Smart Bank Locker Access System Using AI-IoT with ESP32 CAM Enabled Multi Factor Authentication

Pabbala Priyanka[1*], N. Saipavan[2], Ambati Nikitha[2], Lenkala Rakesh[2], Poola Madhav[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Electronics & Communication Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

*Correspondence: Pabbala Priyanka (Priyanka.pabbala@gmail.com)

Abstract

The increasing need for advanced security systems in banking and high-value asset protection has intensified due to rising cyber-physical threats, with global financial fraud losses exceeding 40 billion USD annually and smart security systems projected to grow at over 16% per year. Additionally, traditional locker systems remain vulnerable to unauthorized access, identity spoofing, and delayed threat detection, necessitating intelligent and predictive security solutions. Conventional locker systems rely on single-layer authentication methods such as keys or PINs, which are prone to theft, duplication, or brute-force attacks, and lack real-time monitoring and anomaly detection capabilities. Furthermore, they do not provide immediate alerts or predictive insights, making them inefficient against modern security threats. To overcome these limitations, the proposed AI-IoT secure smart bank locker access system utilizes the ESP32 microcontroller to implement a predictive, multi-layered security framework. The system integrates fingerprint biometric authentication, keypad-based PIN verification, and ESP32-CAM facial recognition to establish a robust three-factor authentication mechanism. Upon successful validation, a DC motorized lock grants access, while LCD and buzzer modules provide real-time feedback. The AI-driven fraud detection module continuously analyzes access patterns to identify anomalies such as unusual timings or repeated failures, triggering preventive actions including system lockdown and instant alerts. IoT connectivity enables remote monitoring, real-time notifications, and data logging for enhanced security management. This intelligent system significantly enhances safety, prevents unauthorized access, and delivers a scalable, proactive solution for modern secure storage applications.

Keywords: Biometric Authentication, ESP32, Facial Recognition, Fraud Detection, Internet of Things, Multi-Factor Authentication, Predictive Security, Smart Locker System, Vault Security.

1. Introduction

The demand for advanced security systems in banking and high-value asset protection has increased significantly due to the rise in cyber-physical threats and financial fraud [1]. Recent reports indicate that global financial fraud losses exceed 40 billion USD annually, highlighting the growing vulnerability of traditional security infrastructures. At the same time, the smart security systems market is projected to grow at a rate of over 16% per year [2], driven by the adoption of Artificial Intelligence (AI) and Internet of Things (IoT) technologies. In high-security environments such as banks, financial institutions, jewelry storage facilities, and personal vaults, there is a critical need for intelligent systems capable of ensuring real-time monitoring, multi-layered authentication, and proactive threat detection to safeguard valuable assets effectively [3].

Problem Statement: Traditional locker and vault systems primarily rely on single-layer authentication mechanisms such as physical keys or PIN-based access. These methods are inherently vulnerable to security breaches [4], including key duplication, password guessing, and unauthorized access through brute-force attacks. Additionally, conventional systems lack integration with modern technologies,

resulting in no real-time monitoring, remote accessibility, or automated alert mechanisms. The absence of intelligent data analysis further limits their ability to detect suspicious behavior or prevent security threats before they occur, making them inadequate for handling modern security challenges.

Motivation: In real-time scenarios, these limitations lead to several critical security risks that compromise asset protection [5]. Unauthorized access attempts may go undetected due to the lack of continuous monitoring and anomaly detection systems. Delayed response to suspicious activities increases the chances of theft or fraud [6]. Moreover, single-factor authentication systems fail to verify user identity comprehensively, making them susceptible to identity spoofing and credential theft. The absence of instant alerts and predictive analysis prevents timely intervention and reduces overall system reliability [7]. These challenges emphasize the need for an intelligent, AI-IoT-based security solution that incorporates multi-layered authentication, real-time monitoring, and predictive threat detection to ensure enhanced safety, rapid response, and robust protection for high-value assets.

