to attach personal devices used for work into the corporate network), the risk of harm posed to professional environments is now higher than ever. Fitness trackers, smart TVs, home automation hubs and voice assistants are among the many commonly used IoT devices that lack enterprise level security and therefore pose harm by acting as access points through installing malware, stealing information or lateral movement from one device to another inside the secure network for the worker.

It has been proven that smart TVs, even when not in use, can be turned into spying devices for stealing confidential information. Anything brought from home rather than work poses danger and the risks associated with IoT devices are not limited to IoT gadgets that are actively used only.

The constant change of user behavior—which includes the spontaneous connection of new or replacement devices—coupled with the diversity of an IoT ecosystem, makes traditional inventory and control systems obsolete. Enterprises today need self-adaptive systems that automatically and continuously track, classify, and manage all connected or unauthorized IoT devices as threats to the network infrastructure. Systems like these require dimensioning and design features that will make them robust to circumvention and also agnostic to specific vendor markings.

Our goal is to address this challenge by providing an oversight network monitoring model that can make active scan streams of device traffic for classified device types and also integrates with a firm's existing security infrastructure to neutralize any emerging threats.

While IoT devices are becoming more common in homes and workplaces, keeping them secure remains a big challenge. Most traditional security systems rely on fixed methods like MAC address filtering or preset device signatures. But attackers today are smarter. They can easily fake device identities or copy the behavior of known devices. (Neshenko et al., 2019) Comprehensive studies have systematically documented numerous IoT vulnerabilities and provided empirical evidence of widespread exploitation. As recent studies show (Bagaa et al., 2020; Almasabi et al., 2024), machine learning can potentially improve this by learning how devices normally behave and spotting anything unusual. Still, it’s not easy to build a system that works well across different brands of devices and unpredictable network setups. In this paper, we tackle this issue by introducing a smart detection system that uses machine learning to monitor how devices behave on the network. It works in real time, doesn’t depend on the device manufacturer, and can fit into existing company security systems with minimal changes.

In this study, we’re tackling the real-world challenge of spotting unauthorized IoT devices in enterprise networks quickly and accurately. The main goal is to build a system that works at scale, doesn’t rely on knowing the device brand, and can handle tricks like spoofing. It also needs to fit smoothly into the security tools companies already use. Instead of using outdated methods that check device IDs or fixed signatures, our approach looks at how devices behave on the network, using machine learning to catch anything unusual.

2. SYSTEM AND ATTACK MODEL

We simulate a model of an enterprise network that consists of a large user base subdivided into unique departments as well as numerous interrelated devices like printers, IP cameras, sensors, smart displays, and employee workstations. (Pedro Miguel Sánchez Sánchez et al., 2024) Sophisticated adversarial attacks have recently been analyzed, showing that attackers often attempt to mimic authorized devices by replicating behavioral patterns, highlighting the critical need for robust device fingerprinting.In such intricate systems, unauthorized devices may connect either deliberately in the case of a malicious insider attack, or inadvertently such as an employee attaching a personal smartphone, tablet, or smart device that contains malware or breaches corporate security standards.

Whether deliberately or through negligence, the steps taken by these devices can lead to significant security risks within the business system, especially in Bring-Your-Own-Device (BYOD) situations where work and personal lives become increasingly intermingled. Attached devices can be used as means by which assailants can strategically launch attacks on the vast infrastructure.

We differentiate this with two sub-categories of attack vectors:

• Untargeted Attacks: These are broad and opportunistic attacks such as botnets and scanning malware that indiscriminately infect vulnerable devices without targeting specific organizations. These drains take the easiest infection path and often rely on common configuration blunders or outdated firmware.

o Targeted Attacks: These include sophisticated, strategic operations that intentionally compromise devices. They range from supply chains integrated into their system to more traditional corporate espionage.

By posing as benign devices or imitating the actions of approved device types, attackers can take advantage of the implicit trust in the network, according to our threat model. Traditional device identification techniques, such as MAC address whitelisting or static IP controls, are rendered useless by this trust-based vulnerability because attackers can easily spoof these identifiers.

Our detection approach uses more than just static identifiers to combat this. Rather, it concentrates on examining the behavioral fingerprints of devices—patterns in their interactions, communication, and use of network resources. Devices are marked as suspicious whenever they try to replicate the permitted behaviors but show small variations in timing, protocol usage, or session structure.

