PROGRESS IN ENGINEERING APPLICATION AND TECHNOLOGY
e-ISSN: 2773-5303

PEAT

Vol. 6 No. 2 (2025) 216-224
https://publisher.uthm.edu.my/periodicals/index.php/peat

IoT-Enabled Dual Authentication System Using RFID and Passcode for College Dormitories

Deeva Haren Pannirselvam[1], Mohd Hakimi Zohari[1*]

[1] *Department of Electrical Engineering Technology, Faculty of Engineering Technology, Universiti Tun Hussein Onn Malaysia, 84600, Pagoh, Johor, MALAYSIA*

*Corresponding Author: hakimi@uthm.edu.my
DOI: https://doi.org/10.30880/peat.2025.06.02.023

Article Info

Received: 26 June 2025
Accepted: 11 August 2025
Available online: 30 October 2025

Keywords

Internet of Things (IoT), Dual authentication, RFID (Radio Frequency Identification), Access control system

Abstract

This project developed an IoT-enabled dual authentication system using RFID and passcodes for university dormitory security. Conventional access control methods like mechanical locks, standalone RFID cards, or passwords alone are insufficient due to vulnerabilities such as duplicated keys, cloned cards, and compromised passwords. The proposed system integrates RFID and passcode validation using an ESP32 microcontroller, providing two-step verification for authorized residents. The system includes IoT functionality through Firebase Realtime Database to log all access attempts and failed authentications, enabling real-time monitoring. Hardware components include RFID readers, keypads, SG90 servo motors, LCD display, and buzzer for user feedback. When both authentication factors are verified, the system unlocks doors and automatically re-locks after a set period. Administrative override using master RFID card and passcode is available for lockout recovery. Testing demonstrated reliable user authentication, unauthorized entry prevention, and effective event recording. The prototype showed good usability, response speed, durability, and feedback mechanisms. The dual verification approach significantly enhances security over traditional methods and offers a scalable solution for dormitory access control. By combining secure hardware with real-time cloud integration, the system improves student safety and provides administrators with efficient monitoring tools.

1. Introduction

Security systems played a crucial role in protecting residential and institutional facilities. Access control systems, particularly door locks, evolved dramatically in recent decades to address contemporary security challenges [1]. College dormitories required specialized access control systems that differed from other accommodation types due to their unique environment of shared and private spaces housing multiple inhabitants [2].

RFID (Radio Frequency Identification) technology gained popularity in access control applications because of its speed, reliability, and contactless operation capabilities. RFID systems used electromagnetic fields to automatically identify, and track tags attached to objects or carried by individuals [3]. When combined with passcode authentication, RFID formed a two-factor authentication system that provided enhanced security solutions. IoT (Internet of Things) technologies further improved access control by enabling real-time system

monitoring, event logging, and remote administration capabilities. IoT referred to the network of physical devices embedded with sensors and software that connected and exchanged data over the internet [4].

Most existing single authentication systems, such as standalone RFID or passcode systems, proved insufficiently secure as they remained vulnerable to cloning, password leaks, and brute-force attacks. Traditional methods that relied on single authentication factors or basic mechanical locks failed to provide adequate security for student housing environments. Passcodes were easily compromised or shared among users, RFID tags could be cloned or stolen, and physical keys were frequently misplaced or duplicated. These conventional solutions lacked real-time monitoring capabilities and did not provide administrators with proper tools to track access events or respond quickly to security emergencies [5].

The main limitations of current systems included the absence of real-time control, remote monitoring capabilities, and room-specific access management. These deficiencies led to inefficiencies and potential security hazards in student accommodation areas [6]. The question remained where dual authentication systems could combine RFID and passcode technologies with IoT capabilities providing secure, monitored access control specifically designed for college dormitory environments in this setting [7].

This project aimed to develop an IoT-enabled dual authentication system that integrated RFID and passcode authentication to provide secure access control for college dormitories. The system was designed to offer real-time monitoring, event logging, and remote management capabilities while ensuring room-specific access control and enhanced privacy for students.