2. Literature Survey

Rouchdi et al. [7] proposed a new Radio Frequency Identification (RFID) middleware integrated with the BagTrac application for efficient tracking and management of items in transport systems. Haibi et al. [8] proposed an RFID-based luggage tracking system for aerial transport that enabled real-time monitoring of baggage movement across different checkpoints.

Kisic et al. [9] proposed the design and simulation of a 13.56 MHz RFID tag using ink-jet printing technology for cost-effective manufacturing. The system focused on flexible and low-cost tag fabrication techniques. Good et al. [10] proposed a low-frequency RFID system addressing security and privacy concerns by analyzing vulnerabilities and proposing secure communication mechanisms. The system enhanced data protection through improved authentication strategies.

Haibi et al. [11] proposed a compact dual-band Ultra High Frequency (UHF) RFID tag antenna with adapted middleware for transport and supply chain management applications. Turner et al. [12] proposed a bi-directional RFID-based Application-Specific Integrated Circuit (ASIC) that interfaced with Serial Peripheral Interface (SPI) bus peripherals for efficient communication.

Lee et al. [13] proposed an RFID-based recursive process mining system for quality assurance in the garment industry that enabled tracking and analysis of production processes. Wang [14] proposed a tennis robot design using Internet of Things (IoT) and deep learning techniques for intelligent operation and performance optimization. Herrojo et al. [15] proposed a review of chipless RFID technology that analyzed recent developments and design approaches for low-cost identification systems. Ramzan et al. [16] proposed an RFID-based system for vending machines that enabled cashless transactions and automated user authentication.

Lodhi et al. [17] proposed an RFID-based smart shopping booth that automated billing and product identification through real-time tag scanning. Ahtsham et al. [18] proposed an Internet of Things (IoT)-based door-lock surveillance system that integrated cryptographic algorithms for secure access control. Orji et al. [19] proposed a microcontroller-based digital door-lock security system using keypad authentication for controlled access. Prabhakar et al. [20] proposed a password-based door-lock system that enabled secure access through user authentication mechanisms.

3. Proposed System

The proposed system as shown in Figure 1 represents an AI-IoT based smart bank locker architecture centered on the ESP32 controller, which acts as the core processing and decision-

making unit. The system integrates multiple authentication mechanisms such as fingerprint recognition, keypad-based PIN entry, and ESP32-CAM for face recognition, ensuring multi-layer security. A regulated power supply provides stable voltage to all components, while input devices send user credentials and environmental data to the ESP32. The controller processes this information using embedded software and TinyML-based intelligence to detect anomalies and control output modules such as LCD display, buzzer alerts, IoT communication, and DC door locking mechanism. The integration of sensing, processing, and communication enables real-time monitoring, intelligent decision-making, and secure cloud connectivity for enhanced locker protection.

Figure 2 shows the proposed flowchart. The detailed working procedure is given as follows:

Step 1: Power Supply Initialization: The regulated power supply unit provides a stable DC voltage (typically 5V/3.3V) to the ESP32 and all peripheral components. This ensures reliable and uninterrupted operation of the system. Proper voltage regulation and filtering protect sensitive electronics from fluctuations and noise.

Step 2: User Authentication Inputs: The system accepts multiple authentication inputs including fingerprint sensor, keypad for PIN entry, and ESP32-CAM for facial recognition. These inputs are processed by the ESP32 to verify user identity. Multi-factor authentication significantly enhances security by requiring multiple credentials before granting access.

Step 3: Data Processing and AI Analysis: The ESP32 processes all incoming data using embedded software logic and a lightweight TinyML model. It analyzes user behavior patterns, sensor inputs, and authentication results to detect anomalies or suspicious activities. This enables predictive fraud detection and proactive security measures.

Step 4: Sensor Monitoring and Event Detection: Additional sensors (such as vibration, temperature, or door status—conceptually included) continuously monitor the locker environment. Any abnormal condition, such as forced entry or unusual movement, is detected and sent to the ESP32 for immediate action.