We use supervised machine learning here to maintain a whitelist of acceptable device types. We allow the system to identify previously unknown or unauthorized devices, even when they attempt to replicate the communication profiles of trusted devices.

The following are made possible by this behavioral approach:

- Dynamic adaptation to changing threats and newly connected devices
- Proactive containment of potentially compromised endpoints; granular visibility into device-specific risk levels;
- Resistance to spoofing and impersonation attempts

These attack paths are illustrated in Figure. 1, which categorizes threats as targeted and untargeted based on intent and sophistication.

Figure 1: Classification of IoT Attacks in Enterprise Networks

3. WHITELISTING FOR IOT SECURITY

IoT communications are limited to a predetermined list of authorized device types by whitelisting, a network access control technique. This approach becomes extremely inefficient and prone to human error in large-scale enterprise environments, even though it works well in settings with a small number of devices, like controlled testbeds or small businesses. The static nature of traditional whitelisting finds it difficult to change dynamically as the number and variety of IoT devices increase, from printers and IP cameras to industrial sensors and employee-connected personal devices.

Our suggested system offers an automated whitelisting framework based on machine learning to address this. It uses sophisticated behavioral fingerprinting techniques to continuously monitor and analyze network traffic in real time. It uses learned communication to categorize devices rather than MAC address lists or hardcoded device identifiers such as packet size distributions, protocol usage, session intervals, and flow entropy.

Our system detects anomalies that indicate the presence of unauthorized or potentially dangerous devices by comparing observed behaviors to known profiles of authorized devices. Regardless of whether they are trying to mimic genuine devices, devices that do not fit into any pre-established behavioral category are marked as unauthorized.

This strategy has a number of significant benefits:

- Scalability: enables smooth scaling across thousands of devices and does away with the need for manual updates.
- Adaptability: Adapts to changing device behavior, enabling detection even when firmware updates or modifications to communication patterns are made to IoT devices.
- Real-time Integration: Provides alerts and starts automated reactions (like quarantining a device or blocking its traffic) by establishing a direct connection with already-existing Security Information and Event Management (SIEM) tools.
- Vendor-Agnostic Operation: This feature functions with devices of all types and vendors without requiring agent installations or vendor-specific signatures.

Overall, our intelligent whitelisting framework modernizes network defense by combining the rigor of traditional access control with the flexibility and responsiveness of machine learning—providing robust protection against unauthorized IoT activity in enterprise-scale deployments.

4. CONTRIBUTIONS

1. **Novel Application of Random Forest Classifiers for IoT Device Type Identification**

   We demonstrate a novel application of Random Forest (RF) classifiers to reliably distinguish between different types of IoT devices based only on the features of their TCP/IP traffic. Our method uses session-level flow metadata, including packet sizes, inter-arrival times, port usage, and protocol distribution, to create a very strong behavioral fingerprint for each device class, in contrast to the previous methods that rely on deep packet inspection or device-specific signatures. As a result, our solution is highly scalable, lightweight, and protocol-agnostic for real-time enterprise deployment.

2. **Evaluation on a Real-World Dataset of IoT Devices Across Extended Durations**

A large, real-world dataset comprising 17 different IoT devices of 9 functional types—such as security cameras, smart plugs, sensors, and hubs—is used to train and assess our model. The data, which was gathered over several months under various operating circumstances, captured the inevitable variations in device behavior brought on by firmware updates, usage trends, and network load. We can assess our classifier's stability and long-term performance in real-world scenarios thanks to this realistic dataset.

3. **High Detection Accuracy Through Session-Based Voting**

   Using a sliding window voting mechanism over 20 consecutive sessions, we show that our system can detect unauthorized or anomalous device types with 96% accuracy. This method improves reliability in dynamic environments by efficiently smoothing out temporary misclassifications. The model ensures high precision in identifying rogue or spoof devices by avoiding false positives caused by transient anomalies by aggregating predictions over several sessions..

4. **Generalization Across Device Vendors and Laboratory Environments**

   Our approach's capacity to generalize across manufacturers and deployment environments is one of its main advantages. Even when devices from different vendors perform similar tasks, the classifier is able to successfully differentiate between them. The robustness of our behavioral feature extraction and model training pipeline under various network conditions is further validated by experiments carried out in various lab locations, which show consistent performance.

