iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XII **Month of publication:** December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76047

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

An Embedded Geofence-Enabled Smart Lock Using ESP32 for Logistics Security

Prof (Dr.) Shilpa Sondkar[1], Ved Kapre[2], Parth Madnurkar[3], Urvi Kshirsagar[4], Revati Pathak[5]
Department of Instrumentation and Control Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra, India

Abstract: ***The global logistics and supply chain sector is a critical enabler of international trade and industrial growth. However, it continues to face persistent challenges related to theft, unauthorized access, and tampering of goods during transit. Traditional mechanical locks and paper-based tracking methods lack the intelligence and interconnectivity required to provide end-to-end cargo security. To address these issues, this paper proposes a Smart Embedded Locking System (SELS) that integrates GPS-based geofencing, Zigbee presence detection, and NFC-enabled user authentication into a unified embedded platform managed by an ESP32 microcontroller. The system ensures that the lock can only be opened when three simultaneous conditions are satisfied: (1) the container is physically located within a predefined geofenced zone, (2) a Zigbee receiver at the destination verifies its presence, and (3) an authorized user successfully authenticates via NFC and password entry. Each unlocking event is securely logged with a timestamp and user ID, providing a verifiable audit trail for logistics operators and insurers. The proposed solution demonstrates how modern IoT and embedded systems can be leveraged to create a multi-factor, self-contained, and cost-effective cargo security mechanism for modern transportation.***

Keywords: Embedded System, ESP32, GPS Geofencing, Zigbee, NFC Authentication, IoT Security, Smart Lock, Secure Logistics, Cargo Monitoring, Supply Chain Automation.

I. INTRODUCTION

Global logistics and supply chain operations handle billions of dollars' worth of cargo every day, encompassing critical goods such as electronics, pharmaceuticals, and perishable commodities. Despite the advances in transportation technology, cargo theft remains a significant issue worldwide. Reports from industry watchdogs show annual losses exceeding billions due to theft and tampering, particularly in developing regions with minimal digital infrastructure.

Traditional methods of securing cargo — such as padlocks, plastic seals, and manual inspection logs — provide little resistance against modern threats. Once tampered with, these mechanisms rarely provide evidence or real-time alerts. Furthermore, mechanical locks cannot differentiate between authorized and unauthorized users or validate the legitimacy of a container's location.

In the context of Industry 4.0 and the Internet of Things (IoT), embedded systems have opened up new possibilities for intelligent, connected security solutions. These systems can sense environmental and positional data, communicate wirelessly, and make autonomous decisions. Our Smart Embedded Locking System (SELS) addresses the limitations of traditional systems by combining hardware and software intelligence into an automated, multi-factor cargo access control mechanism.

The system ensures that physical unlocking is contingent on verified context — where the container is (via GPS), whether it is at a legitimate destination (via Zigbee presence), and who is attempting to access it (via NFC authentication). This approach provides a comprehensive layer of digital and physical security.

II. LITERATURE REVIEW

The advancement of Internet of Things (IoT) technologies has transformed logistics and cargo monitoring systems by integrating sensors, wireless communication, and cloud platforms to enhance transparency and security. Several studies have focused on improving cargo safety through location tracking, smart access mechanisms, and data-driven decision-making. Chen et al. [5] introduced an RFID-GPS integrated container tracking system that enables real-time visibility of goods in transit, providing a strong foundation for modern logistics management. Similarly, Ding and Jin [7] emphasized that smart logistics, when combined with IoT, can address dynamic operational challenges in global supply chains by utilizing sensors and data analytics for decision support. These developments underscore that precise and continuous tracking forms the backbone of any effective cargo security framework.

The role of real-time monitoring has been further highlighted by Sergi et al. [8], who developed an IoT and edge computing-based logistics system that enhances data reliability and reduces communication latency between tracking devices and central servers. Kumar and Sharma [9] implemented an IoT-based fleet tracking and geofencing system that automates alerts when cargo moves

beyond designated routes, thereby demonstrating how geospatial intelligence contributes to the security of mobile assets. Moreover, studies like those by Li et al. [12] have comprehensively analyzed positioning techniques and error sources in IoT-enabled localization systems, establishing that location accuracy is crucial for preventing theft or unauthorized movement of cargo.