2. Methodology

This section presents the system design documentation for an IoT-based dual authentication access control system. The documentation includes comprehensive system architecture representations through block diagrams, operational flow analysis via flowcharts, and detailed hardware implementation through circuit schematics. These visual representations collectively illustrate the integration of RFID technology, keypad authentication, and automated control mechanisms within a cohesive security framework. The following diagrams provide systematic documentation of the system's structural components, operational procedures, and electrical connections to demonstrate the complete implementation of the dual-verification access control solution.

2.1 Materials

The main electronic components that are used in this project are ESP32. The rest are listed below in Table 1. The system implementation utilized several key electronic components to achieve dual authentication functionality. The ESP32 microcontroller served as the central processing unit, coordinating all system operations and providing Wi-Fi connectivity for IoT integration. The RFID RC522 module enabled contactless card scanning for the first authentication layer, while the 4x4 matrix keypad facilitated passcode entry for the second security level. Visual feedback was provided through the I2C LCD 20x4 display, showing system status and user prompts, complemented by a passive buzzer for audio alerts. The SG90 servo motor controlled the physical door locking mechanism, with a 5V step-down voltage regulator module ensuring stable power distribution from the 7.4V LiPo battery to all components. This combination of components created a comprehensive access control system that integrated RFID technology, keypad authentication, real-time feedback, and automated door control for enhanced dormitory security.

Table 1: List of Components Used

List of Components	
- RFID RC522	- Servo Motor SG90
- 4x4 Matrix Keypad	- 5V Step Down Voltage Regulator Module
- Passive Buzzer	- 7.4V LiPo Battery
- I2C LCD 20x4	

2.2 System Block Diagram

Figure 1 below visually depicted the block diagram consisting of the hardware architecture of the IoT-based dual verification system for authorized entrance control. The process started with an RFID token communicating wirelessly through radio waves with the RFID Reader Module, which extracted the unique numerical code stored on the RFID tag and transmitted this data to the ESP32 microcontroller for authentication. The system utilized a 4x4 keypad interface for passcode input, adding a secondary security layer where users entered their individual passcode after RFID verification. Access was granted only when both the RFID card and matching passcode corresponded to stored credentials in the system database.

The ESP32 microcontroller functioned as the central processing unit, analyzing data received from both the RFID Reader Module and keypad interface before dispatching control signals to servo motors for door unlocking. A DC-DC 5V step-down converter regulated voltage to ensure the ESP32, buzzer, and LCD display received consistent 5V power supply. The buzzer produced audio alerts with high-pitched tones for granted access and low-pitched tones for denied entry, while the LCD I2C display provided visual feedback showing messages like "Scan your card", "Enter passcode", "Access Granted", or "Access Denied". The system integrated RFID technology, keypad input, servo control, power management, and Firebase logging (cloud database for data storage) to ensure secure and efficient access control with real-time monitoring capabilities.