5. **Resilience Against Adversarial Mimicry and Behavioral Spoofing**

   Strong resistance to adversarial attacks, in which malevolent devices try to imitate the traffic patterns of whitelisted devices, is demonstrated by the suggested framework. Our model is intrinsically resistant to surface-level spoofing because it relies on multi-dimensional, session-level behavior rather than static identifiers or header fields. Furthermore, even in the presence of obfuscated or purposefully altered traffic patterns, Random Forests' ensemble nature enhances the classifier's robustness and transportability.

6. **Deployment Blueprint for Enterprise-Scale SIEM Integration**

   For the purpose of incorporating our detection framework into current Security Information and Event Management (SIEM) systems, we offer implementation guidelines. To generate alerts, isolate suspicious devices, or initiate automated incident response workflows, our design facilitates the use of modular, real-time classification engines that can interface with enterprise monitoring tools. We also go over useful factors like network impact, computational overhead, and incremental model updates, which allow security teams to implement our solution with little interference with their current setup.

5. PROPOSED METHOD

- In order to treat each authorized device type as a separate class, we formulate the identification of IoT devices as a multi-class classification problem. A Random Forest classifier, which learns to differentiate between the communication patterns of various device types, is trained using a labeled training dataset that includes TCP/IP session features from known authorized devices.
- Let D={d1,d2,...,dn}D = \{d_1, d_2,..., d_n\}D={d1,d2,...,dn} represent the set of known authorized device types, also known as the whitelist. A high-dimensional feature vector based on packet-level attributes is used to represent each network session, such as:
- Average packet size

- Protocol distribution (TCP, UDP, HTTP, etc.)
- Session duration
- Number of packets exchanged
- Time interval between packets
- Source/destination port patterns
- Flow entropy

When the confidence in any known type is not high enough, the classifier CCC maps an input session sss to a 'unknown' class or to a predicted device type di∈Dd_i \in Ddi∈D.

A probability distribution Ps=[p1,p2,...,pn] is the classifier's output.P_s = [p_1, p_2,..., p_n]The probability that session sss belongs to each class is represented by Ps=[p1,p2,...,pn]. The session is deemed to originate from an unauthorized or novel device type if the highest confidence score max⁡(Ps)\max(P_s)max(Ps) is less than a predetermined threshold trt_rtr. The F1 score is used to optimize this threshold trt_rtr on a validation dataset to efficiently balance false positives and false negatives.

We use a majority voting approach over a sliding window of 20 sessions, which guarantees reliability during the real-time deployment process. This method assigns the final predicted class based on the majority label after aggregating the classification results from several consecutive sessions from a device. An alert is raised and the device is marked as unauthorized if the majority class label that is produced does not match the whitelist DDD.

The following are some benefits of this session-level aggregation:

- Lessen noise from temporary misclassifications
- Faster identification of unauthorized or compromised devices is made possible by increased resistance to hostile attempts to impersonate behavior.
- Sliding window voting, threshold tuning, and probabilistic inference are combined in the suggested detection model to provide reliable, scalable, and understandable identification of IoT device types in business networks.

A step-by-step overview of this detection and classification process is presented in Figure. 3.

6. EVALUATION

Over the course of several weeks, we gathered traffic data from 17 commercially available IoT devices in order to assess our methodology in a variety of realistic scenarios. These gadgets fell into nine different functional categories, including hubs, smart speakers, security cameras, and smart plugs. In order to replicate real-world variations in infrastructure, topology, and ambient traffic, the devices were set up in two physically distinct laboratory environments. We were able to record a variety of device behaviors under uncontrolled, natural usage patterns thanks to this configuration.

High-fidelity Pipeline for Session Capture and Feature Extraction

Wireshark was used to record all device communications, resulting in millions of TCP/IP sessions being recorded throughout the two labs. We created a unique traffic feature extraction pipeline to get the data ready for classification. The statistical, temporal, and protocol-level characteristics of the network flow were recorded by

processing and converting each recorded session into a high-dimensional feature vector. For every session, more than 330 features were created, including metrics like:

- Average and variance of packet sizes
- Time between packets (jitter)
- Protocol ratios (TCP, UDP, HTTP, etc.)
- Flow duration
- Inter-packet arrival patterns
- Entropy of destination ports and IPs

The most influential features contributing to device classification decisions are summarized in Figure. 5. The classifier was able to identify subtle yet dependable behavioral signatures linked to every kind of device thanks to this granular representation.