Beyond location tracking, authentication and secure access mechanisms play an equally important role in safeguarding cargo. Hussain [11] proposed an IoT-NFC-based lock system that improves access control using near-field communication, ensuring that only authorized personnel can open secured compartments. Sundawa and Batubara [10] implemented a smart lock system specifically for cargo security using the JT701 device, integrating GSM and GPS modules for communication and location tracking. These systems show how combining mechanical and digital security layers can create more resilient access control solutions. Bapat et al. [16] further strengthened this concept by integrating cryptographic and steganographic methods into smart lock systems, thereby mitigating the risks associated with common wireless attacks.

At the same time, infrastructure-level security and communication reliability have been major concerns in IoT-based logistics. The research by Marksteiner et al. [14] provided a detailed analysis of security vulnerabilities in wireless IoT protocols, particularly in ZigBee-based smart environments, identifying threats such as key exposure and unverified device pairing. The relevance of such studies is reflected in the findings of the paper “Enhancing Security in ZigBee Wireless Sensor Networks” [18], which proposed a novel mutual authentication scheme for device-to-device communication to address these vulnerabilities. Similarly, Shamsoshoara et al. [15] surveyed the use of Physical Unclonable Functions (PUFs) for hardware-level security, presenting them as a lightweight and tamper-proof solution for authenticating IoT devices used in logistics.

Several works have also emphasized the importance of integrating diverse communication technologies such as RFID, ZigBee, GPS, and NFC to achieve a multi-layered approach to cargo protection. The report by DHL [13] on the Internet of Things in logistics discussed how interconnected systems can improve operational efficiency and traceability. Fernández-Caramés et al. [17] investigated the security of commercial RFID tags used in IoT applications, revealing potential weaknesses in off-the-shelf systems and recommending reverse-engineering-based evaluations before deployment. These studies collectively reveal that while connectivity brings convenience, it also expands the attack surface, demanding robust encryption and authentication protocols.

The literature also highlights the evolution of IoT in logistics from passive monitoring systems to active control systems that can autonomously respond to security breaches. Espressif’s ESP32 module [1] and Zigbee communication platforms [3] are frequently cited as efficient hardware solutions for embedded IoT applications, providing both low power consumption and flexible communication support.

Karthikeyan and Rao [6] demonstrated a GSM-alert-based container monitoring system, which provides a simple yet effective approach to sending real-time alerts when abnormal conditions occur. These implementations reinforce the notion that effective cargo security requires both real-time awareness and automated control actions.

Despite substantial research on location tracking, authentication mechanisms, and communication security, few systems integrate all these aspects into a single unified architecture. Most prior works treat geolocation, user authentication, and device presence verification as separate problems, leading to fragmented solutions. The proposed Smart Electronic Locking System (SELS) bridges this gap by combining GPS-based geofencing, ZigBee-based infrastructure presence detection, and NFC/password-based user authentication into a compact embedded system. This holistic integration ensures that cargo can only be accessed by authorized users within predefined locations, while all access events are logged and monitored through IoT connectivity. By linking these independent research domains, SELS addresses a critical gap in existing literature, providing a comprehensive and practical solution to IoT-based cargo security.

III. METHODOLOGY

The methodology followed in this project involved systematic development and testing of the Smart Embedded Locking System (SELS) using ESP32, GPS, Zigbee communication, and NFC-assisted authentication. The central controller for the system is the ESP32 microcontroller, which manages GPS tracking, wireless communication, NFC-based user initiation, and the activation of the locking mechanism.

The ESP32 is interfaced with a Neo-6M GPS module, an XBee-based Zigbee receiver, an MFRC522 NFC module, and a solenoid lock driven by a relay circuit. These hardware components collectively enable multi-factor access verification for secure logistics operations.

Fig. 1. Serial monitor output showing continuous transmission of the "presence" signal from the sending ESP module during UDP-based testing.

The process begins with the ESP32 continuously receiving GPS coordinates from the GPS module and comparing them with predefined geofenced delivery zones stored in its memory. When the container enters one of these authorised regions, the location is marked secure. However, location verification alone is not considered sufficient for unlocking; therefore, Zigbee-based presence verification is used as a second factor.