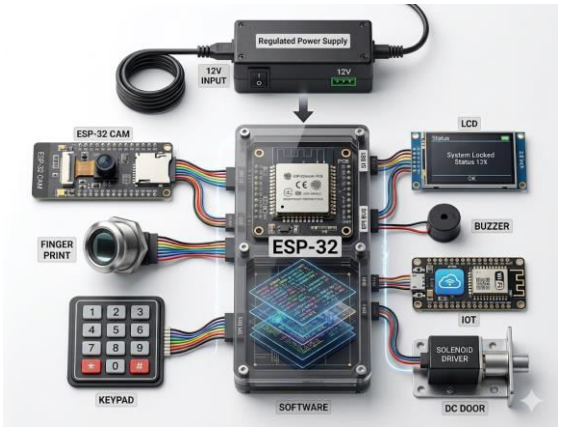

Figure 1. Block Diagram of Proposed Security System.

Step 5: Output Display and Alerts: The LCD module displays system status, authentication results, and alerts to the user. In case of unauthorized access or abnormal activity, the buzzer is activated to provide an audible warning, ensuring immediate attention.

Step 6: IoT Communication and Cloud Integration: The ESP32 uses its built-in Wi-Fi capability to transmit data securely to a cloud server via MQTT or HTTP protocols. This enables remote monitoring, event logging, and real-time alert notifications to authorized personnel through a dashboard.

Step 7: Locker Control Mechanism: Based on authentication and system conditions, the ESP32 controls the DC door lock mechanism. If access is granted, the locker opens; otherwise, it remains locked or enters a security lockout mode during suspicious events.