A. Sturdy Assessment Using Whitelist Exclusion Tests

We carried out nine exclusion experiments, each of which removed a single device type from the whitelist during training, to assess the system's capacity to identify unauthorized or unusual devices. This mimics a real-world situation in which a compromised or new device that hasn't been seen or authorized by the system before tries to connect to the network. Based on its departure from learned behavior, the classifier was then entrusted with classifying this excluded device type as unauthorized.

The system's average detection accuracy for unauthorized devices across these tests was 96%. As seen in Figure. 4, the model maintains consistently high accuracy across different unauthorized device types. Even when confronted with devices that are absent from the training data, this exhibits strong generalization and anomaly detection capabilities.

High Classification Accuracy for Authorized Devices

The system continuously achieved 99% classification accuracy when classifying sessions coming from whitelisted (authorized) devices. This suggests that the model can consistently maintain low false positive rates while differentiating between known device types.

B. Assessment of Transferability Across Environments

We conducted cross-lab transferability experiments to evaluate our model's robustness and portability. In these, data from one lab environment was used to train the model, and data from the second lab was used for testing. Our feature extraction process and model design are resilient and environmental agnostic, as demonstrated by the classifier's high accuracy in spite of environmental variations like background traffic and IP configurations.

These findings demonstrate the scalability and usefulness of our framework for real-world implementation, where devices might be introduced in various organizational branches or move across networks.

The overall design of the proposed detection system, including its components for traffic capture, feature extraction, classification, and SIEM integration, is shown in Figure. 2.