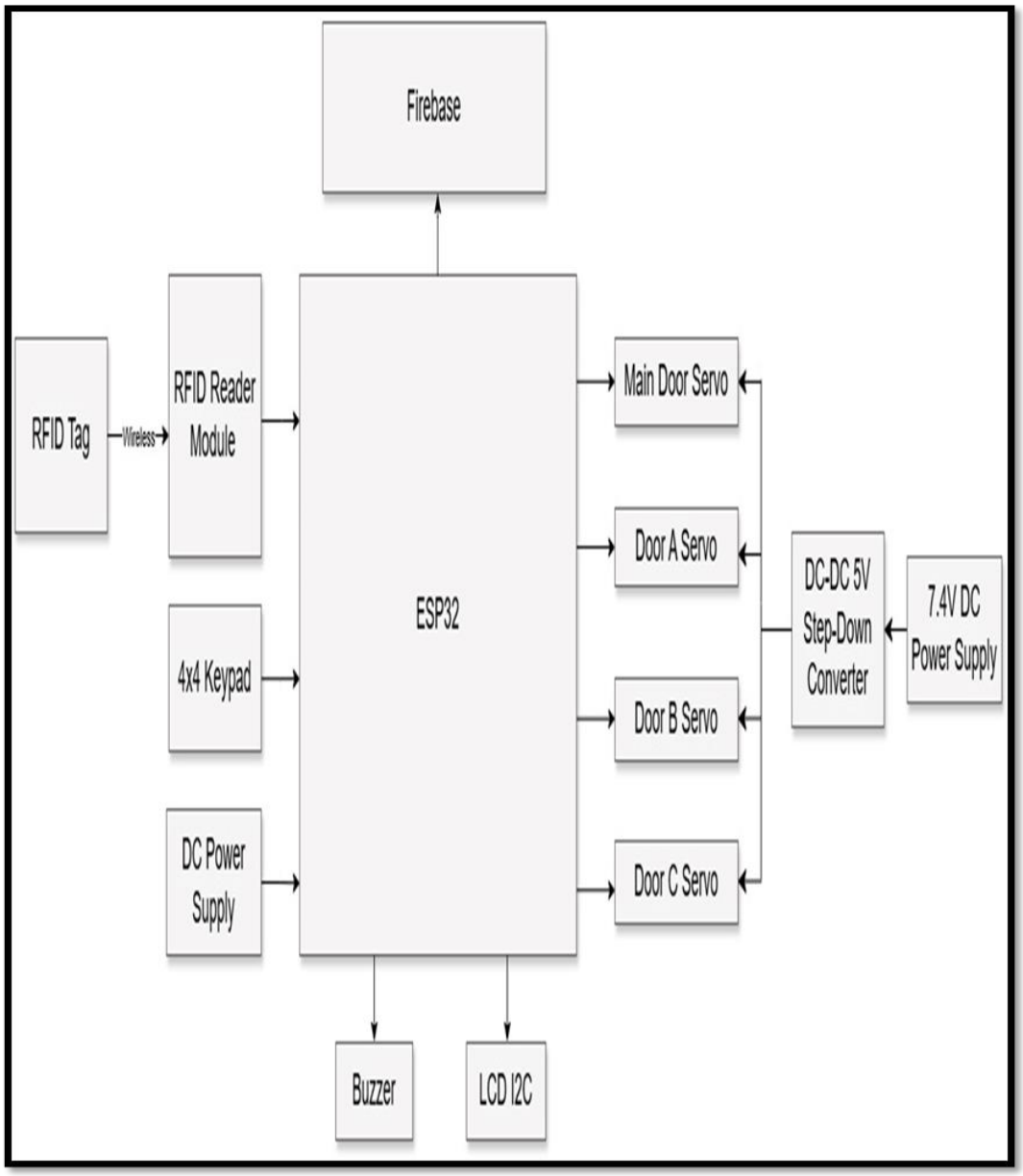

Figure 1: System Block Diagram

2.3 System Flowchart

Figure 2 shows the system flowchart started with initializing all components including the RFID Reader Module, keypad, LCD screen, buzzer, and servo motors, followed by Wi-Fi connectivity for real-time Firebase logging (cloud database platform for storing data). The system then waited for RFID scanning at Step A, where valid scans proceeded to passcode entry while invalid scans returned to await another attempt. When an RFID card was scanned, the system checked if the identifier matched stored credentials and prompted users to enter their

Progress in Engineering Application and Technology Vol. 6 No. 2 (2025) p. 216-224

passcode through the keypad interface. The system recorded each digit input with an internal timer and compared entered digits against encrypted stored versions.

In Step C, valid passcode authentication granted access by displaying "Room X Accessed" on the LCD with a high-pitched buzzer tone, while servo motors unlocked both main entrance and specified room doors with a 10-second countdown timer. Invalid passcodes triggered "Try Again" messages, and after three failed attempts, the system required master reset in Step D. The master reset process involved detecting the Master RFID UID (Unique Identifier - distinctive code for each RFID tag) and entering the master passcode, which displayed "Master Reset" on the LCD with continuous buzzer beeping before returning the system to default state for normal re-authentication procedures.