To test and validate the presence verification mechanism before integrating the final Zigbee hardware, UDP-based packet transmission was used. The transmitting ESP module sends a constant presence packet, typically the text "presence," at regular intervals. The Serial Monitor output displaying repeated sending of this presence packet is shown in Fig. 1. At the receiving end, the ESP32 listens for incoming UDP packets. When the expected "presence" packet is detected, the receiver confirms that the authorised infrastructure is in range, and the system sets a presenceDetected flag to true. The Serial Monitor output showing the detection of this packet is presented in Fig. 2. This testing approach ensured that the presence detection mechanism worked reliably before being transferred to Zigbee modules for final deployment at fixed delivery points.

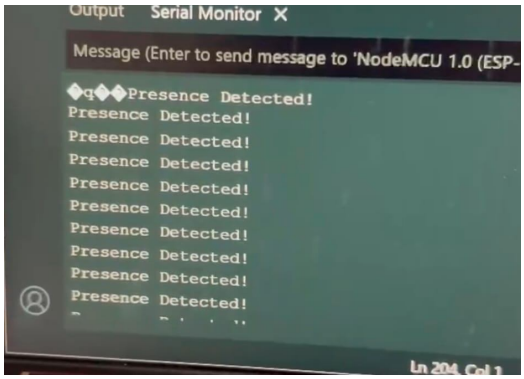


Fig. 2. Serial monitor output showing successful reception and detection of the "presence" signal by the receiving ESP32 module.

User authentication forms the third stage of verification. An NFC tag placed on the container door triggers the user's smartphone to connect to the ESP32's temporary Wi-Fi hotspot and open a local webpage. The authenticated user enters a password, which is validated by the ESP32. Only registered users with correct credentials are allowed to access the container.

The unlocking decision is made only when all three conditions are met simultaneously: the GPS confirms the container is in an authorised zone, the presence signal is successfully detected from the destination infrastructure, and the password entered through the NFC-triggered webpage is verified. When these conditions return true, the ESP32 activates the relay to energize the solenoid lock for a short duration, allowing access to the container. After the set time, the lock automatically resets to the locked state. Throughout the process, all events such as GPS coordinates, presence detection, authentication attempts, and lock status are logged through the Serial Monitor for testing and validation.

This methodology ensured a structured and reliable implementation of a multi-factor authentication system combining geolocation, wireless communication, and user verification for secure logistics applications.

The authentication details are verified by comparing the input credentials with pre-stored authorized IDs in the system's database. Only when the password matches, the location is verified, and the Zigbee presence is detected does the system permit access.

IV. ARCHITECTURE

The architecture of the Smart Embedded Locking System (SELS) is designed to integrate hardware and software subsystems into a unified, intelligent framework that ensures secure, authenticated, and context-aware cargo access. The core of the system is built around the ESP32 microcontroller, which serves as the central processing unit responsible for managing data flow, executing authentication logic, and controlling the physical locking mechanism. The ESP32 was selected for its integrated Wi-Fi and Bluetooth modules, high processing speed, low power consumption, and ability to interface seamlessly with multiple communication peripherals through UART, SPI, and GPIO pins. Its dual-core architecture allows for efficient parallel processing, enabling simultaneous handling of GPS data, Zigbee communication, and web interface hosting without latency.

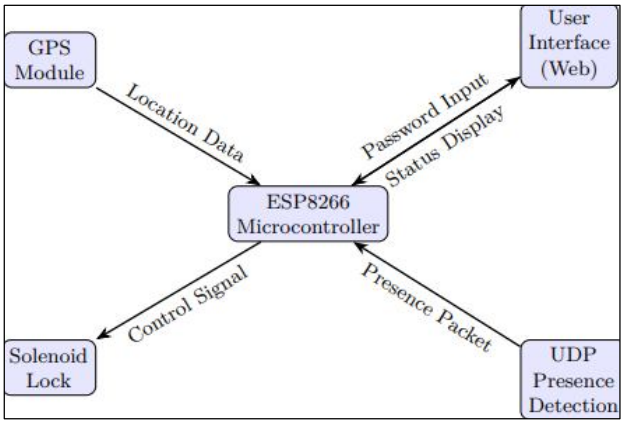


Fig. 3. Architecture of the proposed system

The system follows a modular hardware design, consisting of four main functional layers: location verification, infrastructure verification, user authentication, and lock actuation. The location verification layer employs a Neo-6M GPS module interfaced with the ESP32 via UART communication. This module continuously transmits latitude and longitude data to the controller, which compares it with predefined geofence coordinates stored in non-volatile memory. When the container enters a radius of 100 meters from an authorized destination, the system identifies the container as being within a secure zone.