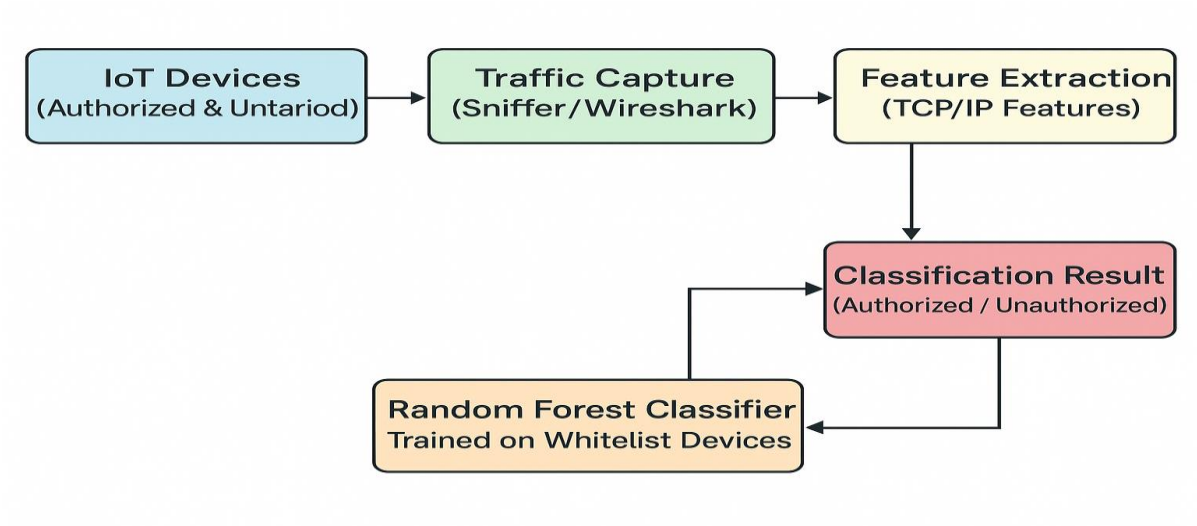

Figure 2: System Architecture for Unauthorized IoT Detection

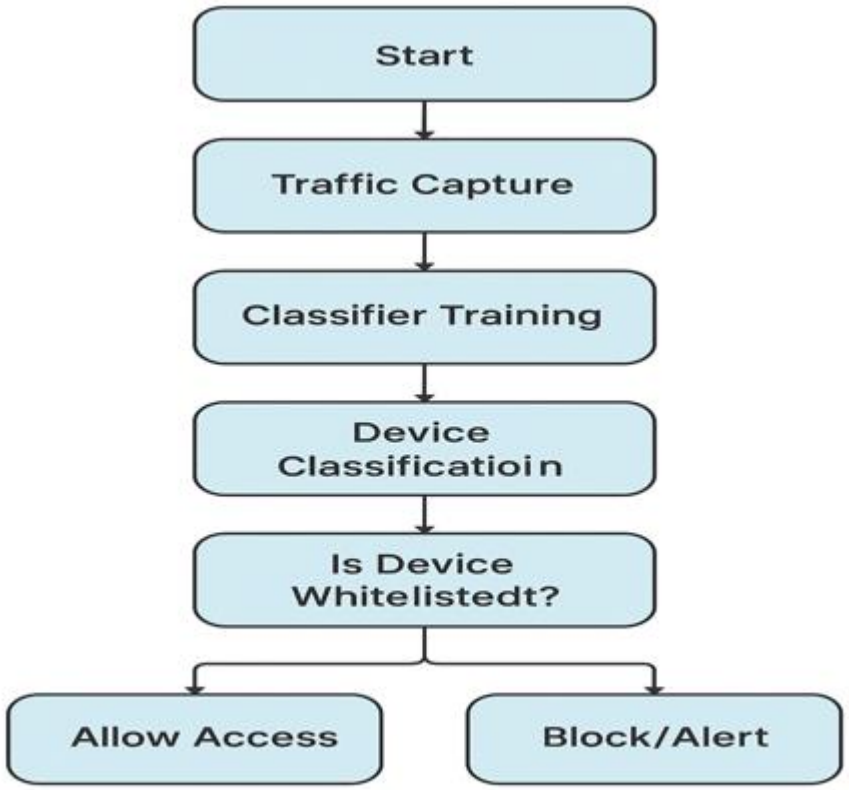

Figure 3: IoT Device Detection Workflow using ML

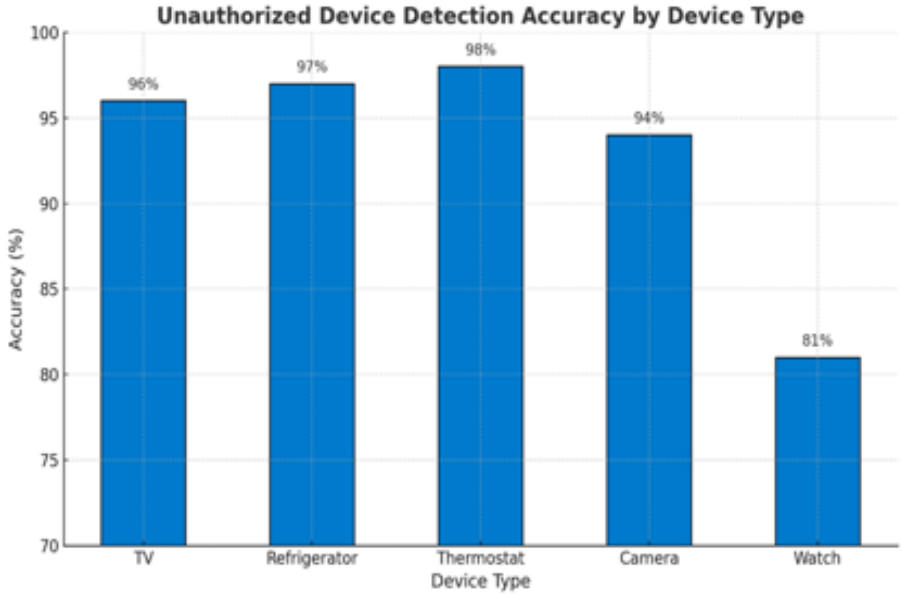

Figure 4: Unauthorized Device Detection Accuracy by Device Type

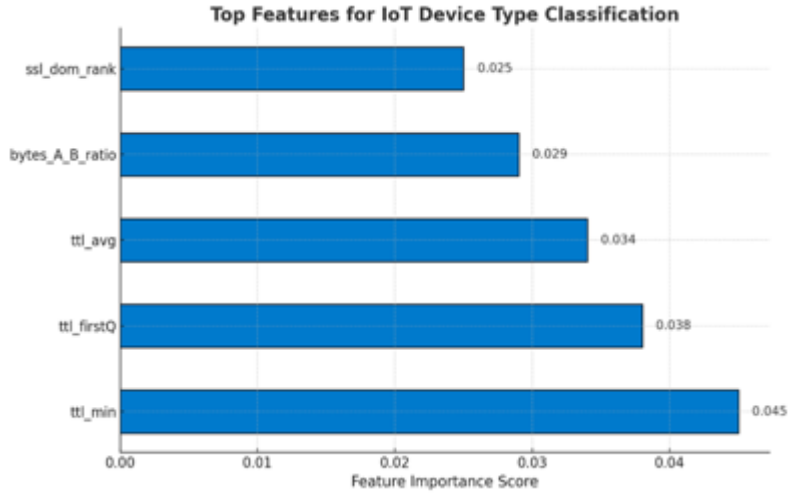

Figure 5: Top Features for IoT Device Type Classification

7. DEPLOYMENT

In order to monitor and categorize device behavior in real time, the suggested detection system is intended to be implemented as a background service within an enterprise network. In response to unauthorized device activity, it can be easily integrated into current Security Information and Event Management (SIEM) platforms, allowing for automatic alert generation, log correlation, and policy enforcement.

The system has the ability to initiate automated mitigation workflows when it detects an unauthorized or suspicious device. The company can use Software Defined Networking (SDN) to dynamically change network rules to isolate the device from important resources, quarantine it, or reroute it to a remediation zone. This shortens the window of exposure and speeds up incident response times by enabling quick reaction to threats without the need for manual intervention.

The classification window size, or the number of sessions examined to reach a device-level conclusion, is a crucial

system operating parameter. Faster identification is possible with smaller windows, but temporary anomalies may reduce their confidence. Larger windows, on the other hand, increase classification accuracy but cause detection latency. After conducting an empirical evaluation, we discovered that a 20-session sliding window provides a nearly ideal balance between detection speed and reliability, resulting in high accuracy and responsiveness appropriate for enterprise applications.

Based on network sensitivity, device criticality, and current response protocols, organizations can choose between faster alerts or higher confidence thanks to the system's adjustable design.

8. RELATED WORK

Techniques like MAC address-based identification, authentication-driven whitelisting, and radio frequency (RF) fingerprinting have been the main focus of earlier IoT device identification research. (Jabraeil Jamali et al., 2020) Various IoT architectures have been thoroughly analyzed, providing foundational understanding necessary for handling complex IoT ecosystems. Although these techniques have proven successful in controlled environments, they have a number of drawbacks that make them unsuitable for use in extensive, real-world enterprise networks.