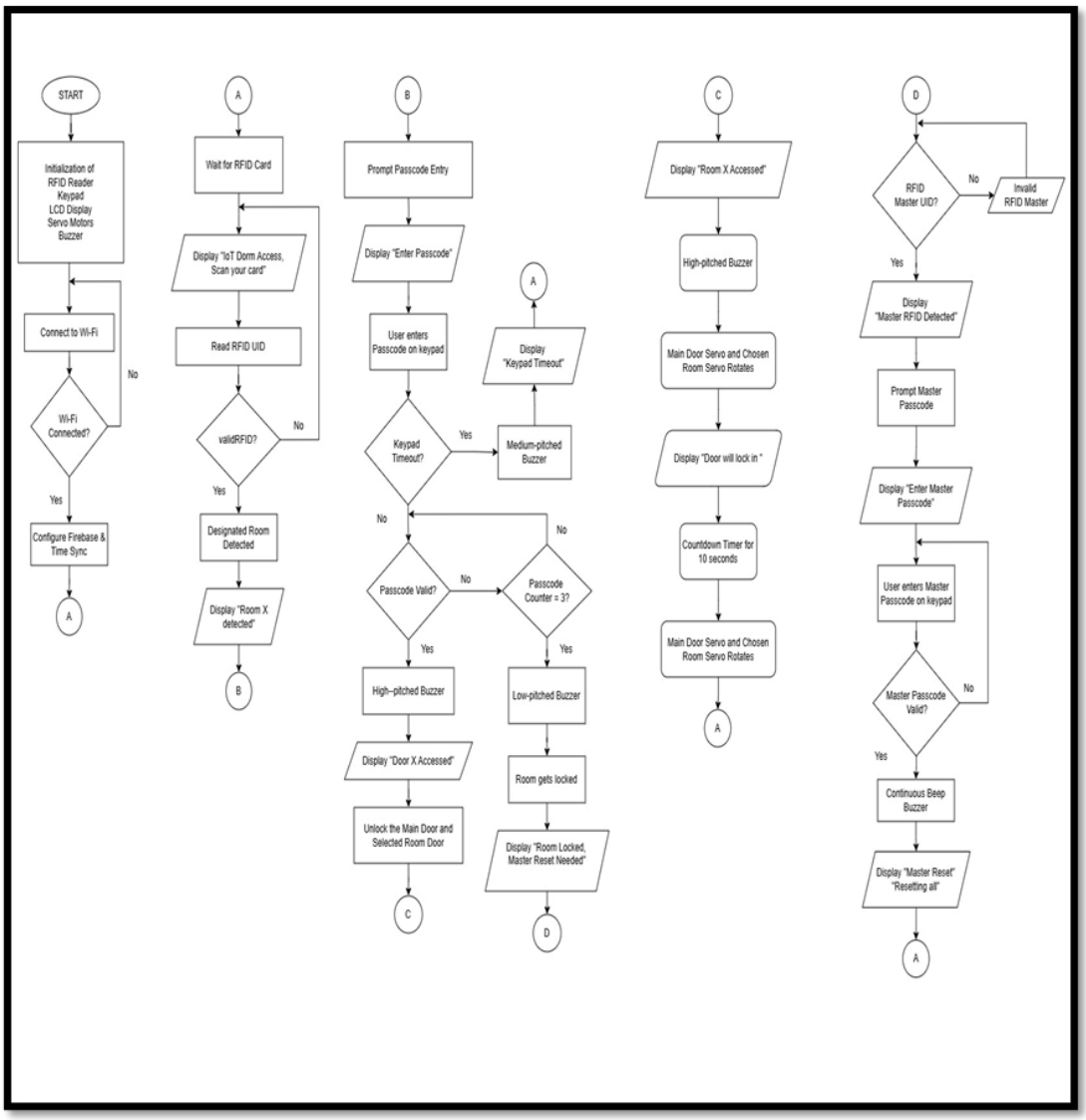

Figure 2: System Flowchart

2.4 Circuit Diagram

Figure 3 shows the circuit schematic representing the dual-authentication IoT access control system that used both RFID (Radio Frequency Identification - wireless technology using radio waves to identify objects) and passcode for secure access. The ESP32 microcontroller acted as the main controller, managing communication between the RFID Reader Module, 4x4 keypad, 20x4 I2C LCD display, buzzer, and four servo motors. The RFID reader received 3.3V power from the ESP32 and communicated through SPI interface (Serial Peripheral Interface - communication protocol for data transfer), while the keypad connected via GPIO pins (General

Purpose Input/Output - programmable digital signal pins). The LCD display provided visual feedback using I2C (Inter-Integrated Circuit - two-wire communication protocol) and showed system status messages.