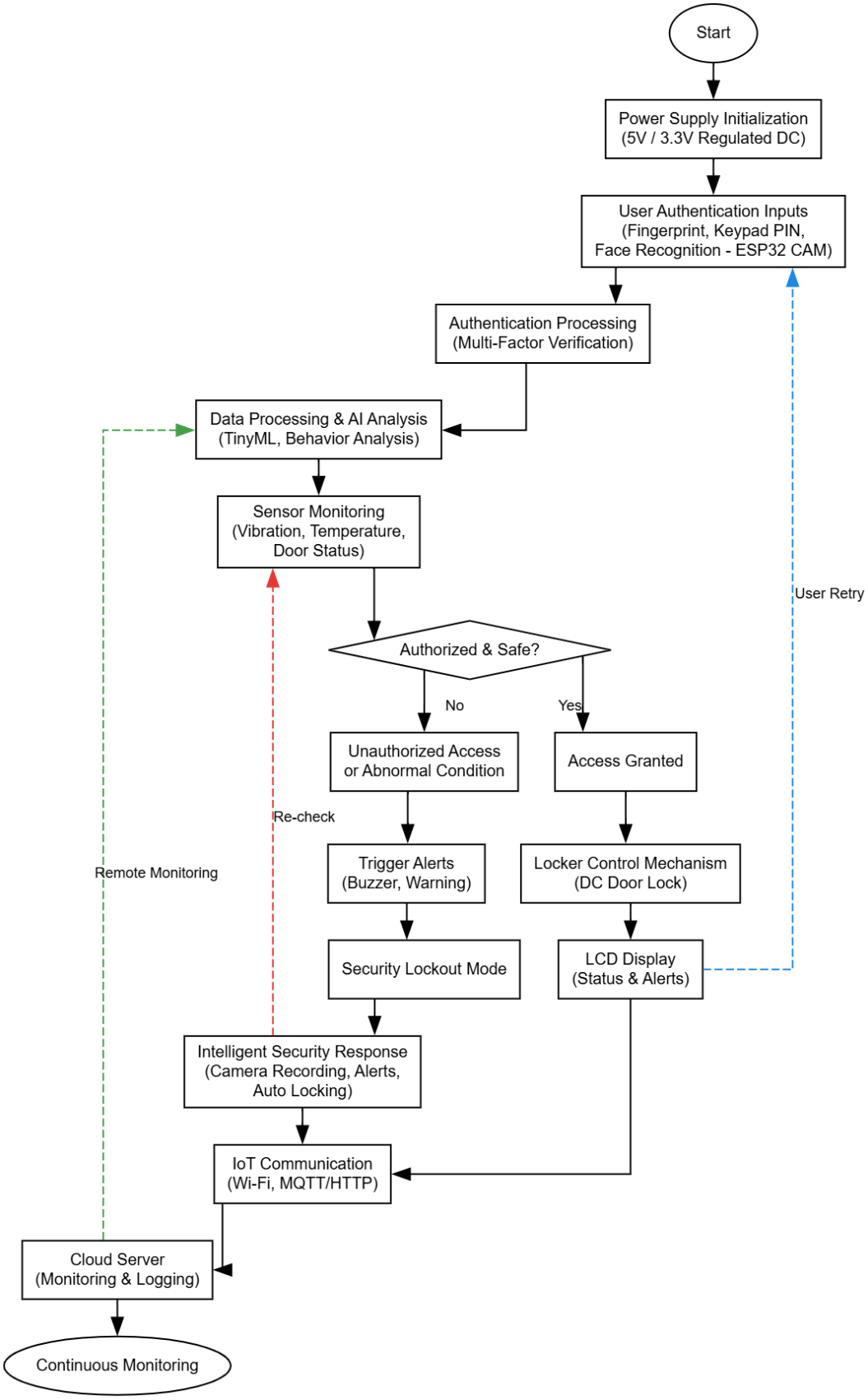

Figure 2. Proposed System Working Procedure.

