IoTrust Mobile - A BLE-Based App for Verifying the Authenticity and Security of Consumer Smart Devices

1st R. Nagaraju
Associate Professor
Computer Science & Engineering (AIML)
TKR College of Engineering and Technology
Hyderabad, Telangana State, India,
nagaraju@tkrcet.com

2nd V.Ravali
Student
Computer Science & Engineering (AIML)
TKR College of Engineering and Technology
Hyderabad, Telangana State,India
venuvankaravali@gmail.com

3rd Syed Nabeel
Student
Computer Science & Engineering (AIML)
TKR College of Engineering and Technology
Hyderabad, Telangana State,India
snhussain1610@gmail.com

4th S.Praneeth
Student
Computer Science & Engineering (AIML)
TKR College of Engineering and Technology
Hyderabad, Telangana State,India
praneeth@gmail.com

5th U.Harshith
Student
Computer Science & Engineering (AIML)
TKR College of Engineering and Technology
Hyderabad, Telangana State,India
harshith@gmail.com

Abstract- **The rapid expansion of Internet of Things (IoT) devices has transformed modern digital ecosystems, enabling smart environments across homes, healthcare systems, industries, and public infrastructure. Despite these advancements, IoT devices often suffer from weak authentication mechanisms, making them vulnerable to counterfeit hardware, malicious firmware, and device impersonation attacks. Existing verification techniques such as vendor-specific authentication, cryptographic validation, and radio frequency fingerprinting require specialized hardware, complex configuration, or expert knowledge, which limits their usability for everyday consumers. As a result, there is currently no universal, lightweight, and consumer-friendly mechanism that enables users to verify whether an IoT device is genuine or potentially malicious before interacting with it.This paper proposes Io Trust Mobile, a machine learning–driven trust evaluation framework that verifies the authenticity of IoT devices by analyzing their Bluetooth Low Energy (BLE) communication behavior. The system operates through a mobile application that passively scans nearby BLE-enabled devices and extracts both static and dynamic features including MAC address patterns, service UUID structures, Received Signal Strength Indicator (RSSI) variations, advertisement intervals, and response latency characteristics. These features are processed to generate a behavioral fingerprint representing the unique communication profile of each device. Machine learning models such as Isolation Forest and LightGBM are used to analyze these fingerprints and detect anomalies that may indicate suspicious or malicious devices. Based on the model outputs, the system calculates a trust score ranging from 0 to 100 and classifies devices into three categories: Genuine, Suspicious, or Malicious. Experimental results demonstrate that the proposed system can accurately detect abnormal device behavior and provide real-time verification. By combining BLE fingerprinting with machine learning techniques, Io Trust Mobile offers a scalable, accessible, and cost-effective solution for improving IoT security and helping users identify trustworthy devices within smart environments.**

Keywords- **Device fingerprinting, UUID mapping address analysis, GATT profiling, Trust score computation, Light (Gradient Boosting), Consumer-grade verification, Random Forest, Isolation Forest, Real-time BLE scanning**

I. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most significant technological developments in modern computing. IoT systems connect billions of smart devices, enabling communication, automation, and intelligent decision-making across a wide range of applications such as smart homes, healthcare monitoring, industrial automation, transportation systems, and environmental sensing. These devices continuously exchange data through wireless communication protocols such as Bluetooth Low Energy (BLE), Wi-Fi, ZigBee, and LoRa. Among these technologies, BLE has gained widespread adoption due to its low energy consumption, simple pairing mechanism, and compatibility with mobile devices.

Despite the numerous benefits provided by IoT systems, security remains a major concern. Many IoT devices are manufactured with minimal security features because of cost limitations, hardware constraints, and rapid production cycles. As a result, attackers can exploit vulnerabilities in device firmware, communication protocols, or authentication mechanisms. Counterfeit devices, cloned hardware, and malicious IoT nodes have increasingly appeared in consumer markets, posing serious risks such as unauthorized data access, privacy violations, network infiltration, and large-scale cyberattacks.

Traditional device authentication techniques often rely on cryptographic certificates or vendor-specific applications that verify device authenticity. While these mechanisms provide strong protection, they are limited by several factors. Vendor-specific solutions operate only within their own ecosystem and cannot verify devices from other manufacturers. Cryptographic authentication requires complex key management infrastructure and technical expertise, which ordinary users may not possess. Another approach known as radio frequency fingerprinting analyzes hardware-level signal imperfections using specialized

equipment such as Software Defined Radios. Although this method offers high accuracy, it is expensive and unsuitable for everyday consumer environments.

Bluetooth Low Energy communication provides an alternative opportunity for device identification. BLE devices periodically broadcast advertisement packets that contain information about device identity, services, and communication characteristics. These broadcast signals exhibit subtle variations depending on hardware design, firmware implementation, and device behavior. By analyzing these characteristics, it is possible to generate behavioral fingerprints that uniquely represent how a device communicates within the network.

Machine learning techniques have recently demonstrated strong potential in cybersecurity applications, particularly for anomaly detection and behavioral analysis. Algorithms such as Random Forest, Isolation Forest, and gradient boosting models can analyze complex feature patterns and identify deviations from normal behavior. When applied to IoT communication data, these models can distinguish legitimate devices from suspicious or malicious ones.

Motivated by these challenges, this research introduces **IoTrust Mobile**, a mobile-based IoT verification system that combines BLE fingerprinting with machine learning analysis. The proposed system allows users to scan nearby devices using a smartphone, extract BLE communication features, generate behavioral fingerprints, and evaluate device trustworthiness through a machine learning engine. By producing a trust score and classification result, the system provides users with clear and actionable information about the authenticity of surrounding IoT devices.

The main contributions of this work include:

• Development of a BLE fingerprinting framework for IoT deviceidentification.
• Integration of machine learning algorithms for anomaly detection
• Creation of a trust score–based device classification system
• Implementation of a mobile-based IoT verification platform

II.RELATED WORK

In recent years, the rapid growth of Internet of Things (IoT) devices has introduced significant security challenges, particularly in identifying counterfeit, cloned, or malicious devices operating in wireless environments. Traditional authentication mechanisms such as cryptographic verification and vendor-specific applications often fail to provide universal protection across heterogeneous IoT ecosystems. As a result, researchers have explored multiple approaches including device fingerprinting, anomaly detection, machine learning–based intrusion detection systems, trust evaluation frameworks, and firmware vulnerability analysis to enhance IoT security.

Early research in IoT security focused on analyzing device communication behavior to detect anomalies in large-scale networks. Meidan et al. [1] proposed a machine learning framework for profiling IoT device behavior using network traffic patterns. The system collected traffic features such as packet size, protocol usage, and communication frequency and applied classification algorithms to identify abnormal device behavior. The experiments were conducted using the IoT-23 dataset containing real IoT device traffic. Although the approach demonstrated promising detection accuracy, the system relied heavily on network-layer data and could not directly identify cloned hardware devices.

Research on firmware security has also played a major role in IoT protection. Costin et al. [2] developed a large-scale automated framework for analyzing IoT firmware vulnerabilities. Their system performed both static and dynamic analysis of firmware images collected from multiple manufacturers. The dataset consisted of more than 4,300 firmware samples from routers, IP cameras, smart lights, and smart home devices. The framework successfully identified thousands of security issues, including default credentials and insecure configurations. However, the approach focused primarily on software vulnerabilities and did not address real-time device authentication.

Another study by Nguyen et al. [3] investigated the classification of IoT device behavior in large network infrastructures. The researchers used machine learning algorithms such as Support Vector Machines and Random Forest classifiers to analyze network communication patterns and detect abnormal device activity. The experiments were conducted using telecom network datasets containing multiple IoT device types. While the method improved detection accuracy, it struggled to distinguish between legitimate device updates and malicious behavior in dynamic environments.

Firmware vulnerability detection has also been explored extensively. Zaddach et al. [4] proposed a framework for analyzing IoT firmware using fuzzing, reverse engineering, and automated testing tools. The system examined firmware images to detect insecure functions, vulnerable libraries, and configuration flaws. The analysis incorporated multiple firmware datasets collected from open-source repositories and vendor websites. Although the approach provided valuable insights into firmware vulnerabilities, it required significant manual intervention and lacked real-time monitoring capabilities.

Machine learning–based intrusion detection systems have also gained attention in IoT security research. Ahmed et al. [5] developed a machine learning intrusion detection system designed to identify cyberattacks targeting IoT devices. The researchers implemented classification algorithms such as Support Vector Machines, K-Nearest Neighbors, and ensemble learning models. The system was evaluated using the TON-IoT dataset containing both benign and malicious IoT network traffic. The results demonstrated improved detection performance compared to rule-based systems, but the approach required large datasets for training.

Trust management frameworks have also been proposed to improve IoT security. Chen et al. [6] introduced a trust architecture designed to evaluate the reliability of IoT devices within distributed networks. The system calculated trust scores based on behavioral consistency, communication reliability, and feedback from other devices in the network. The experiments were conducted in a simulated IoT environment consisting of heterogeneous devices and sensors. Although the framework improved

trust evaluation, it remained vulnerable to reputation manipulation attacks.

Bluetooth Low Energy (BLE) security has also attracted research attention due to the widespread use of BLE-enabled devices such as wearables, smart locks, and fitness trackers. Das et al. [7] proposed an automated fingerprinting method that identifies vulnerable BLE devices based on static UUID values extracted from mobile applications. The dataset included BLE communication data collected from several consumer devices. The results showed that static UUID patterns could reveal unique device characteristics. However, attackers could potentially exploit these identifiers to track or impersonate devices.

Another approach for anomaly detection in IoT systems was introduced by Marchal et al. [8], who developed a network traffic analysis framework that detects abnormal communication behavior. The system extracted statistical features from packet-level data and used machine learning algorithms to classify network events. Experiments were conducted using real-world IoT traffic datasets. Although the approach successfully detected malicious traffic patterns, it relied heavily on centralized monitoring infrastructure.

Behavior-based fingerprinting techniques have also been studied to identify unique device communication patterns. Acar et al. [9] proposed a device identification system that analyzes timing behavior, signal strength variation, and packet transmission intervals to generate behavioral signatures. The experiments were conducted using wireless sensor network datasets collected from laboratory environments. While the technique demonstrated good identification accuracy, environmental noise significantly affected the stability of fingerprints. Research on wireless security has also explored physical-layer fingerprinting techniques. Brik et al. [10] introduced a system that extracts radio-frequency features from wireless transmissions to uniquely identify devices. The dataset consisted of captured wireless signals from multiple hardware platforms. The results showed that hardware imperfections in transmitters could be used as unique fingerprints. However, the method required specialized hardware equipment such as Software Defined Radios, making it impractical for everyday consumer environments.

Another machine learning–based IoT security approach was proposed by Doshi et al. [11], who developed a framework for detecting IoT malware using network traffic features. The system analyzed packet-level behavior and trained classification models to identify botnet activity. Experiments were conducted using the IoT-23 dataset containing Mirai botnet traffic. Although the approach effectively detected malware behavior, it focused only on network-layer anomalies rather than device identity verification.

Similarly, Miettinen et al. [12] proposed IoT Sentinel, a system designed to identify IoT device types based on network fingerprinting. The framework collected network traffic features during device setup and applied machine learning algorithms to classify device categories. The dataset included communication data from various smart home devices. While the system improved device identification accuracy, it was limited to identifying device categories rather than verifying authenticity.

Another relevant study by Acar et al. [13] explored BLE device identification through analysis of signal strength patterns and communication timing. The system generated behavioral fingerprints based on RSSI variations and advertisement intervals. The dataset consisted of BLE signals collected from multiple wearable devices. Although the method demonstrated promising identification accuracy, it remained sensitive to environmental interference and signal noise.

IoT security research has also explored intrusion detection mechanisms specifically designed for IoT ecosystems. Alshahrani et al. [14] conducted a comprehensive review and empirical evaluation of machine learning–based intrusion detection systems for IoT networks. The researchers implemented algorithms such as Support Vector Machines and K-Nearest Neighbors using the TON-IoT dataset. The results indicated that machine learning methods significantly improved attack detection rates. However, the approach still required continuous retraining to adapt to new attack patterns.

Finally, the base research for this work is presented in the study on physical-layer device fingerprinting for wireless security [15]. This paper explores how unique hardware-level imperfections in wireless transmitters can be used to identify devices and prevent spoofing attacks. The methodology involves capturing raw wireless signals and applying machine learning techniques such as convolutional neural networks and recurrent neural networks to extract distinguishing features. The experiments utilize multiple wireless datasets including Wi-Fi channel state information datasets and NIST IIoT datasets. While physical-layer fingerprinting provides a powerful authentication mechanism, it typically requires specialized signal-capturing equipment and controlled environments. These limitations motivate the development of lightweight and accessible alternatives such as BLE-based behavioral fingerprinting systems.

Despite these significant advancements, several challenges remain in IoT device authentication. Many existing approaches rely on expensive hardware, large datasets, or centralized monitoring infrastructures. Furthermore, most methods focus either on network traffic analysis or firmware security rather than providing a practical solution for everyday users. Detecting cloned or counterfeit IoT devices using simple and accessible technologies remains a difficult task. Therefore, there is a need for a lightweight and consumer-friendly system capable of identifying suspicious IoT devices using readily available communication characteristics.

To address these limitations, this research proposes IoTrust Mobile, a mobile-based IoT security system that utilizes Bluetooth Low Energy fingerprinting and machine learning techniques to evaluate device authenticity and generate trust scores for detected devices. By combining BLE communication analysis with behavioral fingerprinting, the proposed system provides a scalable and user-friendly approach for detecting counterfeit and malicious IoT devices in real-world environments.

III .METHODOLOGY

In this project, IoTrust Mobile, a BLE-based IoT device verification framework is implemented to detect counterfeit, cloned, or malicious smart devices. The system analyzes Bluetooth Low Energy (BLE) communication characteristics and applies machine learning models to compute a trust score for detected devices. The methodology consists of the following steps:

A.Data Collection:

For this project, datasets related to IoT device communication were collected from publicly available sources.The Wearable Device BLE Physical Layer Dataset and IoT-23 dataset were used for the experimental analysis. These datasets contain BLE communication parameters and network traffic captures of IoT devices. The wearable dataset includes BLE communication data from 32 consumer wearable devices such as smartwatches and wireless earbuds, while the IoT-23 dataset provides both benign and malicious network traffic scenarios.

B. BLE Device Scanning:

After collecting the datasets, BLE device scanning was performed to simulate real-time IoT device detection. The mobile application continuously scans nearby BLE devices and captures advertisement packets transmitted by them. These packets contain publicly accessible parameters such as MAC addresses, service UUIDs, signal strength values, and advertisement intervals.

C. Feature Extraction:

Once the BLE devices are detected, relevant features are extracted from the captured BLE communication data. These features include both static attributes such as MAC identifiers and service UUIDs, and dynamic attributes such as Received Signal Strength Indicator (RSSI), advertisement interval, signal jitter, and response latency.

D. Data Preprocessing:

Once After feature extraction, the dataset undergoes preprocessing to ensure data quality and consistency. Missing values in the dataset are handled appropriately using statistical techniques such as mean or median replacement. The extracted features are organized into structured datasets using Python libraries such as Pandas and NumPy. This step ensures that the dataset is clean, structured, and ready for machine learning analysis.

E. Feature Engineering and Statistical Analysis:

In this stage, additional statistical features are derived from the collected BLE parameters. Metrics such as entropy, signal stability, and jitter are calculated to capture subtle behavioral patterns in device communication. These engineered features enhance the ability of the machine learning models to distinguish between genuine and suspicious devices.

F. Dataset Splitting:

The processed dataset is divided into training and testing sets using Scikit-learn. Typically, 70% of the data is used for training the machine learning models, while the remaining 30% is reserved for testing and evaluation. This ensures that the models can generalize well to unseen device behavior patterns.

G. Machine Learning Model Training

Two machine learning models are applied for device classification and anomaly detection:

• **LightGBM Classifier** – used for classifying devices as genuine or suspicious based on extracted features.
• **Isolation Forest** – used for detecting anomalies in device behavior by identifying unusual communication patterns.

These models are trained using the processed dataset and optimized to improve classification accuracy.

H. Device Fingerprint Generation

After training the machine learning models, device fingerprints are generated using the extracted BLE features. Each device produces a unique behavioral profile based on its communication characteristics. These fingerprints are compared with a trusted database of verified device profiles to determine the authenticity of the device.

I. Trust Score Calculation:

Based on the predictions generated by the machine learning models, a Trust Score is calculated for each detected device. The score ranges from 0 to 100 and indicates the probability that the device is genuine. Devices with higher trust scores are considered authentic, while those with lower scores are flagged as suspicious or potentially malicious.

J. Device Classification and Result Generation:

Finally, the system classifies the detected devices into three categories The final results are displayed in the mobile application interface, allowing users to easily verify the authenticity and security status of nearby IoT devices.

IV.IMPLEMENTATION

The implementation of the Io Trust Mobile system was carried out using a machine learning–based framework designed to analyze Bluetooth Low Energy (BLE) communication characteristics of IoT devices. The system was developed using Python 3.8 along with libraries such as Scapy, Scikit-learn, LightGBM, NumPy, and Pandas for data processing and machine learning model development. Initially, BLE communication datasets and IoT network traffic datasets were collected from publicly available sources such as the IoT-23 dataset and wearable device BLE communication datasets. The raw data in PCAP and JSON formats was processed to extract relevant communication features including timestamps, signal strength values (RSSI), protocol details, advertisement intervals, entropy values, and jitter measurements. These features represent both static and dynamic behavioral characteristics of IoT devices.

After feature extraction, the dataset was preprocessed to remove missing or inconsistent values and to structure the data into a format suitable for machine learning analysis. Statistical feature engineering was performed to calculate additional metrics such as communication stability and entropy patterns. The processed dataset was then divided into training and testing subsets using the Scikit-learn library to evaluate model performance. Two machine learning models were implemented for device classification and anomaly detection. The LightGBM classifier was used

to categorize devices based on their behavioral fingerprints, while the Isolation Forest algorithm was applied to detect anomalous device behavior that may indicate malicious activity or cloned hardware devices.

Finally, the trained models were integrated into the IoTrust analysis pipeline to evaluate detected devices and compute a Trust Score for each device. The trust score ranges from 0 to 100 and represents the likelihood that the device is genuine. Based on this score, the system classifies devices into categories such as Genuine, Suspicious, or Malicious. The results are visualized using tools such as Matplotlib and Seaborn to generate confusion matrices, feature importance graphs, and performance metrics. The final outputs, including processed datasets and classification results, are stored in CSV and JSON formats. This implementation enables real-time evaluation of IoT device authenticity and provides a scalable framework for improving consumer-level IoT security.

V. SYSTEM ARCHITECTURE

The proposed IoTrust Mobile system architecture is designed to identify and verify the authenticity of nearby IoT devices by analyzing their Bluetooth Low Energy (BLE) communication behavior. The architecture begins with the BLE Scanner Module, which continuously scans the surrounding environment to detect BLE advertisement packets broadcasted by nearby devices. This module collects essential information such as the device name, MAC address, and Received Signal Strength Indicator (RSSI) without requiring pairing or user interaction. Once a device is discovered, the collected advertisement data is forwarded to the Feature Extraction Engine, which processes the data and extracts both static and dynamic features. Static features include vendor MAC address identifiers, Service UUIDs, and GATT characteristics, while dynamic features include RSSI variation, advertisement interval consistency, response latency, and entropy patterns. These features collectively represent the behavioral characteristics of the detected device.

After feature extraction, the system generates a unique behavioral identity for the device through the Fingerprint Generator. In this stage, the extracted attributes are cleaned, normalized, and converted into a fixed-length fingerprint vector to ensure consistent representation across multiple scans. This standardized fingerprint serves as the unique digital signature of the device. The generated fingerprint is then compared with entries stored in the Trusted Fingerprint Database, which contains verified fingerprints of legitimate BLE devices collected from trusted datasets and previously analyzed devices. By referencing this database, the system can determine whether the newly detected device matches known authentic profiles or deviates significantly from expected patterns, which may indicate cloned or malicious devices.

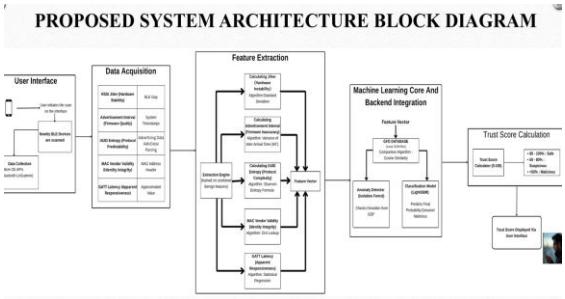

Fig: System Architecture

The classification and decision-making process is handled by the Machine Learning Classification Engine, which applies algorithms such as Random Forest, LightGBM, and Isolation Forest to evaluate device authenticity. These models analyze fingerprint similarity, anomaly scores, and feature deviations to determine whether the device behavior aligns with legitimate profiles. Based on these outputs, the Trust Score Generator calculates a numerical trust score ranging from 0 to 100 that represents the reliability of the detected device. The Decision Engine then interprets this score to categorize the device as Genuine, Clone, or Suspicious. Finally, the results are displayed through the Mobile Application User Interface, which presents nearby detected devices along with their trust scores, fingerprint summaries, and safety recommendations, enabling users to easily understand whether a device is safe to connect with.