Four servo motors physically controlled door locking, with one operating the main door and three controlling Rooms A, B, and C. After successful authentication, the ESP32 sent PWM signals (Pulse Width Modulation - method to control motor position) to rotate servo motors and unlock doors for 10 seconds before automatically re-locking. The buzzer provided audio feedback with high-pitched tones for successful access and low-pitched sounds for errors. The entire system operated on a 5-volt power supply with a DC-DC converter ensuring servo motors received precise voltage when their power consumption exceeded the microcontroller's capacity.

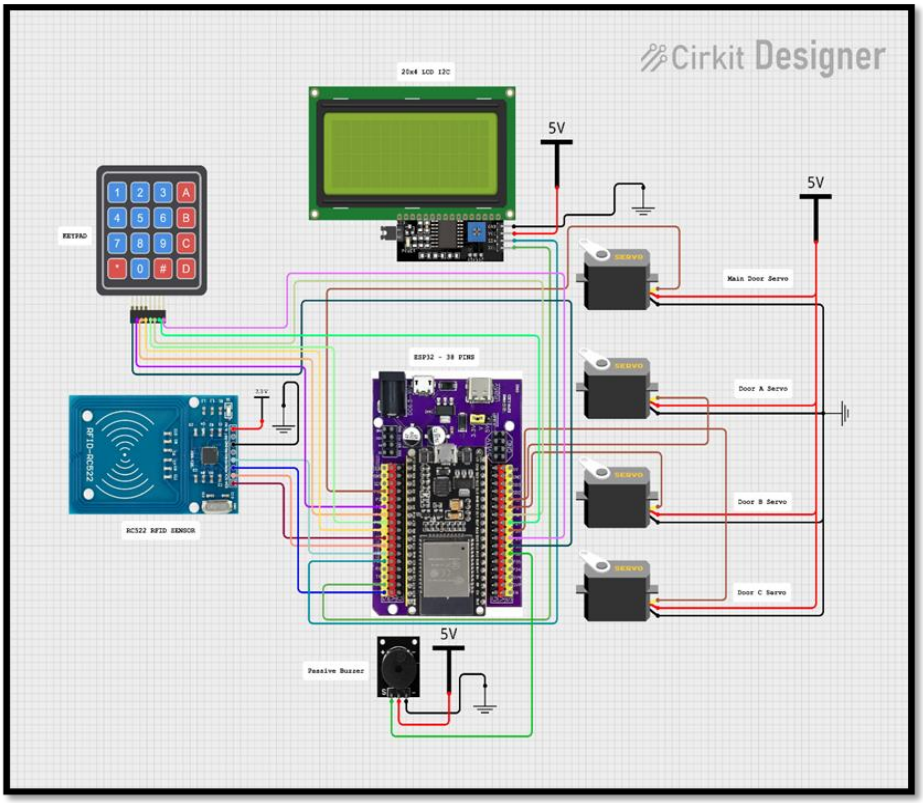

Figure 3: Circuit Diagram

3. Results and Discussion

Figure 4 and Figure 5 below shows the dual authentication system that was implemented for secure dormitory access, requiring both Radio Frequency Identification (RFID) card verification and unique passcode entry. Each student received an RFID card with a distinct digital signature, and access was granted only after successful verification of both authentication factors. The system employed servo motors as shown in figure 4 with independent power supplies to control door mechanisms, ensuring reliable operation despite microcontroller power fluctuations. Performance testing demonstrated zero unauthorized access incidents, with the system incorporating a three-attempt limit before administrative lockout to prevent brute force attacks.

The system is integrated with Firebase to enable real-time logging of all access events, categorizing them as Access Approved, Access Denied, or Master Reset. This comprehensive logging provided administrators with immediate visibility into system operations and created detailed audit trails for security oversight. Testing confirmed reliable Firebase integration with accurate real-time event recording and no data loss incidents. While the current implementation met immediate requirements, scalability considerations were evaluated for larger dormitory deployments, particularly addressing General Purpose Input/Output (GPIO) pin limitations on the ESP32 microcontroller for future expansion capabilities.

