EMPIRICAL-STUDY-BASED ANALYSIS OF TRUE-PASS SYSTEM

Manish Singh, *Naman Sharma, Rahul, and Romanchit

Lovely Professional University, Phagwara, Punjab, India

Abstract

The development of smart campuses has made it possible to combine technologies with intelligent identification and presence tracking solutions to enhance safety, attendance control and operational efficiency in residential and non-residential educational institutions. This review paper represents an empirical-study-based analysis of the True-Pass system. The smart ID-card framework incorporates Near Field Communication (NFC), Ultra-Wideband (UWB), Bluetooth Low Energy (BLE 5.2), and Radio Frequency Identification (RFID) technologies to automate presence detection and improve campus safety. The system is created to overcome the shortcomings of the current attendance roll-call in hostels and security systems for entry and exit of the students, especially in residential academic settings where real-time surveillance, privacy protection, and restricted mobility of students to grey areas are essential. This paper aims to display all available empirical evidence about smart ID-based tracking systems and their applicability to enhance presence checks, geofencing-based attendance, and emergency response characteristics. The suggested True-Pass architecture integrates the IoT-based sensing modules, embedded with a microcontroller unit, a secured backend infrastructure, and geospatial analysis to provide automated attendance recording and smart movement tracking. The system ushers in a multi-layered tracking approach whereby the BLE and UWB technologies are used for proximity-based localization, while NFC and RFID are used for identity authentication and synchronization of data. The integration provides opportunity to monitor all users dynamically in safe zones and restricted areas and provide feedback to the authorities with automated alerts in case of illegal movement, restricted movement, trespassing or absence. The study finds that the True-Pass system is a promising work towards future campus management systems. Through the integration of multi-protocol wireless communication, automated geofencing and safe IoT architecture, the system offers a scalable and effective solution to the automation of attendance and safety surveillance.

Keywords: *Smart Campus, Internet of Things, True-Pass, Near Field Communication, Ultra-Wideband, Bluetooth Low Energy, Radio Frequency Identification, Geofencing, Presence Tracking*

I. INTRODUCTION

As the world is entering Industry 5.0 with a steep-paced development of intelligent technologies, the usage of Internet of Things (IoT)-based solutions has profoundly changed the landscape of managing educational establishments [Gubbi et al., 2013]. Colleges and residential campuses have been struggling with constant problems of tracking the presence of students, safety of students in the hostels, and efficiency in operations without reducing the personal privacy of any student.

The classic systems of attendance—where attendance is recorded manually, authenticated biometrically, or by a static RFID tag—have been noted to be constrained by limitations such as non-real-time monitoring, administration overhead, and susceptibility to proxy attendance [Want, 2006; Bhattacharya et al., 2010]. This necessitates the development of more intelligent and adaptive solutions that can offer accurate, automated, and secure presence tracking.

The new possibilities of intelligent identification systems have been realized by recent advances in wireless communication technologies, including Near Field Communication (NFC), Ultra-Wideband (UWB), Bluetooth Low Energy (BLE), and Radio Frequency Identification (RFID) [Liu et al., 2007]. All these technologies have distinct benefits: NFC provides secure authentication over short distances, RFID enables efficient identification, BLE supports low-power proximity-sensing, and UWB provides high-precision localization [Alarifi et al., 2016; Zafari et al., 2019]. The majority of current implementations, however, use a single technology, which restricts their accuracy, reliability, and scalability [Brena et al., 2017]. The combination of various communication standards in a single smart identification system can greatly enhance performance and provide high-tech opportunities like automated geofencing, real-time tracking, and emergency alerting.

Empirical assessment of multi-technology smart ID systems requires analysis across many dimensions, such as localization accuracy, energy consumption, scalability, user acceptance, and privacy compliance [Al-Fuqaha et al., 2015; Perera et al., 2014]. The current review synthesizes empirical observations of such systems, specifically hybrid wireless tracking systems like the True-Pass framework. Through the analysis of performance metrics and deployment factors, the review pinpoints the realistic viability of introducing smart ID-based presence management systems in large-scale campus settings.

The paper is structured as follows. Section 2 provides the background and motivation of smart ID-based tracking systems. Section 3 outlines how the review was conducted. Section 4 presents the findings and discussion of the empirical results. Section 5 gives the conclusion of the paper and sets the future direction of research.

Corresponding author: naman.sharma231@lpu.in

II. LITERATURE REVIEW

The creation of intelligent identification and tracking systems has become a topic of great interest over the last several years, especially in smart campuses, IoT-powered attendance control, and real-time safety surveillance [L. P. University, 2025]. This literature review synthesizes empirical research pertaining to multi-technology smart ID systems analogous to the proposed TruePass framework.