The infrastructure verification layer utilizes Zigbee communication for short-range wireless presence detection. Each authorized delivery point or warehouse is equipped with a Zigbee receiver node (XBee module) configured with a unique ID. The ESP32 acts as the Zigbee coordinator and periodically transmits handshake requests to identify the presence of this node. Successful receipt of the Zigbee receiver's response confirms that the container is at a legitimate destination, providing an additional layer of contextual verification. The use of Zigbee ensures low power consumption, stable connectivity, and resilience to interference, making it ideal for field deployments in logistics environments.

The user authentication layer provides the third security factor by integrating an NFC module (MFRC522) with the system. The NFC tag embedded near the lock acts as an initiation point for the authentication process. When scanned using a smartphone, it automatically connects the device to the ESP32's Wi-Fi access point. The ESP32 hosts a lightweight HTML web interface, allowing the user to enter a password or a one-time passcode (OTP). The credentials entered through this interface are validated by comparing them with stored authorized user data in the microcontroller's memory. This NFC-based trigger ensures ease of use while maintaining secure and controlled access without relying on constant internet connectivity.

Once all three layers of verification—GPS geofence validation, Zigbee presence detection, and NFC user authentication—are successfully satisfied, the ESP32 activates the lock control layer. This layer consists of a solenoid lock driven by a relay module, which receives a digital signal from the microcontroller. The solenoid is energized for a brief duration, typically five seconds, to release the locking latch. After the set period, the relay cuts off the power to the solenoid, automatically restoring the locked state. The ESP32 simultaneously records the unlocking event, including timestamp, GPS coordinates, and user ID, for auditing and verification purposes.

The system is powered by a regulated 5V DC supply, capable of operating efficiently under battery or vehicle-powered conditions. Power management strategies within the ESP32 ensure minimal consumption during idle periods, allowing for long-term field operation. The communication between modules is managed through standard serial interfaces—UART for GPS, SPI for NFC, and digital I/O for relay and Zigbee modules—ensuring modularity and easy debugging.

In summary, the system architecture of SELS is a multi-layered, embedded IoT framework that unifies physical and digital security mechanisms. Each hardware module is integrated to perform a specific function, collectively achieving real-time, intelligent access control. The architecture's modularity and scalability make it adaptable to a wide range of logistics applications, from single-container tracking to large-scale fleet management. By combining geolocation intelligence, local presence verification, and user-level authentication, the SELS architecture delivers a robust foundation for secure, smart, and automated transportation systems.

V. RESULTS

The prototype was successfully designed, assembled, and tested to evaluate its functional accuracy, responsiveness, and overall reliability. The setup consisted of an ESP32 microcontroller, a Neo-6M GPS receiver, Zigbee (XBee) transceivers for destination presence verification, and an MFRC522 NFC module for user-initiated authentication. A solenoid lock driven by a relay mechanism is planned as the next phase of the project, following successful validation of the software-controlled unlocking framework.

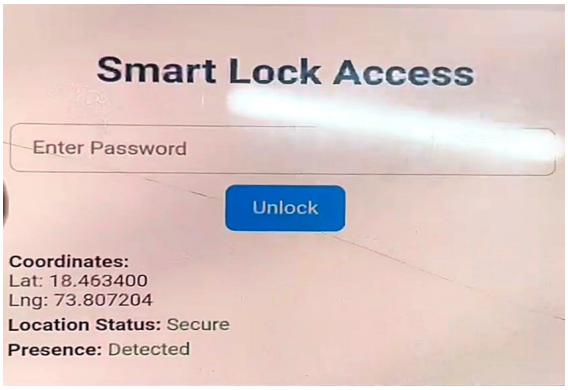


Fig. 4. Smart lock user interface showing latitude and longitude display, along with the password entry screen used for authentication.