Even though RF fingerprinting can identify devices with finer details, it usually requires specialized hardware and controlled signal environments, (Honar Pajooh et al., 2021) Blockchain-based multi-layer security architectures have gained popularity as effective tools to enhance IoT network defenses against unauthorized access. Which makes it inappropriate for use in enterprise settings that are heterogeneous and have different electromagnetic and physical conditions. On the other hand, MAC address-based identification is extremely susceptible to MAC spoofing attacks. (Xie et al., 2017) Focused surveys have detailed numerous security weaknesses prevalent in IoT device firmware, highlighting the critical need for more secure firmware practices. In which adversaries impersonate an authorized device's address in order to get around access controls. Preconfigured device credentials are a major component of authentication-based whitelisting, but they become unmanageable at scale and are unable to account for devices that are unknown or compromised without manual updates. Secure and lightweight authentication schemes have been proposed as essential measures to effectively safeguard next-generation IoT infrastructures (Rana et al., 2021).

Our work addresses these limitations through several key innovations:

- Multi-Class Behavioral Classification: Unlike many prior studies that frame device detection as a binary classification task (i.e., authorized vs. unauthorized), our system performs multi-class classification to accurately distinguish among multiple authorized device types. This approach allows for fine-grained control, ensuring that even subtle deviations from known device profiles are detected.
- Resilience to Identifier Spoofing: By relying on behavioral features extracted from standard TCP/IP traffic, our system becomes inherently robust against MAC address spoofing and other superficial impersonation techniques. The classification is based on how the device behaves rather than what it claims to be.
- No Need for Additional Hardware: Our method operates on passively collected network traffic, requiring no specialized sensors or modifications to the network infrastructure. This significantly simplifies deployment and supports integration into existing enterprise monitoring solutions.

Additionally, recent literature emphasizes the importance of integrating privacy-preserving techniques into IoT security frameworks. Emerging privacy-preserving techniques such as lightweight homomorphic encryption are increasingly suggested as solutions to secure sensitive IoT data without compromising operational efficiency (Li et al., 2021).