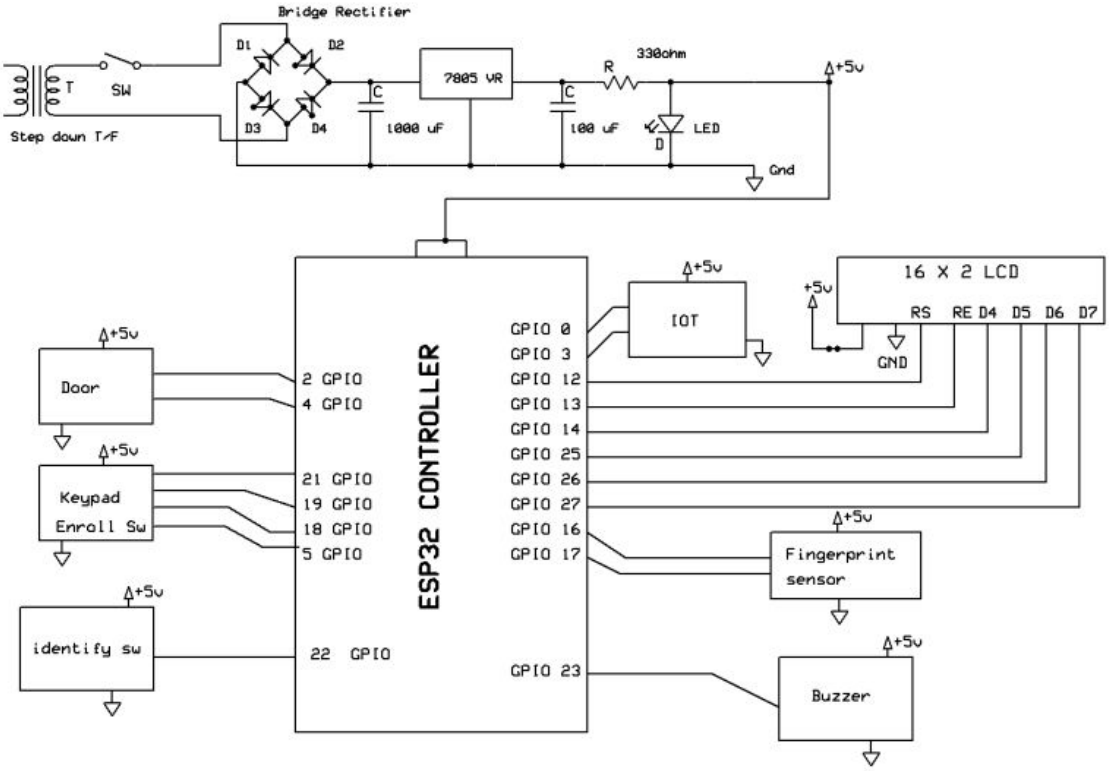

Figure 3. Schematic Diagram.

Step 8: Intelligent Security Response: In case of detected threats, the system triggers multiple responses such as locking the door, activating alarms, sending alerts to the cloud, and recording evidence through the camera module. This layered response ensures maximum protection and resilience.

Figure 3 illustrates the circuit diagram of an ESP32-based IoT smart door lock system that utilizes fingerprint authentication for secure access control. The system is powered by a regulated power supply consisting of a step-down transformer, bridge rectifier, filtering capacitors, and a 7805-voltage regulator to provide a stable +5V supply. The ESP32 microcontroller acts as the central control unit, interfacing with a fingerprint sensor for user authentication, a keypad and enrollment switch for registering new users, and an identification switch for verification operations. A door locking mechanism is connected to the controller to enable or restrict access based on authentication results. The system also includes a 16×2 LCD to display real-time status messages such as access granted or denied, and a buzzer for audible alerts during unauthorized attempts. Additionally, IoT connectivity allows remote monitoring and control of the door system, enhancing security and convenience. This integrated design provides a reliable, secure, and intelligent access control solution suitable for smart homes and security applications.

4. Results and Discussion

Figure 4 shows the complete hardware prototype of the smart bank locker security system built using the ESP-32 controller. The system integrates modules such as fingerprint sensor, ESP32-CAM for facial recognition, keypad for PIN entry, DC lock mechanism, LCD display, and buzzer for multi-layer authentication.

Figure 5 illustrates the LCD interface displaying the system startup message “Access System”, indicating that the security system is initialized and ready for user authentication through fingerprint, password, and facial recognition verification.

Figure 6 presents the IoT cloud interface used to monitor locker access activities remotely. The dashboard records authentication events such as valid fingerprint access, wrong password attempts, and facial detection results along with timestamps for real-time security monitoring and fraud detection.

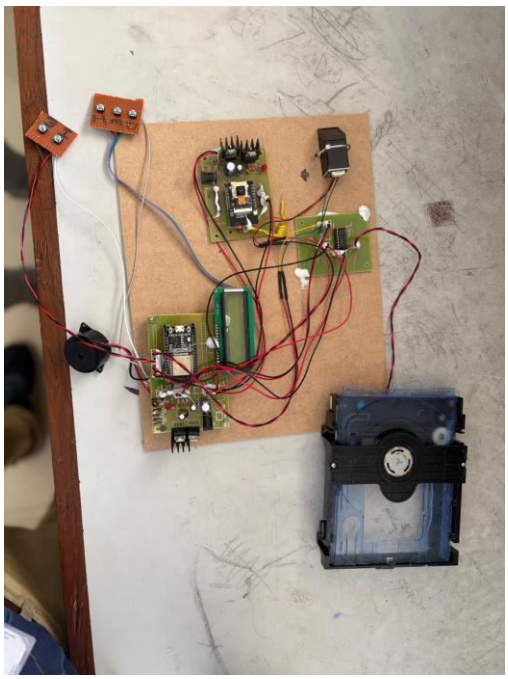

Figure 4. Hardware Implementation of AI-IoT Smart Bank Locker System.

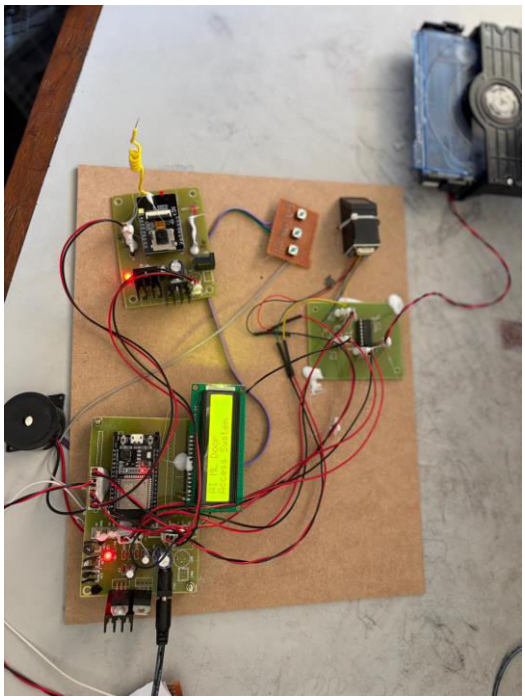

Figure 5: LCD Display Showing Access System Initialization

S.No	Status	Date
1	FP_Not_Found	2026-02-10 13:17:10
2	Fp_Valid_Pwd_Correct_Face_Det	2026-02-10 13:15:01
3	Fp_Valid_Pwd_Correct_Face_Det	2026-02-10 13:12:50
4	FP_Valid_Wrong_pwd	2026-02-10 10:52:36
5	Fp_Valid_Pwd_Correct_Face_Det	2026-01-31 12:40:13
6	FP_Valid_Wrong_pwd	2026-01-31 12:38:50
7	FP_Not_Found	2026-01-31 12:37:35

Figure 6. IoT Cloud Monitoring Dashboard for Security Logs

5. Conclusion

The proposed intelligent locker security system demonstrates a robust and advanced approach to secure storage by integrating multi-factor authentication, IoT connectivity, and AI-based anomaly detection. By combining fingerprint recognition, PIN verification, and facial recognition through the ESP32-CAM, the system ensures a high level of access control and significantly reduces the risk of unauthorized entry. The incorporation of TinyML-based data analysis enables proactive threat detection, while continuous sensor monitoring enhances situational awareness within the locker environment. Real-time alerts through LCD display, buzzer notifications, and cloud-based communication ensure immediate response to security events. Additionally, the IoT integration allows remote monitoring, data logging, and efficient management through connected platforms. The automated locker control mechanism, coupled with intelligent security responses such as alarm activation and evidence recording, provides a comprehensive and layered defense system. Finally, this solution enhances security, reliability, and user convenience, making it suitable for applications in smart homes, banking lockers, and high-security storage systems.

References

[1] Divya, R.S.; Mathew, M. Survey on various door-lock access control mechanisms. In Proceedings of the 2017 International Conference on Circuit, Power and Computing Technologies (ICCPCT), Kollam, India, 20–21 April 2017.

[2] Haibi, J.A.; Yassini, K.E.; Oufaska, K. Suitcase traceability system via RFID and NoSQL database. In Proceedings of the SCA'18: 3rd International Conference on Smart City Applications, Tetouan, Morocco, 10–11 October 2018; pp. 1–6.

[3] Gabsi, S.; Kortli, Y.; Beroulle, V.; Kieffer, Y.; Alasiry, A.; Hamdi, B. Novel ECC-based RFID mutual authentication protocol for emerging IoT applications. IEEE Access 2021, 9, 130895–130913.

[4] Khan, M.U.A.; Raad, R.; Foroughi, J.; Raheel, M.S.; Houshyar, S. An octagonal-shaped conductive HC12 and LIBERATOR-40 thread embroidered chipless RFID for general IoT applications. Sens. Actuators A Phys. 2021, 318, 112485.

[5] Agarwal, A.; Mehandiratta, E.; Sanket, R.; Samkaria, R.; Gupta, T.; Singh, R.; Gehlot, A. Smart door-lock system for elderly, handicapped people living alone. Int. J. Smart Home 2016, 10, 155–162.

