Article Information

Received: March 01, 2024
Accepted: September 12, 2024
Published: September 16, 2024

Citation: Praveen Kumar. (2024) Secure Tracking Using BLE and IoT in Mobile Applications: A Technical Overview. Ku J of Art Int, Rob, Mach and Data sci. 1(1): 027-030.

Copyright: ©2024 Praveen Kumar. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Research Article

Secure Tracking Using BLE and IoT in Mobile Applications: A Technical Overview

Naga Satya Praveen Kumar Yadati

***Corresponding author:** Narendar Kumar Ale, Sr. System Engineer (Information Technology), Employment, University of the Cumberlands, Williamsburg, Kentucky, USA, E-mail: narenderkumar.net@gmail.com

1.Abstract

With the proliferation of mobile devices and the Internet of Things (IoT), secure tracking systems have become increasingly important in various applications, including logistics, healthcare, and asset management. This paper presents a comprehensive technical overview of implementing secure tracking using Bluetooth Low Energy (BLE) and IoT technologies in mobile applications. It discusses the architecture, protocols, and security mechanisms necessary to ensure data integrity, confidentiality, and availability in BLE-enabled IoT tracking systems. The paper also explores potential vulnerabilities and provides recommendations for enhancing security in mobile-based tracking applications.

2.Introduction

The convergence of mobile technologies, BLE, and IoT has revolutionized tracking systems, enabling real-time monitoring and management of assets and resources. BLE, a power-efficient version of Bluetooth, is particularly suitable for IoT applications due to its low energy consumption and ability to connect multiple devices. However, the widespread adoption of BLE and IoT in mobile applications brings significant security challenges, such as unauthorized access, data breaches, and signal interception.

This paper aims to address these challenges by presenting a secure tracking solution using BLE and IoT in mobile applications. It provides an in-depth analysis of the system architecture, communication protocols, and security measures required to protect data and maintain the reliability of tracking systems.

3.System Architecture

The proposed secure tracking system consists of three primary components: IoT devices, BLE-enabled mobile applications, and cloud-based servers. Each component plays a crucial role in ensuring the seamless and secure operation of the tracking system.

3.1. IoT devices

IoT devices equipped with BLE capabilities are the primary data sources in the tracking system. These devices can be embedded with various sensors to collect data such as location, temperature, humidity, and motion. The data collected by IoT devices is transmitted to mobile applications via BLE for further processing and analysis.

3.2. BLE-enabled mobile applications

Mobile applications act as intermediaries between IoT devices and cloud servers. They receive data from IoT devices using BLE and perform preliminary data processing, such as filtering and aggregation. The processed data is then securely transmitted to cloud servers for storage and advanced analytics.

3.3. Cloud-based servers

Cloud-based servers provide scalable storage and computational resources for the tracking system. They receive data from mobile applications, store it securely, and perform advanced analytics to derive meaningful insights. The cloud servers also serve as a central repository for historical data, which can be accessed by authorized users for reporting and decision-making.

4.Communication Protocols

The secure tracking system employs various communication protocols to facilitate data exchange between IoT devices, mobile applications, and cloud servers. These protocols ensure data integrity, confidentiality, and availability throughout the communication process.

4.1. BLE communication protoco

BLE is a wireless communication protocol optimized for low-power consumption and short-range communication. It operates in the 2.4 GHz ISM band and uses frequency hopping to minimize interference. BLE communication is initiated by a central device (mobile application) that scans for advertising packets from peripheral devices (IoT devices). Once a connection is established, data can be exchanged between the central and peripheral devices using predefined profiles and services.

4.2. HTTPS/TLS for cloud communication

To ensure secure communication between mobile applications and cloud servers, the system uses HTTPS (Hypertext Transfer Protocol Secure) combined with TLS (Transport Layer Security). HTTPS encrypts data transmitted over the network, preventing unauthorized access and tampering. TLS provides additional security features, such as certificate-based authentication and integrity checks, to ensure the authenticity of the communication parties and the integrity of the transmitted data.

5.Security Mechanisms

Security is a critical aspect of the proposed tracking system, as it ensures the protection of sensitive data and prevents unauthorized access. The following security mechanisms are implemented to safeguard the tracking system:

5.1. Authentication and authorization

Authentication and authorization are essential for verifying the identity of users and devices and controlling access to system resources. The tracking system uses multi-factor authentication (MFA) to authenticate users, combining something they know (password) with something they have (OTP or biometric verification). Device authentication is achieved using BLE pairing, where devices exchange unique identifiers and cryptographic keys to establish a trusted connection.

5.2. Data encryption

Data encryption ensures the confidentiality of information transmitted between IoT devices, mobile applications, and cloud servers. The tracking system uses AES (Advanced Encryption Standard) for data encryption, which provides a high level of security with minimal computational overhead. Data is encrypted at rest and in transit, ensuring that it remains protected even if intercepted by unauthorized parties.

5.3. Secure key management

Key management is a critical component of the tracking system's security architecture. It involves generating, distributing, storing, and revoking cryptographic keys used for encryption and authentication. The system uses a centralized key management service (KMS) hosted on the cloud server to manage keys securely. The KMS generates unique keys for each session and periodically rotates them to minimize the risk of key compromise.

5.4. Intrusion detection and prevention

Intrusion detection and prevention systems (IDPS) monitor the tracking system for signs of malicious activity, such as unauthorized access attempts and data breaches. The IDPS uses anomaly detection techniques to identify deviations from normal behavior and trigger alerts or automated responses to mitigate potential threats. The system also employs access control lists (ACLs) to restrict access to sensitive resources based on predefined rules and policies.