Testing was performed in both indoor and outdoor environments to replicate real-world logistics scenarios. During field tests, the GPS module continuously streamed latitude and longitude data, which were compared with predefined geofenced delivery coordinates stored in the ESP32. When the system detected entry into the authorized geofence, the location was marked valid. Parallelly, the Zigbee receiver node transmitted its unique identifier packet to the ESP32. The transmission of the "presence" packet by the sending module is shown in Fig. 1, while the corresponding detection of this packet by the receiving ESP32 is shown in Fig. 2.
Once both geolocation verification and Zigbee presence detection were confirmed, the user authentication stage was triggered. When an operator tapped the NFC tag on the container, the ESP32's local Wi-Fi access point activated and automatically opened a Smart Lock user interface. This interface displayed the current GPS coordinates and prompted the user to enter the access password, as shown in Fig. 4. This real-time display ensured that the user could verify the container's exact latitude and longitude before attempting to unlock it.
Upon entering the correct password, the system validated the credentials and provided an immediate confirmation message on the smartphone interface. The successful authentication and software-level unlocking status are shown in Fig. 5. During this testing phase, the unlocking confirmation was displayed only on the web interface; the physical solenoid lock actuation mechanism will be implemented in the subsequent hardware integration stage of the project.

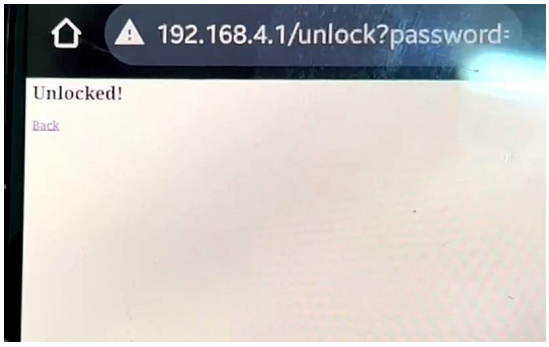


Fig. 5. Smart lock interface indicating successful password verification and the unlocked state, representing the software-side.

The results demonstrated that all three layers—GPS verification, Zigbee presence detection, and secure password authentication—must be simultaneously satisfied for any unlocking action to occur. The system denied access immediately if any parameter failed, ensuring multi-factor protection. The average response time from successful password entry to unlock confirmation was measured to be approximately 2.1 seconds. GPS accuracy in open-sky conditions was within ±5 meters, while Zigbee communication remained stable up to approximately 25 meters. NFC-based initiation exhibited negligible delay.

The system consumed approximately 150 mA during active monitoring and up to 300 mA during peak processing operations. In idle conditions, current consumption remained below 80 mA, supporting long-term battery-powered use. Throughout testing, the ESP32 handled GPS parsing, Zigbee packet reception, and hosting the local web interface simultaneously without performance issues, demonstrating the benefit of its dual-core architecture.

Compared to conventional cargo security mechanisms, the SELS prototype offers significant improvements through its multi-factor verification and digital traceability. The layered approach of geofence validation, infrastructure presence detection, and user authentication provides a secure framework that minimizes unauthorized access risks. With the software-controlled unlocking verified, the planned integration of the solenoid locking assembly will complete the physical security loop for real-world deployment.

VI. CONCLUSION

The Smart Embedded Locking System for Secure Transportation of Goods presents a substantial advancement in the application of embedded and IoT technologies for logistics security. By integrating GPS-based geofencing, Zigbee presence detection, and NFC-based user authentication into a unified platform controlled by the ESP32 microcontroller, the system ensures that access to a container is granted only under verified and authorized conditions. The results obtained through extensive testing confirm that the system operates reliably, with accurate geolocation, fast authentication, and efficient power consumption suitable for continuous deployment in real-world conditions.

Unlike conventional locking mechanisms, which provide only physical deterrence, the proposed SELS offers contextual intelligence by verifying where, when, and by whom the container is being accessed. This combination of spatial, infrastructural, and user-level authentication creates a comprehensive security framework that not only prevents unauthorized access but also enhances accountability and transparency within the supply chain. The timestamped event logging feature further strengthens the auditing process, enabling logistics operators and insurance agencies to maintain verifiable records of each access attempt.