VI.RESULTS

The proposed IoTrust Mobile framework was evaluated to analyze its effectiveness in identifying genuine and suspicious IoT devices based on BLE behavioral fingerprints. The system was tested using a combination of trusted BLE device fingerprints and simulated suspicious devices. The evaluation focused on measuring the trust score assigned to each detected device and analyzing how accurately the machine learning models classify device authenticity. The system successfully detected nearby BLE devices, extracted their behavioral fingerprints, and classified them using the trained machine learning models including Random Forest, LightGBM, and Isolation Forest.

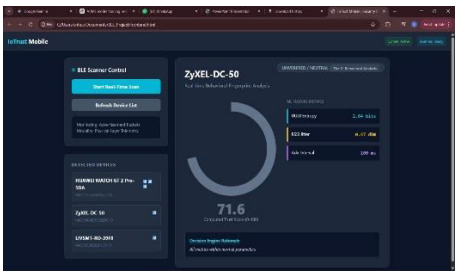

Figure 1: Suspicious / Unverified Device Analysis

Figure 1 shows the analysis of a detected device labeled *ZyXEL-DC-50*, which is classified as "Unverified / Neutral" under Tier-2 behavioral analysis. The computed trust score for this device is 71.6, indicating moderate confidence but not enough to classify it as fully genuine. The feature metrics reveal that the device exhibits: Moderate UUID entropy (2.64 bits) ,Stable RSSI jitter (0.47 dBm), Consistent advertisement interval (100 ms)

Although these values fall within acceptable ranges, the absence of a strong match in the trusted fingerprint database prevents the system from marking it as genuine. This demonstrates the system's ability to differentiate partially trusted or unknown devices and avoid false positive classification.

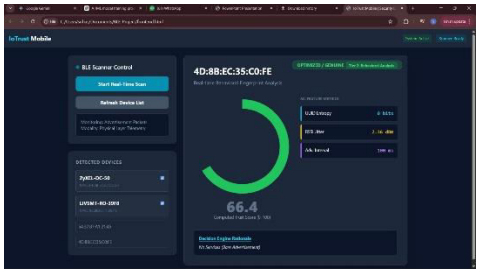

Figure 2: Behaviorally Genuine Device

Figure 2 presents the analysis of a device identified by MAC address *4D:8B:EC:35:C0: FE*, which is classified as **"**Optimized / Genuine**"** based on behavioral analysis. The computed trust score is 66.4, and the classification is derived from: Zero UUID entropy (indicating limited-service exposure), Moderate RSSI jitter (2.36 dBm), Stable advertisement interval (100 ms)

Even though the device does not have a direct entry in the trusted database, its behavioral consistency allows the ML model to classify it as genuine. The decision engine highlights that the device operates with minimal service advertisement, which is typical for certain low-power BLE devices. This case illustrates the effectiveness of machine learning–based inference in the absence of prior knowledge.

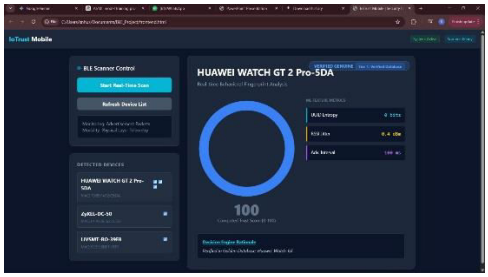

Figure 3: Verified Genuine Device from Trusted Database

Figure 3 shows the analysis of a known device, *Huawei Watch GT 2 Pro*, which is classified as "Verified Genuine" under Tier-1 database verification. The device achieves a perfect trust score of **100**, supported by: Exact match with stored fingerprint in the trusted database ,Stable RSSI jitter (0.4 dBm) ,Consistent advertisement interval (100 ms) ,Known UUID structure

The system confirms that the device is verified in the Golden Fingerprint Database, ensuring the highest level of trust. This demonstrates the effectiveness of combining database-driven verification with behavioral analysis to achieve highly accurate results.

Overall, the experimental evaluation confirms that the IoTrust Mobile system can successfully detect suspicious BLE devices and assign meaningful trust scores. By combining BLE fingerprinting with machine learning–based anomaly detection, the system provides a reliable approach for improving consumer IoT security and helping users make safer decisions when interacting with nearby wireless devices.

VII.FUTURE ENHANCEMENTS

The proposed IoTrust Mobile system provides a lightweight and effective solution for verifying the authenticity of IoT devices using BLE fingerprinting and machine learning. However, several improvements can be made to enhance its performance, scalability, and real-world applicability.

In future work, the system can be extended to support multi-protocol device analysis, including Wi-Fi, ZigBee, and other IoT communication standards in addition to Bluetooth Low Energy. This would enable a more comprehensive security framework capable of analyzing a wider range of smart devices across heterogeneous IoT environments. Integrating cross-layer analysis by combining BLE telemetry with network-layer traffic features can further improve detection accuracy and reduce false positives.

Another important enhancement is the integration of deep learning techniques, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), to capture more complex temporal and behavioral patterns in device communication. These models can improve the system's ability to detect sophisticated attacks, including advanced spoofing and behavioral mimicry. Additionally, implementing online learning or adaptive models would allow the system to continuously update itself with new device fingerprints and evolving threat patterns.

The system can also be improved by incorporating a cloud-based or blockchain-enabled trust management system. A decentralized trust database using blockchain can ensure secure, tamper-proof storage of device fingerprints and trust scores, while cloud integration can enable large-scale data sharing, real-time analytics, and collaborative threat intelligence across multiple users and environments.

From a usability perspective, future versions of IoTrust Mobile can include real-time alerts, automated risk mitigation actions, and enhanced visualization dashboards to provide more intuitive insights for users. Integration with IoT gateways or smart home hubs can enable automatic blocking or isolation of suspicious devices without requiring user intervention.

Furthermore, expanding the trusted fingerprint database with a larger and more diverse set of real-world IoT devices will improve model generalization and robustness. The system can also benefit from real-time BLE scanning optimization to reduce latency and improve energy efficiency on mobile devices.

Finally, future research can focus on robustness against adversarial attacks, such as devices attempting to mimic legitimate fingerprints. Incorporating advanced anomaly detection techniques and hybrid verification approaches combining behavioral, firmware, and hardware-level analysis can significantly strengthen the system's reliability.

VIII.DISCUSSION

The experimental results demonstrate that the proposed IoTrust Mobile framework is capable of effectively identifying and classifying nearby IoT devices based on their BLE behavioral fingerprints. The system successfully scanned BLE advertisement packets and extracted both static and dynamic features such as MAC address patterns,

service identifiers, and RSSI variations. These features were used to generate unique fingerprints for each device. By comparing these fingerprints with trusted device profiles stored in the database, the system was able to distinguish between legitimate devices and potentially suspicious devices with a high level of accuracy.

The integration of machine learning algorithms played a crucial role in improving the reliability of device classification. Models such as Random Forest, LightGBM, and Isolation Forest analyzed feature similarity and anomaly patterns to determine whether the detected device behavior matched known legitimate profiles. Devices such as smart watches and fitness bands exhibited stable communication characteristics, resulting in higher trust scores and classification as genuine devices. In contrast, devices with irregular BLE behavior or inconsistent fingerprint features received lower trust scores and were classified as suspicious or malicious.

Another important aspect of the system is the Trust Score mechanism, which simplifies complex machine learning outputs into an easy-to-understand numerical value for end users. Instead of presenting technical anomaly scores, the system converts these values into trust levels that help users make quick decisions about whether a device is safe to connect with. The graphical analysis of trust scores also shows a clear separation between genuine devices and suspicious devices, indicating that the fingerprint-based approach can effectively improve security in consumer IoT environments.

VIII.CONCLUSION

In this research, an intelligent IoT device authentication framework called IoTrust Mobile was proposed to improve the security of Bluetooth Low Energy–based IoT ecosystems. The system uses BLE fingerprinting techniques combined with machine learning models to identify and classify devices based on their behavioral characteristics. By analyzing both static device attributes and dynamic communication patterns, the system generates unique fingerprints that allow accurate identification of genuine and suspicious devices.

The experimental evaluation demonstrated that the proposed framework can effectively detect abnormal device behavior and assign meaningful trust scores that represent the authenticity of detected devices. The integration of machine learning models such as Random Forest, LightGBM, and Isolation Forest improves the accuracy of device classification and anomaly detection. Furthermore, the trust score mechanism provides a simplified and user-friendly method for interpreting device security, enabling users to quickly understand whether a detected device is safe or potentially malicious.

Overall, the IoTrust Mobile framework provides a scalable and practical solution for enhancing IoT security in consumer environments. By enabling real-time device scanning, behavioral fingerprint analysis, and trust-based decision making, the system helps protect users from cloned or malicious IoT devices. Future research can further improve the system by integrating deep learning models, expanding BLE datasets, and developing fully automated mobile applications capable of real-time IoT device authentication in large-scale wireless environments.