Machine learning approaches significantly advance the detection capabilities within IoT cybersecurity.Computational intelligence has emerged as a vital tool in enhancing IoT cybersecurity, enabling dynamic and automated threat detection (Zhao et al., 2020).

Further emphasizing the role of machine learning, previous research demonstrates robust cyberattack detection capabilities.

Deep learning techniques have shown significant promise in accurately detecting cyberattacks within IoT networks due to their adaptability and superior predictive capabilities (Zhou et al., 2018).

Intrusion detection systems are extensively reviewed in the literature. Previous surveys have extensively discussed the efficiency, energy consumption, and privacy implications of various intrusion detection systems specifically designed for IoT environments (Arshad et al., 2020).

Research continues to explore critical IoT security challenges. Addressing security challenges and key vulnerabilities within IoT continues to be a significant area of research due to their critical impact on network security (Azrour et al., 2021).

Moreover, machine learning-based semi-supervised approaches are being utilized effectively in IoT.

Machine learning-based semi-supervised frameworks have been successfully applied to IoT scenarios, especially in tasks such as object and anomaly detection (Wang et al., 2019).

Finally, detailed surveys have documented firmware vulnerabilities and detection strategies comprehensively. Recent comprehensive surveys have underscored methodologies for detecting vulnerabilities specifically within IoT firmware, thus reinforcing the necessity of rigorous security evaluations (Feng et al., 2022).

Our study overcomes the scalability and validation gaps of prior work in addition to these methodological advancements. Numerous previous methods were tested on brief, tiny datasets that were collected in carefully monitored laboratory settings. On the other hand, a varied dataset of 17 IoT devices in 9 functional categories that was gathered over several weeks from two separate lab environments was used to train and test our system. Our framework's scalability and generalizability to dynamic enterprise deployments are guaranteed by this degree of real-world variability and longitudinal testing. All things considered, our contributions mark a substantial advancement in the scalable and useful machine learning-based identification of unauthorized IoT devices.

9. CONCLUSION

In this study, we proposed a machine learning-based framework for detecting unauthorized IoT devices in enterprise networks that is scalable, reliable, and extremely accurate. Our system does not require invasive device-level instrumentation or specialized hardware because it only uses passively collected TCP/IP traffic. With a 99% classification accuracy for authorized device types and an average detection accuracy of 96% for previously unseen devices, the framework employs a multi-class Random Forest classifier trained on rich session-level features.

Our framework takes a big step forward in securing IoT networks by making it possible to detect unauthorized devices in real time without needing to physically touch or change anything on the devices themselves. What makes it especially useful is that it works well across different brands and setups, which is perfect for companies with constantly changing environments. Since it fits easily into the tools many organizations already use and doesn’t need any special hardware, it’s a simple and effective way for teams to boost their security and react quickly when new threats appear.

Looking ahead, several directions can further enhance the effectiveness and applicability of our system:

- Protocol Diversity: Current implementation focuses on TCP/IP traffic. Expanding support to non-TCP/IP protocols such as Bluetooth, Zigbee, and MQTT will broaden applicability, particularly for industrial and home automation networks with heterogeneous communication stacks.
- Federated Learning for Privacy-Preserving Deployment: To enable collaborative model training across distributed enterprise environments without sharing raw traffic data, future versions of the system will explore federated learning. This will allow organizations to benefit from shared intelligence while preserving data privacy and complying with regulatory requirements.
- Adaptive Learning and Online Updates: Incorporating online learning mechanisms would allow the model to dynamically adapt to evolving device behaviors and newly introduced devices, further reducing maintenance overhead and manual intervention.