A. RFID-Based Attendance and Tracking Systems

The initial smart campus attendance systems were mainly based on RFID technology because of its low cost and ease of implementation. RFID-based solutions automate attendance recording by sensing card proximity to readers mounted at entry points. These systems, however, have limitations such as short range and inability to provide continuous tracking [Want, 2006]. Bhattacharya et al. (2010) showed that RFID-based attendance systems improved administrative efficiency but failed to offer real-time monitoring. Similarly, Kamaruddin et al. (2013) adopted RFID-based campus attendance and observed issues with scalability and proxy detection. These restrictions prompted researchers to examine hybrid wireless methods integrating RFID with other technologies.

B. Bluetooth Low Energy (BLE)-Based Proximity Tracking

BLE technology was introduced as a low-power solution for indoor localization and proximity detection. Faragher and Harle (2015) explored the use of BLE beacons in indoor positioning, finding them more flexible compared to RFID systems. Subhan et al. (2011) applied BLE-based indoor tracking and reported moderate localization accuracy in closed environments. Zafari et al. (2019) conducted a comprehensive review of indoor positioning technologies and determined that BLE has potential as a cost-effective deployment in smart campuses. Sadowski and Spachos (2018) investigated BLE-based attendance automation systems, emphasizing energy efficiency and scalability. Despite these benefits, BLE-based systems are often affected by fluctuating signal quality, motivating the combination of UWB with BLE to achieve more accurate positioning.

C. Ultra-Wideband (UWB) for High-Precision Localization

UWB technology offers high-resolution indoor positioning and is common in safety-critical tracking applications. Alarifi et al. (2016) carried out a survey of UWB localization methods, proving centimeter-level accuracy indoors. Zwirello et al. (2012) compared UWB to real-time tracking and found it more precise compared to Wi-Fi and BLE. Nonetheless, UWB systems have higher infrastructure costs, promoting hybrid systems that combine BLE and UWB.

D. Hybrid Wireless Tracking Architectures (WTAs)

Hybrid tracking systems combine several technologies to enhance reliability and accuracy. He and Chan (2016) presented a hybrid localization system based on BLE and Wi-Fi, achieving better performance than single-technology systems. Yassin et al. (2017) compared hybrid indoor localization methods and highlighted the advantages of combining numerous wireless signals. Chawla and Ha (2018) explored hybrid RFID and BLE systems, achieving better attendance automation and reduced false detection. Brena et al. (2017) studied sensor fusion methods of indoor positioning and found that multi-protocol systems are highly effective. The TruePass architecture is conceptually based on these hybrid approaches.

E. IoT-Based Smart Campus Management Systems

IoT integration allows smart campus applications to be centrally monitored with advanced analytics. Gubbi et al. (2013) discussed IoT architectures in smart environments with focus on real-time data processing. Al-Fuqaha et al. (2015) examined IoT communication protocols and their use in scalable tracking systems. Perera et al. (2014) studied IoT middleware for smart environment management. Such studies affirm the applicability of IoT infrastructure in multi-technology tracking.

F. Privacy and Security in Tracking Systems

Privacy is a major concern in real-time monitoring applications. Roman et al. (2013) addressed security issues in IoT-based tracking, while Sicari et al. (2015) studied privacy-preserving systems in smart environments. These studies highlight the importance of encrypted communication and role-based access control in smart ID deployments.

G. Summary of Literature Findings

- RFID systems offer minimal identification and limited tracking.
- BLE provides proximity detection over low power.
- UWB provides high-precision localization.
- Hybrid architectures enhance accuracy and reliability.
- IoT architecture promotes scalability.
- Privacy controls must be deployed.

All these findings support the multi-technology design of the TruePass system.

III. METHODOLOGY FOR REVIEW

The present review paper utilizes a structured empirical review approach to examine smart identification and tracking systems in the context of the proposed True-Pass system [Bahl and Padmanabhan, 2000; Hightower and Borriello, 2001]. The methodology is aimed at systematically assessing the existing implementations, identifying performance metrics, and synthesizing results related to multi-technology smart ID-based presence management systems.

A. Review Design

The review is conducted using a combined qualitative and quantitative synthesis approach. The qualitative aspect examines system architectures, communication protocols, and deployment models of smart campus tracking systems. The quantitative part examines empirical performance measures including localization accuracy, response time, battery efficiency, scalability, and system reliability [Youssef and Agrawala, 2005].