Progress in Engineering Application and Technology Vol. 6 No. 2 (2025) p. 216-224

Figure 4: Hardware Prototype

Figure 5*:* Front view of Prototype Hardware

3.1 First Level of Authorization: RFID System

Figure 6 shows the door access control system operated through a sequential authentication process involving RFID scanning, passcode verification, and servo motor activation. When a valid RFID card was scanned, the system identified the corresponding room designation and displayed the recognition message on the Liquid Crystal Display (LCD). Upon successful authentication of both RFID credentials and passcode entry, the system activated servo motors to unlock both the main entrance and the designated room door simultaneously. The LCD confirmed successful access while an audible buzzer provided acoustic feedback to indicate authentication completion.

The system-maintained doors in an unlocked state for a predetermined 10-second interval, allowing sufficient time for user entry before automatic re-locking occurred. During this period, servo motors remained in the unlocked position until the timeout elapsed, after which both doors returned to the locked state accompanied by low-pitched buzzer confirmation. Each successful access event was automatically logged to Firebase with comprehensive details including event type classification, RFID unique identifier, timestamp, and user room assignment, providing administrators with complete audit trail documentation for security monitoring and analysis.

(a) **(b)** **(c)**

Figure 6: RFID System (a) Starting Display (b) Room Card Detected (c) Invalid RFID

3.2 Second Level of Authorization: Passcode System

The system strengthened security by requiring students to enter unique passcodes as shown in Figure 7 that worked only for their specific rooms after scanning their RFID cards. This two-step process meant users needed both their physical card and their secret code to gain access. When students entered the wrong passcodes, the system denied access and recorded the failed attempt. After three incorrect passcode tries, the room automatically locked and required an administrator to reset it using master credentials. This approach effectively prevented unauthorized users from guessing passcodes and ensured that even if someone found a lost RFID card, they still could not enter without knowing the correct passcode.

(a) **(b)**

Figure 7: Passcode System (a) Input Passcode (b) Valid Passcode

3.3 Firebase Integration with ESP32

The ESP32 microcontroller was connected to Firebase as shown in Figure 8 through Wi-Fi communication to enable real-time data logging and remote monitoring capabilities. Every system event, including successful access attempts, failed authentication tries, and administrative resets, was automatically transmitted to Firebase's real-time database with detailed information such as timestamps, user identifications, and event descriptions. This integration allowed administrators to monitor dormitory access from any internet-connected device and provided a comprehensive audit trail for security analysis. The Firebase database organized events into categories like "AccessGranted," "AccessDenied," and "MasterReset," making it easy for administrators to track system performance and identify potential security issues as they occurred.

Progress in Engineering Application and Technology Vol. 6 No. 2 (2025) p. 216-224

Figure 8: Firebase log events

3.4 Functionality Tests

Table 2 below shows the implemented system comprehensive error handling for authentication failures through multiple security layers. Invalid RFID card scans triggered immediate rejection with LCD display notifications and low-pitched audible alerts, prompting users to retry with valid credentials. When correct RFID authentication occurred but incorrect passcodes were entered, the system initiated a progressive security protocol allowing three authentication attempts before implementing administrative lockout. Each failed passcode attempt generated specific feedback indicating remaining opportunities, with Firebase logging all access denial events including RFID unique identifiers and timestamp documentation.

Upon exhaustion of three passcode attempts, the affected room entered automatic lockout status requiring administrative intervention through master reset procedures. The security architecture-maintained room-specific isolation, ensuring that lockout conditions for one room did not impact access to other dormitory units. Table Administrative recovery utilized master RFID credentials and passcodes to restore normal operation, with all reset events logged to Firebase under "MasterReset" classification. This hierarchical security approach provided robust protection against unauthorized access attempts while maintaining system functionality for legitimate users across multiple room assignments.

Table 2: Functionality Tests of different events

Event	RFID	Keypad	Buzzer Tone	Description
Access Granted	Success	Success	High-pitched	It indicates that the authentication was successful, and access is granted. The servo motor of the designated door and main door unlocks. This is logged in Firebase.
Access Denied	Fail	-	Low-pitched	Indicates that the RFID or passcode is incorrect, and access is denied. This is logged in Firebase.
Incorrect Passcode	Success	Fail	Low-pitched	It indicates that the passcode entered is incorrect, and access is denied. This is logged in Firebase
Master Reset	Master RFID	Master Passcode	Continuous Beep	Indicates that the system has been reset by the admin (master reset).
Passcode Timeout	-	-	Medium-pitched	It indicates that the passcode entry timed out, prompting the user to reattempt. This event is not logged in Firebase.