[6] Haibi, A.; Oufaska, K.; El Yassini, K.; Boulmalf, M.; Bouya, M. Systematic mapping study on RFID technology. IEEE Access 2022, 10, 6363–6379.

[7] Rouchdi, Y.; Haibi, A.; El Yassini, K.; Boulmalf, M.; Oufaska, K. A New RFID Middleware and BagTrac Application. In Proceedings of the International Conference on Advanced Intelligent Systems for Sustainable Development (AI2SD'2018), Tangier, Morocco, 12–14 July 2018; pp. 869–884.

[8] Haibi, A.; Oufaska, K.; El Yassini, K. Tracking Luggage System in Aerial Transport via RFID Technology. In Proceedings of the Third International Conference on Smart City Applications, Oujda, Morocco, 10–11 October 2018; pp. 289–299.

[9] Kisic, M.; Dakic, B.; Damnjanovic, M.; Blaz, N.; Zivanov, L. Design and simulation of 13.56 MHz RFID tag in ink-jet printing technology. In Proceedings of the 36th International Spring Seminar on Electronics Technology, Alba Iulia, Romania, 8–12 May 2013.

[10] Good, T.; Benaissa, M. A low-frequency RFID to challenge security and privacy concerns. In Proceedings of the 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, China, 12–15 October 2009.

[11] Haibi, A.; Bouazza, H.; Bouya, M.; El Yassini, K.; Oufaska, K.; Boulmalf, M.; Lazaro, A.; Hadjoudja, A. A new compact metal mountable dualband UHF RFID tag antenna with an adapted middleware for transport and SCM fields. Int. J. Commun. Antenna Propag. 2021, 11, 106–117.

[12] Turner, M.; Naber, J. The design of a bi-directional, RFID-based ASIC for interfacing with SPI bus peripherals. In Proceedings of the 2010 53rd IEEE International Midwest Symposium on Circuits and Systems, Seattle, WA, USA, 1–4 August 2010.

[13] Lee, C.; Ho, G.; Choy, K.L.; Pang, G. A RFID-based recursive process mining system for quality assurance in the garment industry. Int. J. Prod. Res. 2014, 52, 4216–4233.

[14] Wang, X. Tennis robot design via Internet of Things and deep learning. IEEE Access 2021, 9, 127460–127470.

[15] Herrojo, C.; Paredes, F.; Mata-Contreras, J.; Martín, F. Chipless-RFID: A review and recent developments. Sensors 2019, 19, 3385.

[16] Ramzan, A.; Rehman, S.; Perwaiz, A. RFID technology: Beyond cash-based methods in vending machine. In Proceedings of the 2017 2nd International Conference on Control and Robotics Engineering (ICCRE), Bangkok, Thailand, 1–3 April 2017.

[17] Lodhi, E.; Fenghua, Z.; Lodhi, Z.; Saleem, Q.; Xiong, G.; Wang, F. Design and Implementation of RFID based Smart Shopping Booth. In Proceedings of the 2019 6th International Conference on Information Science and Control Engineering (ICISCE), Shanghai, China, 20–22 December 2019.

[18] Ahtsham, M.; Yan, H.Y.; Ali, U. IoT based door-lock surveillance system using cryptographic algorithms. In Proceedings of the 2019 IEEE 16th International Conference on Networking, Sensing and Control (ICNSC), Banff, AB, Canada, 9–11 May 2019.

[19] Orji, E.Z.; Nduanya, U.I.; Oleka, C.V. Microcontroller Based Digital Door-lock Security System Using Keypad. Int. J. Latest Technol. Eng. Manag. Appl. Sci. 2019, 8, 92–97.

[20] Prabhakar, A.; Oza, S.; Shrivastava, N.; Srivastava, P.; Wadhwa, G. Password Based Door-lock System. Int. Res. J. Eng. Technol. 2019, 6, 1154–1157.