B. Criteria of Inclusion and Exclusion

Included studies met the following requirements:

- Adoption of smart ID or wearable tracking systems.
- Use of wireless technologies: BLE, UWB, NFC, or RFID.
- Empirical measurement using performance measures.
- Use in educational institutions, intelligent campuses, or other controlled settings.
- System architecture and workflow description.

Studies were eliminated in case they:

- Concentrated on theoretical models without empirical proof.
- Used only GPS-based tracking without short-range wireless technologies.
- Addressed industrial monitoring unrelated to human presence tracking.
- Did not have quantifiable performance measurements.
- Offered insufficient technical information about system implementation.

C. Data Collection Strategy

The data collection procedure entailed identification of empirical research and technical applications of smart identification systems. Data were extracted from experimental reports, prototype descriptions, and performance evaluation sections of selected works. Extracted data categories included: stacked technology (BLE, UWB, NFC, RFID), embedded systems and hardware components, communication architecture, geofencing implementation methods, localization techniques, security and privacy mechanisms, power consumption characteristics, automation and user interaction, and scalability considerations [Ni et al., 2004; Liu et al., 2007].

D. Evaluation Parameters

Localization Accuracy: Defined as the degree to which the system can detect user presence in pre-defined areas. Systems combining UWB and BLE technologies are typically more precise than single-protocol systems [Alarifi et al., 2016; Zwirello et al., 2012].

Attendance Automation Efficiency: Assesses the efficiency of automated attendance tracking with geofencing, including the capability of tracking entry and exit without manual data entry [Sadowski and Spachos, 2018].

Energy Efficiency: Battery life and power consumption are critical for embedded smart ID cards. The analysis covers low-power communication protocols, duty cycling, and hardware optimization methods [Zafari et al., 2019].

System Scalability: Defined as the capacity of the system to serve large numbers of users across various tracking zones, evaluated based on distributed IoT gateways, cloud-based architectures, and edge computing solutions [Al-Fuqaha et al., 2015].

Privacy and Security: Security measures including encryption, authentication systems, and access control were audited, with special focus on end-to-end encryption and role-based access [Roman et al., 2013; Sicari et al., 2015].

Response Time: Identifies the speed of detection of movement or absence and alert generation, crucial for emergency tracking and safety applications.

E. Methodological Limitations

Although a systematic approach is taken, some limitations exist. The review is based on reported empirical data which can vary across experimental conditions and prototype implementations. Performance results can be affected by environmental conditions including building structure, signal interference, and user density. Differences in hardware setups between studies can also undermine direct comparability.

IV. RESULTS AND DISCUSSION

The following section presents synthesized empirical results regarding smart identification and tracking systems using multi-technology wireless communication protocols. Performance indicators analyzed include localization accuracy, automated attendance performance, energy consumption, scalability, privacy protection, and system responsiveness. Discussions are grounded on the proposed TruePass framework incorporating NFC, UWB, BLE 5.2, and RFID technologies [L. P. University, 2025].

A. Localization Accuracy of Multi-Technology Tracking Systems

According to empirical research, hybrid wireless tracking systems are substantially more accurate in localization than single-technology systems. RFID-only or BLE-only systems offer moderate accuracy in short-range settings, providing proximity but not precise positioning [Want, 2006; Faragher and Harle, 2015]. The addition of UWB technology enables centimeter-level localization in controlled indoor environments [Alarifi et al., 2016; Zwirello et al., 2012]. The integration of BLE and UWB in smart ID systems supports hierarchical localization: BLE offers coarse proximity detection to identify the general zone, while UWB provides fine-grained positioning for sensitive areas. Multi-anchor UWB deployments further enhance positioning accuracy, especially in dense settings like hostels and academic structures.

B. Attendance Automation Efficiency

Geofencing-based automated attendance systems show significant enhancements compared to manual and biometric systems. Empirical findings show that automated systems reduce time in attendance recording by eliminating manual roll calls and limiting proxy attendance problems [Bhattacharya et al., 2010; Kamaruddin et al., 2013]. The TruePass system leverages this approach by defining virtual attendance areas within hostel facilities. Presence is automatically registered when a student enters the specified radius, eliminating the need for physical contact.

C. Power Consumption and Battery Life

Smart ID cards require high energy efficiency and long operational lifespans. Empirical tests reveal that BLE technology offers low-power communication adequate for continuous monitoring [Zafari et al., 2019]. UWB is more power-intensive but is normally activated only when high localization accuracy is needed, minimizing overall power consumption [Zwirello et al., 2012]. Hybrid systems employ duty-cycling in which BLE is used during intermittent scanning, while UWB is activated event-driven for precision needs. Empirical evidence suggests that smart ID cards employing such techniques can achieve operational lifetimes of several months to years.

D. System Scalability in Large Campus Deployments

Smart ID tracking systems need to be scalable to serve large universities with thousands of users. Empirical evidence suggests that distributed IoT architectures enhance scalability through multiple receivers deployed across campus areas, connected to a centralized backend server [Al-Fuqaha et al., 2015; Perera et al., 2014]. Cloud-based infrastructure and edge computing minimize network latency by computing location data at the point of origin. The TruePass system incorporates IoT gateways across campus architecture with multiple geofencing areas, each with independent functionality synchronized to the central database.

E. Privacy and Security

Privacy is critical in real-time tracking system adoption. Practical applications prove that encryption and role-based access control enhance user trust and system acceptability [Roman et al., 2013; Sicari et al., 2015]. TruePass incorporates end-to-end encrypted message communication between smart ID cards, IoT receivers, and backend servers. Only authorized personnel (warden or administrator) can access location data.

F. Response Time and Emergency Alert Performance

Response time is a key performance measure for safety-oriented tracking systems. Empirical evidence demonstrates that proximity detection using BLE combined with real-time backend processing enables real-time alert generation [Chawla and Ha, 2018]. The TruePass system issues real-time notifications when users enter restricted areas or go out of bounds, enabling quick administrative response.

G. Effect on Administrative Efficiency

Empirical data show that smart ID tracking systems substantially decrease administrative workload. Automated attendance logging eliminates manual record keeping, and real-time dashboards provide immediate access to user presence data. The TruePass architecture supports administrative efficiency through centralized monitoring interfaces, enabling wardens and administrators to access real-time attendance records, movement histories, and notifications.

H. User Experience and Acceptance

User acceptance is crucial for successful system implementation. Empirical deployments demonstrate that passive smart ID tracking enhances user convenience by removing the need for active interaction [Gubbi et al., 2013]. The use of lightweight smart ID cards is more acceptable compared to wearable devices requiring frequent charging. TruePass's smart ID card design minimizes user effort since the card is automatically tracked.

I. Comparative Discussion

The empirical study shows that hybrid smart ID monitoring systems outperform single-technology solutions across multiple dimensions. Multi-technology integration enhances accuracy, reliability, and operational flexibility [Yassin et al., 2017; Brena et al., 2017]. Nonetheless, increased system complexity and higher deployment costs should be considered. Despite these drawbacks, the advantages of enhanced safety, automation, and scalability outweigh the limitations.

J. Summary of Findings

- Localization accuracy is enhanced with multi-technology tracking [Alarifi et al., 2016].
- Automated geofencing improves attendance efficiency [Sadowski and Spachos, 2018].
- Hybrid communication reduces energy consumption [Zafari et al., 2019].
- Distributed IoT architecture ensures scalability [Al-Fuqaha et al., 2015].
- Access control and encryption enhance privacy protection [Roman et al., 2013].
- Instantaneous alerting improves emergency response [Chawla and Ha, 2018].
- Automated dashboards reduce administrative overhead.
- Passive tracking enhances user acceptance.

V. CONCLUSION AND FUTURE WORK

This review article empirically investigated smart identification-based presence management systems, with a specific focus on multi-technology systems that combine Near Field Communication (NFC), Ultra-Wideband (UWB), Bluetooth Low Energy (BLE 5.2), and Radio Frequency Identification (RFID) [L. P. University, 2025]. The research examined the usefulness of hybrid wireless communication models in automated attendance control, real-time tracking, and safety monitoring in college settings.

The analysis showed that localization accuracy can be significantly enhanced with multi-technology smart ID systems combining coarse-grained and fine-grained tracking mechanisms. BLE-based geofencing provides effective zone detection, and UWB provides higher accuracy in positioning for limited or sensitive spaces. Geofencing-based automated attendance systems are more efficient, proxy-free, and less administratively burdensome.

Energy efficiency is another critical design consideration for smart ID systems. Hybrid communication models employing duty-cycling and event-activation extend battery life while maintaining continuous monitoring [Zafari et al., 2019]. Scalability testing showed that distributed IoT systems with multiple receivers and centralized backend servers can handle large campus deployments.