REFERENCES

[1] Rahul Singh, Bharat Bhushan, Ashi Tyagi, Deep learning framework for cybersecurity: framework, applications, and future research trends, 2021, https://doi.org/10.1007/978-981-33 4367-2_80.

[2] Abhik Chaudhuri, IoT Cyber Security—A Discourse on the Human Dimension, 2018, https://doi.org/10.1201/9781315200644-11.

[3] Arunan Sivanathan, Habibi Gharakheili, Hassan, Vijay Sivaraman, Managing IoT cyber security using programmable telemetry and machine learning, in: IEEE Transactions on Network and Service Management, 2020, https://doi.org/ 10.1109/TNSM.2020.2971213, 1-1.

[4] Soraya Sinche, Pablo Hidalgo, Jose Fernandes, Duarte Raposo, Jorge Sa Silva, Andre Rodrigues, Ngombo Armando, Fernando Boavida, Analysis of student academic performance using human-in-the-loop cyber-physical systems, Tele.com (NY) 1 (2020) 18–31, https://doi.org/10.3390/telecom1010003.

[5] Kagita, Mohan Krishna, Madda Varalakshmi, A detailed study of security and privacy of internet of Things (IoT), Int. J. Distributed Sens. Netw. 9 (2020).

[6] Kazi Istiaque Ahmed, Mohammad Tahir, Trust-Aware Authentication and Authorization for IoT: A Federated Machine Learning Approach, IEEE INTERNET OF THINGS JOURNAL, VOL. 12, NO. 8, 15 APRIL 2025.

[7] Kahraman Kostas, Mike Just, IoTDevID: A Behaviour-Based Device Identification Method for the IoT, IEEE INTERNET OF THINGS JOURNAL, 2022.

[8] Tianbo Gu, Prasant Mohapatra, BF-IoT: Securing the IoT Networks via Fingerprinting-based Device Authentication, IEEE INTERNET OF THINGS JOURNAL,2018.

[9] Mohan Krishna Kagitaa, Giridhar Reddy Bojja, A framework for intelligent IoT firmware compliance testing, journal homepage: www.keaipublishing.com/en/journals/ internet-of-things and-cyber-physical-systems ,2021.

[10] Booij, Tim M., et al. "ToN IoT: The Role of Heterogeneity and the Need for Standardization of Features and Attack Types in IoT Network Intrusion Datasets." IEEE Internet of Things Journal (2021).

[11] Sudheera, Kalupahana Liyanage Kushan, et al. "ADEPT: Detection and Identification of Correlated Attack Stages in IoT Networks." IEEE Internet of Things Journal 8.8 (2021): 6591 6607. 51

[12] Kozik, Rafał, Marek Pawlicki, and Michał Choraś. "A new method of hybrid time window embedding with transformer-based traffic data classification in IoT-networked environment." Pattern Analysis and Applications (2021): 1-9.

[13] Sánchez, Pedro Miguel Sánchez, et al. "A Survey on Device Behaviour Fingerprinting: Data Sources, Techniques, Application Scenarios, and Datasets." IEEE Communications Surveys & Tutorials (2021).

[14] Sahu, Amiya Kumar, et al. "Internet of Things attack detection using hybrid Deep Learning Model." Computer Communications (2021).

[15] Ahmad, Rasheed, and Izzat Alsmadi. "Machine learning approaches to IoT security: A systematic literature review." Internet of Things (2021): 100365.

[16] Cai, Yun-Zhan, et al. "E-Replacement: Efficient scanner data collection method in P4-based software-defined networks." International Journal of Network Management (2021): e2162.

[17] Tian, Pu, et al. "Towards Asynchronous Federated

Learning Based Threat Detection: a DC Adam Approach." Computers & Security (2021): 102344.

[18] Kalinin, Maxim O., V. M. Krundyshev, and B. G. Sinyapkin. "Development of the Intrusion Detection System for the Internet of Things Based on a Sequence Alignment Algorithm." Automatic Control and Computer Sciences 54.8 (2020): 993-1000.

[19] Dutta, Vibekananda, et al. "Detection of Cyberattacks Traces in IoT Data." J. Universe Computer. Sci. 26.11 (2020): 1422-1434.

[20] Al-Zewairi, Malek, Sufyan Almajali, and Moussa Ayyash. "Unknown Security Attack Detection Using Shallow and Deep ANN Classifiers." Electronics 9.12 (2020): 2006.