4. Conclusion

The project successfully completed the development of an IoT-enabled dual authentication system for college dormitories. The system effectively combined RFID and passcode authentication to provide secure access control for dormitory rooms. The dual authentication approach proved effective in restricting unauthorized access to specified rooms while maintaining user convenience.

The RFID technology connected each room to a particular student and provided secure identification capabilities. The passcode served as the second authentication level, ensuring that stolen RFID cards remained useless without the corresponding passcode. Real-time event logging through Firebase provided administrators with comprehensive monitoring capabilities including timestamps, user IDs, room numbers, and authentication status. The dedicated power supply for servo motors ensured reliable locking operations and prevented power supply disruptions. The system demonstrated that IoT-based access control could significantly improve dormitory security while providing scalable solutions and rapid response capabilities that traditional mechanical systems could not provide.

Several recommendations emerged to enhance system effectiveness for larger installations. The system required additional GPIO pins through either upgraded microcontrollers or GPIO expanders to support more sensors and functionalities. Local storage capabilities needed implementation to reduce dependence on external services like Firebase, ensuring continued operation during server outages. Enhanced errors handling mechanisms including timeouts and backup plans would prevent system failures during disruptions. Biometric authentication integration such as fingerprint or facial recognition could provide additional security layers. Energy efficiency improvements would support long-term sustainability and reduce operating costs in large-scale installations. Web or mobile application integration would improve user experience and provide enhanced control for administrators and students. These improvements would create a more robust, scalable, and user-friendly system suitable for diverse dormitory environments.

Acknowledgement

The Department of Electrical Engineering Technology in the Faculty of Engineering Technology at Universiti Tun Hussein Onn Malaysia is truly appreciated by the authors for their important help during the project. This project was successfully completed thanks to the faculty's direction, supply of information sources, and ongoing support.

References

[1] Hercog, D., Lerher, T., Truntič, M., & Težak, O. (2023). Design and Implementation of ESP32-Based IoT Devices. *Sensors*, *23*, 6739. https://doi.org/10.3390/s23156739

[2] Majumder, A. J., & Izaguirre, J. A. (2020). A Smart IoT Security System for Smart-Home Using Motion Detection and Facial Recognition. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 1065–1071. https://doi.org/10.1109/compsac48688.2020.0-132

[3] Abdulshaheed, H. R., Abbas, H. H., Barazanchi, I. A., & Hashim, W. (2022). Control and alert mechanism of RFID door access control system using Iot. 3C Tecnología_Glosas De Innovación Aplicadas a La Pyme, 40–2, 269–285. https://doi.org/10.17993/3ctecno.2022.specialissue9.269-285

[4] Mohammed, S., & Alkeelani, A. H. (2019). Locker Security System Using Keypad and RFID. *Conference: The 2nd International Conference of Computer Science and Renewable Energies 2019 At: Morocco*, 1–5. https://doi.org/10.1109/iccsre.2019.8807588

[5] R. Padmasree, P. Harshitha, Shaik Muskan, & Anokya Kalwala. (2023). Developing a remote access system by interfacing ESP32 microcontroller with 4X4 keypad. *International Journal of Emerging Trends in Engineering Research*, *11*(10), 323–327. https://doi.org/10.30534/ijeter/2023/0211102023

[6] Hoque, M. A., & Davidson, C. (2019). Design and Implementation of an IoT-Based Smart Home Security System. *The International Journal of Networked and Distributed Computing*, *7*(2), 85. https://doi.org/10.2991/ijndc.k.190326.004

[7] Alzhrani, A. A., Balfaqih, M., Alsenani, F., Alharthi, M., Alshehri, A., & Balfagih, Z. (2024). Design and Implementation of an IoT-Integrated Smart Locker System utilizing Facial Recognition Technology. *Engineering Technology & Applied Science Research*, *14*(4), 16000–16010. https://doi.org/10.48084/etasr.7737