6.Potential Vulnerabilities

Despite the robust security mechanisms implemented in the tracking system, several potential vulnerabilities must be considered:

6.1. BLE spoofing and man-in-the-middle attacks

BLE spoofing occurs when an attacker impersonates a legitimate IoT device to intercept or manipulate data transmitted between the device and the mobile application. Man-in-the-middle (MITM) attacks involve intercepting communication between two parties to eavesdrop or alter the data. These attacks can be mitigated using BLE pairing with strong encryption and regularly updating device firmware to address known vulnerabilities.

6.2.Data breaches and unauthorized access

Data breaches and unauthorized access can occur if the cloud server or mobile application is compromised. To mitigate these risks, the system employs encryption, secure key management, and access controls to protect sensitive data. Regular security audits and penetration testing are also conducted to identify and address potential vulnerabilities.

6.3.Privacy concerns

Privacy concerns arise when sensitive data, such as location information and personal identifiers, is collected and stored without user consent. The tracking system addresses these concerns by implementing data minimization principles, obtaining explicit user consent for data collection, and providing transparency about data usage practices.

7.Recommendations for Enhancing Security

To further enhance the security of BLE and IoT-based tracking systems, the following recommendations are proposed:

7.1. Use of hardware security modules (HSMs)

Hardware Security Modules (HSMs) provide an additional layer of security by protecting cryptographic keys and performing sensitive operations in a secure environment. Integrating HSMs into the tracking system can enhance key management and reduce the risk of key compromise.

7.2. Regular firmware and software updates

Regular updates to device firmware and application software are essential for addressing newly discovered vulnerabilities and enhancing security features. The tracking system should implement automatic update mechanisms to ensure that all components remain up-to-date with the latest security patches.

7.3. Implementing advanced threat detection techniques

Advanced threat detection techniques, such as machine learning-based anomaly detection and behavior analysis, can improve the system's ability to identify and respond to emerging threats. These techniques can be integrated into the IDPS to enhance its detection capabilities and reduce the likelihood of false positives.

8. Conclusions

Secure tracking using BLE and IoT in mobile applications presents a powerful solution for real-time monitoring and management of assets. However, the widespread adoption of these technologies also introduces significant security challenges. This paper has presented a comprehensive overview of the system architecture, communication protocols, and security mechanisms required to implement a secure tracking system. By addressing potential vulnerabilities and adopting best practices, organizations can ensure the security and reliability of their BLE and IoT-based tracking systems, thereby protecting sensitive data and maintaining user trust.

9. References

1. Bluetooth Special Interest Group (SIG). Bluetooth Core Specification Version 5.2.
2. Cybersecurity and Infrastructure Security Agency (CISA). Securing IoT Devices: Defending Against IoT-Based Attacks.
3. National Institute of Standards and Technology (NIST). Guide to Bluetooth Security.
4. IBM Security. Cost of a Data Breach Report 2022.
5. Accenture. The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study.
6. Kuneva M, Risteska A (2018) Bluetooth Low Energy: An Emerging Technology for Smart Home Devices. IEEE Communications Magazine.
7. Zhang X, Liu L. (2019) IoT Security: Challenges, Solutions, and Future Directions. IEEE Internet of Things Journal.
8. Al-Fuqaha A (2015) Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials.
9. Raza S, Wallgren L, Voigt T (2013) SVELTE: Real-Time Intrusion Detection in the Internet of Things. Ad Hoc Networks.
10. Kumar S, Zeadally S (2020) Securing the Internet of Things: A Survey. IEEE Internet of Things Journal.
11. Wang P (2010) A Survey of Security Issues in Wireless Sensor Networks. IEEE Communications Surveys & Tutorials.
12. Miorandi D, Sicari S, De Pellegrini F, et al. (2012) Internet of Things: Vision, Applications, and Research Challenges. Ad Hoc Networks.
13. Hameed S, Iqbal S (2019) Security in Internet of Things: Issues, Challenges, and Solutions. IEEE Sensors Journal.
14. Han G (2016) A Survey of Intrusion Detection Techniques in Cloud Computing. IEEE Access.
15. Ayub N, Afzal S (2020) Blockchain for Secure IoT Systems: A Survey. IEEE Internet of Things Journal.
16. Granjal J, Monteiro E, Silva J (2015) Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials.
17. Roman R, Najera P, Lopez J (2011) Securing the Internet of Things. IEEE Computer.
18. Atzori L, Iera A, Morabito G (2010) The Internet of Things: A Survey. Computer Networks.
19. Sicari S (2015) Security, Privacy, and Trust in Internet of Things: The Road Ahead. Computer Networks.
20. Yang Y, Wu L, Yin G, et al. (2017) A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal.
21. Zhang W, Wang Y (2019) Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control." IEEE Internet of Things Journal.
22. Sun H (2019) A Comprehensive Survey of the Security and Privacy Challenges in Wireless Body Area Networks. Sensors.

23. Zhang J (2020) Lightweight Security and Privacy Preserving Scheme for Smart Healthcare System. IEEE Internet of Things Journal.
24. Sun Y (2018) An Efficient Privacy-Preserving Scheme for Internet of Things Based Healthcare System. Journal of Medical Systems.
25. Fernandez-Carames TM, Fraga-Lamas P (2018) A Review on the Use of Blockchain for the Internet of Things. IEEE Access.
26. Chen Y (2020) Security and Privacy for Healthcare IoT: A Survey. IEEE Internet of Things Journal.
27. Li X (2016) A Comprehensive Survey on Privacy Preserving Data Mining. IEEE Access.
28. Abomhara M, Koien GM (2014) Security and Privacy in the Internet of Things: Current Status and Open Issues. International Journal of Computer Networks & Communications.
29. Lin J (2017) A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal.
30. Reyna A (2018) On Blockchain and Its Integration with IoT. Challenges and Opportunities. Future Generation Computer Systems.