REFERENCES

1. M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A Machine Learning Security Framework for Iot Systems," in *IEEE Access*, vol. 8, pp. 114066-114077, 2020
2. M. Almasabi, M. Khemakhem, F. E. Eassa, A. Ahmed Abi Sen, A. B. Alkhodre and A. Harbaoui, "A Smart Framework to Detect Threats and Protect Data of IoT Based on Machine Learning," in *IEEE Access*, vol. 12, pp. 176833-176844, 2024.
3. Pedro Miguel Sánchez Sánchez, Alberto Huertas Celdrán, Gérôme Bovet, Gregorio Martínez Pérez,Adversarial attacks and defenses on ML- and hardware-based IoT device fingerprinting and identification,Future Generation Computer Systems,Volume 152,2024
4. Li, S.; Zhao, S.; Min, G.; Qi, L.; Liu, G. Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things. *IEEE Internet Things J.* 2021, *9*, 14542–14550. [Google Scholar] [CrossRef]
5. Zhao, S.; Li, S.; Qi, L.; Xu, L.D. Computational Intelligence Enabled Cybersecurity for the Internet of Things. *IEEE Trans. Emerg. Top. Comput. Intell.* 2020, *4*, 666–674. [Google Scholar] [CrossRef]
6. Arshad, J.; Azad, M.A.; Amad, R.; Salah, K.; Alazab, M.; Iqbal, R. A review of performance, energy and privacy of intrusion detection systems for IoT. *Electronics* 2020, *9*, 629. [Google Scholar] [CrossRef]
7. Mercer, D. Smart Home Will Drive Internet of Things To 50 Billion Devices. Available online: https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2017/10/26/smart-home-will-drive-Internet-of-things-to-50-billion-devices-says-strategy-analytics (accessed on 1 January 2023).
8. Ashton, K. Making sense of IoT. In *How the Internet of Things Became Humanity's Nervous System*; Hewlett Packard Enterprise: Spring, TX, USA, 2017. [Google Scholar]
9. Jabraeil Jamali, M.A.; Bahrami, B.; Heidari, A.; Allahverdizadeh, P.; Norouzi, F. IoT architecture. In *Towards the Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 9–31. [Google Scholar]
10. Honar Pajooh, H.; Rashid, M.; Alam, F.; Demidenko, S. Multi-layer blockchain-based security architecture for internet of things. *Sensors* 2021, *21*, 772. [Google Scholar] [CrossRef] [PubMed]

11. Rana, M.; Shafiq, A.; Altaf, I.; Alazab, M.; Mahmood, K.; Chaudhry, S.A.; Zikria, Y.B. A secure and lightweight authentication scheme for next generation IoT infrastructure. *Comput. Commun.* 2021, *165*, 85–96. [Google Scholar] [CrossRef]

12. Azrour, M.; Mabrouki, J.; Guezzaz, A.; Kanwal, A. Internet of things security: Challenges and key issues. *Secur. Commun. Netw.* 2021, *2021*, 5533843. [Google Scholar] [CrossRef]

13. Wang, C.; Dong, S.; Zhao, X.; Papanastasiou, G.; Zhang, H.; Yang, G. SaliencyGAN: Deep learning semisupervised salient object detection in the fog of IoT. *IEEE Trans. Ind. Inform.* 2019, *16*, 2667–2676. [Google Scholar] [CrossRef]

14. Zhou, Y.; Han, M.; Liu, L.; He, J.S.; Wang, Y. Deep learning approach for cyberattack detection. In Proceedings of the IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, 15–19 April 2018; IEEE: New York, NY, USA, 2018; pp. 262–267. [Google Scholar]

15. Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G.; Ghani, N. Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Commun. Surv. Tutor.* 2019, *21*, 2702–2733. [Google Scholar] [CrossRef]

16. Xie, W.; Jiang, Y.; Tang, Y.; Ding, N.; Gao, Y. Vulnerability detection in iot firmware: A survey. In Proceedings of the 2017 IEEE 23rd International Conference on Parallel and dIstributed Systems (ICPADS), Shenzhen, China, 15–17 December 2017; IEEE: New York, NY, USA, 2017; pp. 769–772. [Google Scholar]

17. Feng, X.; Zhu, X.; Han, Q.L.; Zhou, W.; Wen, S.; Xiang, Y. Detecting vulnerability on IoT device firmware: A survey. *IEEE/CAA J. Autom. Sin.* 2022, *10*, 25–41. [Google Scholar] [CrossRef]

18. Eliganti Ramalakshmi, Venkata Srinivas Kompally, Baddam Deepika Reddy. (2020). Solar Powered Smart Irrigation and Monitoring System for Greenhouse Farming using IoT. International Journal of Advanced Science and Technology, 29(04), 8239 -. Retrieved from http://sersc.org/journals/index.php/IJAST/article/view/30559

19. Kompally, V. S. (2025). A microservices-based hybrid cloud-edge architecture for real-time IIoT analytics. Journal of Information Systems Engineering and Management, 10(16s). https://doi.org/10.52783/jisem.v10i16s.2567