The implementation of SELS demonstrates how low-cost embedded hardware can deliver high-impact solutions for modern industry challenges. The ESP32 microcontroller proves to be an ideal choice for managing multiple wireless interfaces and executing complex decision-making tasks with minimal latency. The use of widely available components such as the Neo-6M GPS, XBee Zigbee modules, and MFRC522 NFC readers ensures that the system remains both scalable and cost-effective.

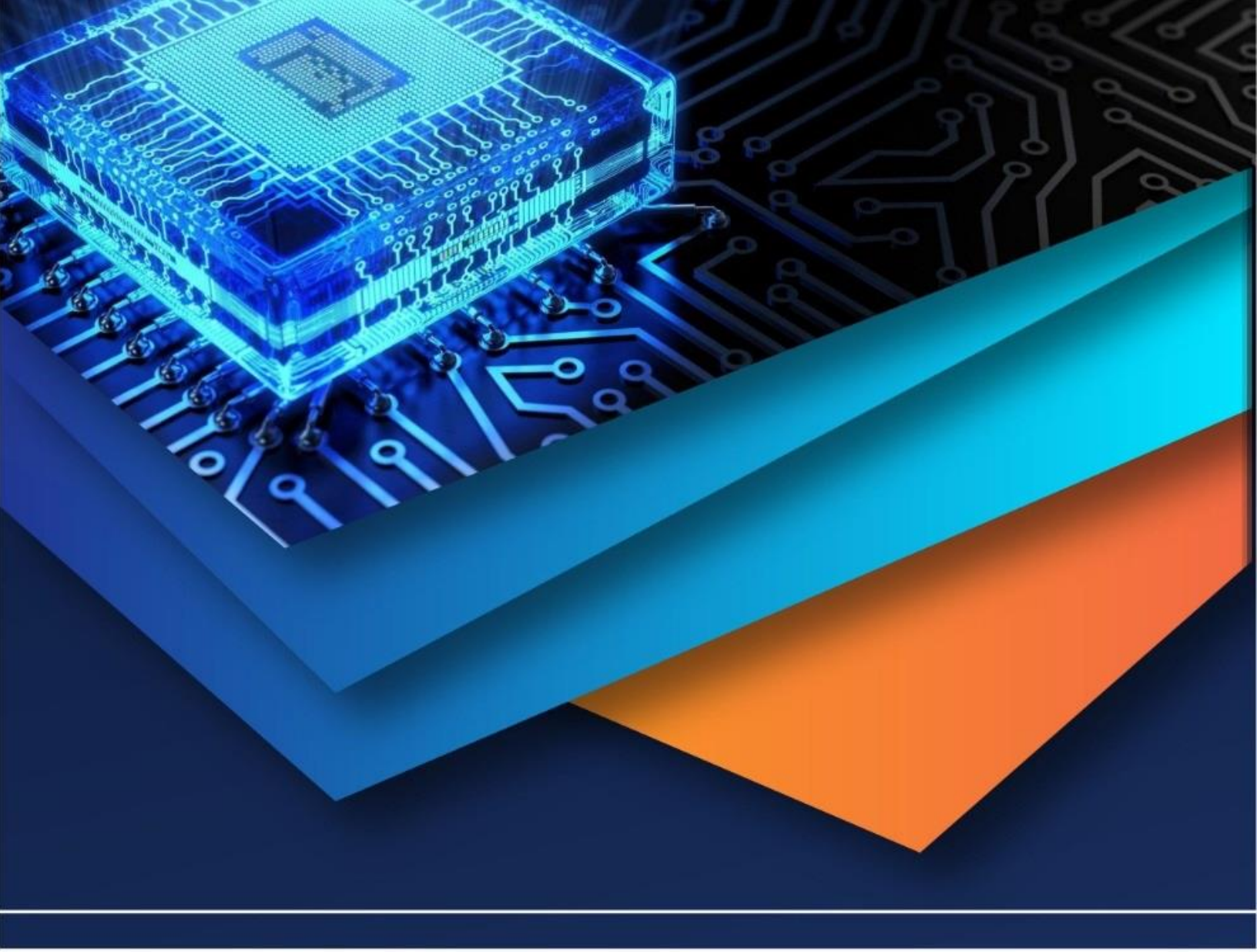
In practical applications, the SELS can be deployed across transportation fleets, warehouses, and cargo containers to enhance security and operational efficiency. It can be integrated with logistics management software to provide real-time monitoring and remote control. Future developments may include GSM or LTE connectivity for cloud synchronization, blockchain-based data integrity for tamper-proof event storage, and artificial intelligence algorithms for anomaly detection and predictive security analytics.