For future work, large-scale empirical implementations of the TruePass system in actual campuses are recommended. Machine learning-based predictive analytics could enhance anomaly detection and behavior modeling. Integration with mobile applications and emergency response systems would further improve user interaction and safety. Adaptive geofencing—where zones dynamically change based on user presence and time schedules—would enhance flexibility and reduce false alerts. Blockchain-based identity management could improve data security and auditability. In conclusion, multi-technology smart ID tracking systems represent a promising path toward next-generation campus presence management.

REFERENCES

[1] L. P. University. (2025). Smart-ID-Based Campus Presence and Safety Management System (Indian Patent No. 202511104180). Lovely Professional University, Phagwara, Punjab, India.

[2] Want, R. (2006). An introduction to RFID technology. IEEE Pervasive Computing, 5(1), 25–33.

[3] Bhattacharya, M., Nanda, P., & Patel, A. (2010). RFID-based attendance management system. Proceedings of the IEEE International Conference on Communication Systems and Network Technologies, pp. 71–74.

[4] Kamaruddin, N., Abdullah, A., & Chuprat, S. (2013). RFID-based attendance system. Procedia Engineering, 53, 358–367.

[5] Subhan, F., Hasbullah, H., Rozyyev, A., & Bakhsh, S. T. (2011). Indoor positioning using Bluetooth Low Energy. Proceedings of the IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE), pp. 218–222.

[6] Zafari, F., Gkelias, A., & Leung, K. K. (2019). A survey of indoor localization systems and technologies. IEEE Communications Surveys and Tutorials, 21(3), 2568–2599.

[7] Sadowski, S., & Spachos, P. (2018). RSSI-based indoor localization with the Internet of Things. IEEE Access, 6, 30149–30161.

[8] Alarifi, A., Al-Salman, A., Alsaleh, M., Alnafessah, A., Al-Hadhrami, S., Al-Ammar, M. A., & Al-Khalifa, H. S. (2016). Ultra wideband indoor positioning technologies: Analysis and recent advances. Sensors, 16(5), 707.

[9] Zwirello, L., Schipper, T., Harter, M., & Zwick, T. (2012). UWB localization system for indoor applications: Concept, realization and analysis. Journal of Electrical and Computer Engineering, 2012, 1–11.

[10] Yassin, A., Nasser, Y., Awad, M., Al-Dubai, A., Liu, R., Yuen, C., Raulefs, R., & Aboutanios, E. (2017). Recent advances in indoor localization: A survey on theoretical approaches and applications. IEEE Communications Surveys and Tutorials, 19(2), 1327–1346.

[11] Chawla, K., & Ha, D. S. (2018). Near real-time indoor positioning using ultra-wideband with IEEE 802.11 Wi-Fi fingerprinting and hybrid localization. IEEE Internet of Things Journal, 5(3), 1775–1785.

[12] Brena, R. F., García-Vázquez, J. P., Galván-Tejada, C. E., Muñoz-Rodriguez, D., Vargas-Rosales, C., & Fangmeyer, J. (2017). Evolution of indoor positioning technologies: A survey. Journal of Sensors, 2017, 1–21.

[13] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660.

[14] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys and Tutorials, 17(4), 2347–2376.

[15] Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context aware computing for the Internet of Things: A survey. IEEE Communications Surveys and Tutorials, 16(1), 414–454.

[16] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. Computer Networks, 57(10), 2266–2279.

[17] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

[18] Liu, H., Darabi, H., Banerjee, P., & Liu, J. (2007). Survey of wireless indoor positioning techniques and systems. IEEE Transactions on Systems, Man, and Cybernetics, Part C, 37(6), 1067–1080.

[19] Youssef, M., & Agrawala, A. (2005). The Horus WLAN location determination system. Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services (MobiSys), pp. 205–218.

[20] Hightower, J., & Borriello, G. (2001). Location systems for ubiquitous computing. IEEE Computer, 34(8), 57–66.

[21] Ni, L. M., Liu, Y., Lau, Y. C., & Patil, A. P. (2004). LANDMARC: Indoor location sensing using active RFID. Wireless Networks, 10(6), 701–710.

[22] Bahl, P., & Padmanabhan, V. N. (2000). RADAR: An in-building RF-based user location and tracking system. Proceedings of the IEEE INFOCOM, 2, 775–784.

[23] Faragher, R., & Harle, R. (2015). Location fingerprinting with Bluetooth Low Energy beacons. IEEE Journal on Selected Areas in Communications, 33(11), 2418–2428.

[24] He, S., & Chan, S. H. G. (2016). Wi-Fi fingerprint-based indoor positioning: Recent advances and comparisons. IEEE Communications Surveys and Tutorials, 18(1), 466–490.