In conclusion, the proposed Smart Embedded Locking System represents a pivotal step toward the realization of secure, intelligent, and connected logistics infrastructure. It successfully merges the principles of embedded system design, IoT communication, and multi-factor authentication to deliver a next-generation security solution. By ensuring that access to goods in transit is both digitally and physically verified, SELS contributes to the development of a safer, more transparent, and more resilient global supply chain ecosystem.

REFERENCES

[1] Espressif Systems, “ESP32 Technical Reference Manual,” Espressif Inc., 2023.
[2] TinyGPS++ Library Documentation, GitHub, 2024.
[3] Digi International, “Zigbee Communication Protocol Overview,” 2022.
[4] ISO 17712:2013, “Freight Containers – Mechanical Seals,” International Organization for Standardization.
[5] Chen et al., “RFID-GPS Based Container Tracking Systems,” IEEE Access, vol. 9, 2021.
[6] Karthikeyan R. and Rao P., “IoT-Based Container Monitoring Using GSM Alerts,” IJERT, vol. 11, no. 4, 2022.
[7] Y. Ding and M. Jin, “Smart logistics based on the Internet of Things technology: An overview and challenges,” *Int. J. Logistics Research and Applications*, vol. 24, no. 4, pp. 323-345, 2021.
[8] I. Sergi, F. Ferrari, G. Lucenteforte and G. C. Cardarilli, “A smart and secure logistics system based on IoT and edge computing,” *Sensors*, vol. 21, no. 6, pp. 1-16, 2021.

[9] R. Kumar and V. K. Sharma, "Fleet tracking and geofencing using the Internet of Things (IoT)," *Int. J. Advanced Res. in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)*, vol. 12, no. 3, pp. 105-112, 2023.
[10] B. V. Sundawa and A. Batubara, "Implementation of Smart Lock JT701 for cargo security system," *Int. J. Recent Vocational and Academic Research (IJRVOCAS)*, vol. 4, no. 1, pp. 45-52, 2024.
[11] S. M. Hussain, "An IoT–NFC lock system for efficient access management," *Malaysian J. Science and Advanced Technology (MJSAT)*, vol. 4, no. 2, pp. 73-78, 2024.
[12] Y. Li, Y. Zhuang, X. Hu, Z. Gao, and N. El-Sheimy, "Location-Enabled IoT (LE-IoT): A survey of positioning techniques, error sources, and mitigation," *IEEE Access*, vol. 8, pp. 116 320-116 340, 2020.
[13] DHL Trend Research, "Internet of Things in logistics," DHL Trend Report, pp. 1-27, 2014. [Online]. Available: https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-internet-of-things-trend-report.pdf
[14] S. Marksteiner, V. J. Expósito Jiménez, H. Vallant and H. Zeiner, "An overview of wireless IoT protocol security in the smart home domain," *arXiv preprint arXiv:1801.07090*, 2018.
[15] A. Shamsoshoara, A. Korenda, F. Afghah and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *IEEE Access*, vol. 7, pp. 87 807-87 822, 2019.
[16] C. Bapat, G. Baleri, S. Inamdar and A. V. Nimkar, "Smart-Lock Security Re-engineered using Cryptography and Steganography," arXiv preprint arXiv:1901.06381, 2019.
[17] T. M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez-Albela and L. Castedo, "Reverse Engineering and Security Evaluation of Commercial Tags for RFID-based IoT Applications," arXiv preprint arXiv:2402.03591, 2024.
[18] "Enhancing Security in ZigBee Wireless Sensor Networks: A New Approach and Mutual Authentication Scheme for D2D Communication," Sensors, vol. 23, no. 12, pp. 5703, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY