International Journal of Simulation, Optimization & Modelling, (2026) Vol 1, 262-276

SCHOLAR PUBLISHING

International Journal of Simulation, Optimization & Modelling
ISSN: 3083-967X

Journal homepage: https://e-journal.scholar-publishing.org/index.php/ijsom

Development of an RFID-Based Automatic Door System Using the ESP8266 Microcontroller

M. Rizki Ramadhan[1], Erdiwansyah[2], Teuku Andiansyah[1]

[1]Department of Computer Engineering, Universitas Serambi Mekkah, Banda Aceh 23245, Indonesia
[2]Department of Natural Resources and Environmental Management, Universitas Serambi Mekkah, Banda Aceh, 23245, Indonesia

Corresponding Author: riskidrr@gmail.com

Abstract
Automatic door systems have become an effective solution for improving access security compared with conventional mechanical locks. This study aims to develop an RFID-based automatic door system using the ESP8266 microcontroller as the main controller. The proposed system integrates an ESP8266 NodeMCU, RFID RC522 reader, relay module, 12 V solenoid door lock, and a 16×2 I2C LCD to provide user authentication and automatic door locking. This research employed a Research and Development (R&D) approach consisting of system design, hardware and software implementation, and functional testing using the Black Box Testing method. The testing results demonstrated that the RFID RC522 successfully identified registered RFID cards while rejecting unauthorised cards. Furthermore, the ESP8266 processed authentication data correctly, controlled the relay and solenoid door lock, and displayed system status on the LCD. All hardware and software components operated according to the system design, indicating that the developed prototype functioned reliably as an access control system. Therefore, the proposed RFID-based automatic door system can improve room security and provide a practical solution for electronic access control. Future work may include database integration, access logging, and Internet of Things (IoT)-based remote monitoring.

Article Info
Received: 20 June 2026
Revised: 10 July 2026
Accepted: 14 July 2026
Available online: 15 July 2026

Keywords
ESP8266
RFID
Automatic Door System
Smart Door Lock
Access Control

1. Introduction

The rapid development of embedded systems, wireless communication, identification technologies, and the Internet of Things (IoT) has significantly transformed modern security and access control systems. Room access security has become an essential requirement for protecting physical assets, confidential information, equipment, and restricted facilities in offices, educational institutions, laboratories, residential buildings, and industrial environments. Modern access control systems are expected not only to prevent unauthorised entry but also to provide reliable authentication, rapid identification, operational efficiency, and convenient security management. Despite advances in electronic security technologies, conventional mechanical locking systems remain widely used because of their simplicity and relatively low implementation costs. However, mechanical keys have several limitations, including the risk of loss, duplication, theft, or transfer to unauthorised individuals. Furthermore, conventional locking mechanisms generally cannot automatically identify users, provide real-time access information, or support digital management of access activities, thereby limiting their effectiveness for modern security applications (Hameed et al., 2021; Khando et al., 2021; Basyir & Nurwijayanti, 2022; Adams & Giap, 2024).

The limitations of conventional locking mechanisms have encouraged the development of electronic and intelligent access control systems. Various authentication technologies, including passwords, Personal Identification Numbers (PINs), keypads, smart cards, biometric recognition, Radio Frequency Identification (RFID), Near Field Communication (NFC), and IoT-based authentication, have increasingly been investigated for modern security applications. The convergence of embedded devices, communication technologies, and intelligent authentication mechanisms has provided opportunities to develop access control systems with improved automation, flexibility, and operational efficiency (Alaba et al., 2021; Pal et al., 2021; Yang et al., 2022). Password- and keypad-based systems are among the most commonly implemented electronic access control solutions because of their relatively simple hardware and software requirements. Nevertheless, these authentication methods remain vulnerable to several security risks because passwords can be forgotten, shared, observed, guessed, or stolen by unauthorised individuals. Consequently, authentication mechanisms based on unique user identities and contactless identification technologies have received increasing attention as practical alternatives to conventional access control methods.

Among the available identification technologies, Radio Frequency Identification (RFID) has emerged as a promising technology for authentication, identification, tracking, asset management, attendance monitoring, and physical access control. RFID technology enables contactless communication between an RFID tag or card and an RFID reader using radio-frequency signals. A typical RFID-based system consists of a tag containing identification information, an RFID reader responsible for capturing the transmitted data, a processing unit for authentication, and an application system responsible for performing specific control functions. Compared with conventional mechanical keys and manually entered passwords, RFID technology offers several advantages, including rapid identification, contactless operation, relatively low implementation costs, ease of integration with embedded systems, and simplified user authentication management (Basyir & Nurwijayanti, 2022; Ishaq & Bibi, 2023; Kassim et al., 2023; Araújo & Lemes, 2025).

The increasing application of RFID technology has also been supported by its compatibility with embedded systems and IoT architectures. RFID systems can be integrated with microcontrollers, sensors, electronic actuators, databases, communication networks, and user interfaces to develop automated identification and control applications. The integration of identification technologies with IoT architectures can improve automation, data exchange, and system management while providing opportunities for the development of intelligent security applications (Ferrag et al., 2021; Ishaq & Bibi, 2023). These developments indicate that RFID technology provides a flexible technological foundation for developing electronic security systems ranging from simple local authentication applications to more complex network-connected platforms.

In RFID-based access control applications, each RFID card contains identification information, such as a Unique Identifier (UID), that can be captured by an RFID reader and processed by a microcontroller. The authentication process is commonly performed by comparing the detected UID with authorised identification data stored within the system. When the detected identification data match those of a registered user, the controller generates an output signal to activate the electronic locking mechanism. Conversely, when an unauthorised RFID card is detected, the system maintains the locked condition and rejects the access request. This authentication mechanism enables RFID technology to provide a practical solution for electronic door security systems while reducing several limitations associated with mechanical keys and manually entered passwords (Caballero-Gil et al., 2022; Kassim et al., 2023; Singh et al., 2024; Araújo & Lemes, 2025).

Despite the advantages offered by RFID technology, security remains an important consideration in RFID-based access control applications. RFID systems may potentially face security challenges, including unauthorised tag reading, eavesdropping, data interception, tag cloning, replay attacks, identity manipulation, and unauthorised system access. Security, privacy, and trust are fundamental concerns in interconnected systems because the increasing integration of embedded devices and communication infrastructures can introduce multiple security vulnerabilities (Tewari & Gupta, 2021; Meneghello et al., 2021; Pal et al., 2021). Therefore, the development of RFID-based access control systems requires not only appropriate hardware integration but also reliable authentication mechanisms and systematic evaluation of system functionality and security.

Several approaches have been investigated to improve authentication security in RFID-based systems. Caballero-Gil et al. (2022) investigated an RFID authentication mechanism intended to improve the security of communication between RFID tags and readers. Similarly, Wang et al. (2023) proposed an RFID authentication protocol based on an encryption mechanism to enhance the protection of RFID communication. More recently, Fernández-Caramés et al. (2024) investigated the security aspects of commercial RFID tags for IoT applications. These studies demonstrate that authentication security remains an important research area in RFID-based applications. Although advanced cryptographic mechanisms can improve system security, relatively simple UID-based authentication remains useful for developing and evaluating low-cost functional prototypes intended for educational facilities, laboratories, offices, and other applications that do not initially require complex network-based security infrastructures.

The increasing availability of affordable and programmable microcontroller platforms has further accelerated the development of intelligent access control systems. Microcontrollers provide essential processing capabilities for receiving identification data, performing authentication procedures, controlling electronic actuators, managing communication between hardware components, and generating information for user interfaces. The integration of microcontrollers with RFID technology has enabled the development of compact and relatively low-cost security systems that can automatically process authentication data and control physical access mechanisms (Basyir & Nurwijayanti, 2022; Kassim et al., 2023; Adams & Giap, 2024).

Among available microcontroller platforms, the ESP8266 NodeMCU has been widely used in embedded systems and IoT applications for its compact architecture, relatively low cost, programmable I/O capabilities, integrated Wi-Fi connectivity, and suitability for prototype development. These characteristics make the ESP8266 appropriate for applications requiring real-time processing, sensor integration, actuator control, and potential future expansion toward network-based applications (Singh et al., 2024; Araújo & Lemes, 2025). Although the ESP8266 provides integrated wireless communication capabilities, the microcontroller can also operate as a local embedded controller without requiring continuous Internet connectivity. This flexibility makes the ESP8266 suitable for developing standalone access control systems in environments where simple architecture, operational independence, and reliable local functionality are required.

The integration of RFID authentication with the ESP8266 microcontroller provides a flexible architecture for developing automatic door access systems. In such systems, the RFID reader captures identification data from an RFID card and transmits the information to the microcontroller for processing. The controller subsequently compares the detected identification information with registered user data and generates an output signal according to the authentication result. Additional hardware components, including relay modules, electronic door locks, and Liquid Crystal Displays (LCDs), can be integrated to provide physical door actuation and real-time information regarding system operation (Basyir & Nurwijayanti, 2022; Adams & Giap, 2024; Singh et al., 2024).

Electronic locking mechanisms represent another essential component of automatic access control systems. Solenoid door locks are commonly employed in prototype applications because they can convert electrical signals into mechanical locking and unlocking movements. Since microcontrollers generally operate at relatively low voltages and currents, an electronic switching device, such as a relay module, is required to interface the microcontroller with the higher-voltage solenoid locking mechanism. When an authorised RFID card is detected, the microcontroller activates the relay, allowing electrical power to operate the solenoid lock for a predefined duration. Conversely, the locking mechanism remains inactive when unauthorised identification data are detected. In addition, an LCD can provide immediate visual feedback by displaying information regarding system status, authentication approval, or access rejection. The integration of authentication, processing, switching, actuation, and display components can therefore provide a relatively simple and practical architecture for automatic door security applications (Adams & Giap, 2024; Singh et al., 2024; Araújo & Lemes, 2025).

The integration of IoT capabilities into access control systems can provide additional functionalities, including remote monitoring, database management, access logging, and real-time communication.

Nevertheless, IoT-enabled systems also introduce additional security challenges because connected devices can be exposed to cyberattacks, unauthorised access, and data privacy threats. Previous studies have extensively discussed security requirements, vulnerabilities, privacy concerns, and cybersecurity approaches associated with IoT environments (Al-Garadi et al., 2021; Hameed et al., 2021; Khando et al., 2021; Meneghello et al., 2021; Pal et al., 2021). Therefore, although IoT connectivity offers significant advantages for advanced access control applications, local embedded systems remain relevant for applications that prioritise simple implementation, reduced network dependency, and independent operation.

Recent studies have demonstrated increasing interest in developing RFID-, microcontroller-, and IoT-based identification and access control systems. Basyir and Nurwijayanti (2022) developed an IoT-based RFID room security system, demonstrating the potential integration of contactless authentication and network communication for electronic security applications. Ishaq and Bibi (2023) reviewed RFID- and IoT-based identification systems and highlighted the potential of these technologies for improving the efficiency, reliability, and automation of identification processes. Kassim et al. (2023) investigated the implementation of RFID technology for controlling access to restricted areas. Collectively, these studies demonstrate the flexibility of RFID technology for developing various automated identification and security applications.

Further developments have focused on integrating microcontrollers, IoT communication, and electronic door-locking mechanisms. Adams and Giap (2024) proposed an IoT-based prototype integrating an automatic door system with fire alarm functionality, highlighting the potential of embedded technologies for multifunctional security applications. Their study is a 2024 publication on automatic doors and IoT-based security systems. Similarly, Singh et al. (2024) investigated an ESP8266-based smart door lock using IoT technology and demonstrated the applicability of low-cost microcontrollers for connected access control applications. More recently, Araújo and Lemes (2025) developed IFGAccess, a web-based RFID access control system that uses the ESP8266 microcontroller, emphasising digital access management and web-based functionality.

The existing literature demonstrates that RFID, IoT, microcontrollers, biometric identification, electronic actuators, databases, and web-based platforms have been extensively investigated for modern access control applications. Nevertheless, several research limitations remain. Some previous studies primarily emphasise IoT connectivity and remote monitoring, whereas others focus on RFID identification, advanced authentication protocols, biometric security, web-based data management, multifunctional security applications, or RFID communication security (Caballero-Gil et al., 2022; Ishaq & Bibi, 2023; Kassim et al., 2023; Wang et al., 2023; Fernández-Caramés et al., 2024; Araújo & Lemes, 2025). Consequently, further investigation is required into the systematic development and functional evaluation of a complete, standalone access control prototype that integrates RFID-based UID authentication, embedded data processing, electronic switching, physical door actuation, and real-time visual feedback within a unified, relatively low-cost system architecture.

Furthermore, dependence on continuous Internet connectivity may increase implementation complexity and potentially affect system availability in environments where network infrastructure is limited, unstable, or unnecessary for basic access control applications. Although IoT connectivity provides significant advantages for remote monitoring and data management, network-connected systems may also introduce additional security, privacy, and implementation challenges (Alaba et al., 2021; Hameed et al., 2021; Tewari & Gupta, 2021; Yang et al., 2022). A locally operated system can therefore offer advantages in terms of implementation simplicity, reduced network dependency, and operational independence. Accordingly, the development and functional evaluation of a local RFID-based automatic door system remains relevant, particularly for small offices, educational facilities, laboratories, and other applications requiring affordable implementation and straightforward system operation.

Based on the identified research gap, this study develops an RFID-based automatic door access control system using the ESP8266 NodeMCU as the main processing unit. The proposed system integrates an RFID RC522 reader for user authentication, an ESP8266 NodeMCU for processing UID data, a relay module for electronic switching, a 12 V solenoid door lock for physical access control, and a 16×2 I2C LCD for displaying authentication status. Unlike network-dependent access control systems, the developed prototype is designed to perform its primary authentication and door-control functions locally without requiring continuous Internet connectivity. Functional testing using the Black Box Testing method is conducted to determine whether each hardware and software component operates according to the predefined system requirements.

The main objective of this study is to design, develop, and functionally evaluate a low-cost RFID-based automatic door system that integrates user authentication, embedded data processing, electronic switching, automatic door locking, and real-time status display within a single functional prototype. The specific contribution of this study lies in the implementation and functional validation of an integrated local authentication-to-actuation architecture that combines the ESP8266 NodeMCU, RFID RC522 UID authentication, relay-based electronic control, a 12 V solenoid locking mechanism, and a 16×2 I2C LCD, without relying on continuous Internet connectivity. In contrast to previous studies that predominantly emphasise IoT communication, remote monitoring, web-based access management, advanced authentication mechanisms, or individual components of access control systems, the proposed approach focuses on evaluating the integrated functionality of the complete process, beginning with RFID identification and authentication and continuing through embedded data processing, electronic switching, physical door actuation, and real-time user feedback. Therefore, the proposed system provides a practical and expandable prototype architecture that can serve as a foundation for future developments involving enhanced RFID security, user databases, digital access logging, wireless communication, and IoT-based remote monitoring.

2. Methodology

This study employed a Research and Development (R&D) approach to design, develop, implement, and evaluate an RFID-based automatic door access control system using the ESP8266 NodeMCU as the main controller. The research methodology was conducted systematically through several stages, including system requirements analysis, hardware and software design, component integration, prototype implementation, and functional testing. The proposed system integrates an RFID RC522 reader for user identification, an ESP8266 NodeMCU for UID authentication and data processing, a 5 V relay module for electronic switching, a 12 V solenoid door lock as the physical locking mechanism, and a 16×2 I2C LCD for displaying real-time system status. The operational process was designed based on the system flowchart presented in Figure 1, which describes the complete sequence from system initialisation and RFID card detection to UID validation, access authorisation, door actuation, and automatic re-locking. Finally, Black Box Testing was conducted to evaluate the functional performance of each component and to verify that the integrated prototype operated in accordance with the predefined system requirements.

2.1 Research Method

Fig. 1 illustrates the operational flow of the proposed RFID-based automatic door access control system, beginning with system initialisation and continuing through user authentication and door-locking operations. During the initialisation stage, the ESP8266 NodeMCU, RFID RC522 reader, 16×2 I2C LCD, 5 V relay module, and solenoid door lock are activated and prepared for operation. The system then enters a standby condition and waits for an RFID card to be presented to the reader. Once a card is detected, the RFID RC522 reads its Unique Identifier (UID), which the ESP8266 subsequently processes. If the UID cannot be read, the system returns to the standby state and waits for another RFID card. When the UID is successfully detected, the ESP8266 compares it with the registered UID data to determine the user's authorisation status. An invalid UID displays an "Access Denied" message on the LCD, while a valid UID activates the relay and unlocks the solenoid door lock. The LCD subsequently displays an "Access Granted" message, allowing the authorised user to enter the restricted area.

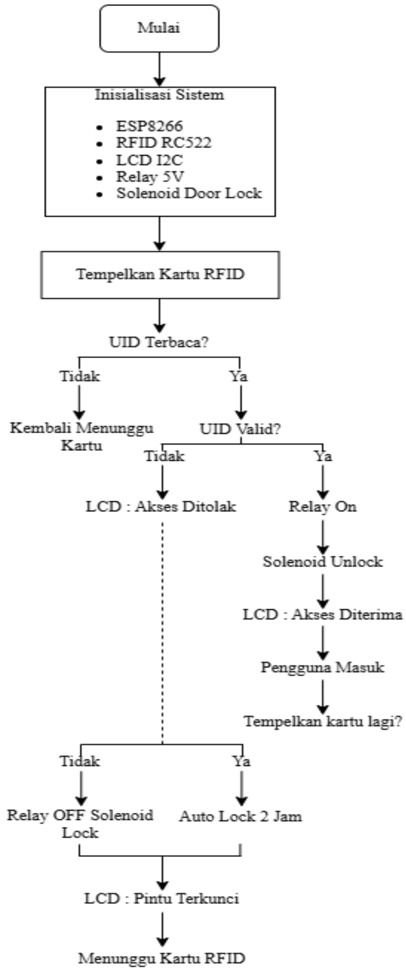


Fig. 1. Operational Flowchart of the RFID-Based Automatic Door Access Control System

The operational flow presented in Figure 1 demonstrates the integration of authentication, decision-making, electronic actuation, and user feedback within a single access control process. After authorised access is granted, the system proceeds to the door-locking stage. The door can be locked again by presenting the RFID card or through the predefined automatic locking mechanism. The relay is then deactivated, causing the solenoid door lock to return to its locked position, while the LCDs a message indicating that the door has been successfully secured. Finally, the system returns to the standby condition and waits for the next RFID card. This operational sequence demonstrates that the proposed system provides a systematic authentication-to-actuation process in which the ESP8266 functions as the main controller responsible for processing RFID data, validating user credentials, controlling the relay and solenoid locking mechanism, and managing real-time information displayed on the LCD. Therefore, the flowchart confirms that the proposed system is designed to provide a simple, automated, and integrated approach to RFID-based room access control.

2.2 Requirement Analysis

Table 1 presents the hardware components, specifications, and corresponding functions used in developing the proposed RFID-based automatic door access control system. The ESP8266 NodeMCU serves as the main controller, processing authentication data and coordinating the operation of all connected hardware components. The RFID RC522, operating at a frequency of 13.56 MHz, is used to detect and read the Unique Identifier (UID) stored on the MIFARE Classic RFID card, which functions as the user authentication credential. Once the UID data are obtained, the ESP8266 processes and compares them with the registered user data to determine whether access should be granted or denied. The selection of these components provides a relatively simple and low-cost authentication architecture suitable for the development of an automatic door access control prototype.

Table 1. Hardware Specifications

Component	Specification	Function
ESP8266 NodeMCU	ESP8266 Wi-Fi MCU	Main controller
RFID RC522	13.56 MHz RFID Reader	Reads RFID card UID
RFID Card	MIFARE Classic	User authentication
Relay Module	5 V Single Channel	Controls the solenoid door lock
Solenoid Door Lock	DC 12 V	Electronic locking mechanism
LCD I2C	16×2 Display	Displays authentication status
Power Supply	DC 12 V Adapter	Supplies electrical power

The remaining hardware components support the actuation, information display, and power supply functions of the proposed system. The 5 V single-channel relay module acts as an electronic switching interface between the ESP8266 NodeMCU and the 12 V solenoid door lock, allowing the low-voltage control signal generated by the microcontroller to operate the electronic locking mechanism. The solenoid door lock physically controls door locking and unlocking based on the authentication result, while the 16×2 I2C LCD provides real-time visual feedback on system conditions, including authentication and door-locking status. Meanwhile, the 12 V DC adapter supplies the electrical power required for system operation, particularly for the solenoid locking mechanism. Overall, the hardware configuration presented in **Table 1** demonstrates that each component has a specific and complementary function, enabling the integration of user identification, data processing, electronic switching, physical actuation, and visual feedback into a complete RFID-based automatic door access control system.

2.3 System Design

Figure 2 presents the overall hardware architecture of the proposed RFID-based automatic door access control system and illustrates the flow of data, control signals, and electrical power among the integrated components. The authentication process begins when an RFID card is placed near the RFID RC522 reader. The reader captures the card's Unique Identifier (UID) and transmits the identification data to the ESP8266 NodeMCU through the Serial Peripheral Interface (SPI) communication protocol. The ESP8266 serves as the central processing unit and compares the received UID with the authorised UID stored in program memory. The authentication result is then displayed on the 16×2 I2C LCD through the Inter-Integrated Circuit (I2C) communication interface, allowing the user to receive immediate visual information regarding whether access has been granted or denied. This configuration reduces the number of communication wires required between the microcontroller and the LCD while enabling efficient real-time status display. In addition, the architecture separates the identification, processing, and user-interface functions, thereby creating a structured data flow from the RFID card to the RFID reader, microcontroller, and display module.

The ESP8266 also controls the physical door-locking mechanism through one of its General-Purpose Input/Output (GPIO) pins connected to the 5 V relay module. When a valid UID is detected, the microcontroller sends a control signal to activate the relay, which functions as an electrically isolated switching interface between the low-voltage ESP8266 and the higher-power 12 V solenoid door lock. Once the relay is energised, the 12 V DC supply is delivered to the solenoid, causing the locking mechanism to retract and unlock the door. When access is denied or the predefined unlocking period has ended, the relay is deactivated, the electrical supply to the solenoid is interrupted, and the door returns to its locked condition. The power subsystem consists of a 12 V DC adapter connected through a female DC jack, supplying power directly to the relay and solenoid lock, while the ESP8266 is powered separately by a 5 V USB source. This arrangement is necessary because the solenoid requires a higher operating voltage and current than the microcontroller can provide directly. Overall, the architecture shown in Figure 2 demonstrates a complete authentication-to-actuation process in which the RFID RC522 performs user identification, the ESP8266 manages decision-making and control, the LCD provides user feedback, and the relay-solenoid combination performs the physical locking and unlocking operation.

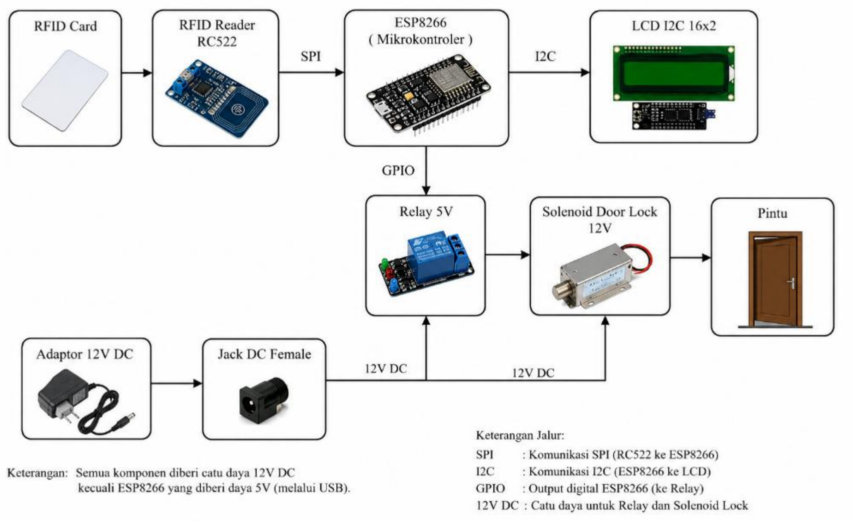


Fig. 2. System Architecture of the Proposed RFID-Based Automatic Door Access Control System

2.4 Hardware Circuit Design

Fig. 3 illustrates the detailed hardware circuit configuration and electrical connections among the main components of the proposed RFID-based automatic door access control system. The ESP8266 NodeMCU functions as the central controller that coordinates RFID authentication, data processing, status display, and door-lock actuation. The RFID RC522 reader is connected to the ESP8266 via the Serial Peripheral Interface (SPI), enabling transmission of the Unique Identifier (UID) data detected by the RFID card. The RC522 module operates at 3.3 V and is connected to the corresponding digital pins of the ESP8266 for the SCK, MOSI, MISO, SDA/SS, and RST signals. Meanwhile, the 16×2 I2C LCD is connected to the ESP8266 through the Inter-Integrated Circuit (I2C) interface using the SDA and SCL communication lines. The I2C configuration reduces the number of GPIO pins required for display communication and enables the ESP8266 to provide real-time visual information regarding authentication and door status. Through this circuit arrangement, the ESP8266 receives the UID data from the RFID RC522, processes the authentication result, and displays the corresponding system information on the LCD.

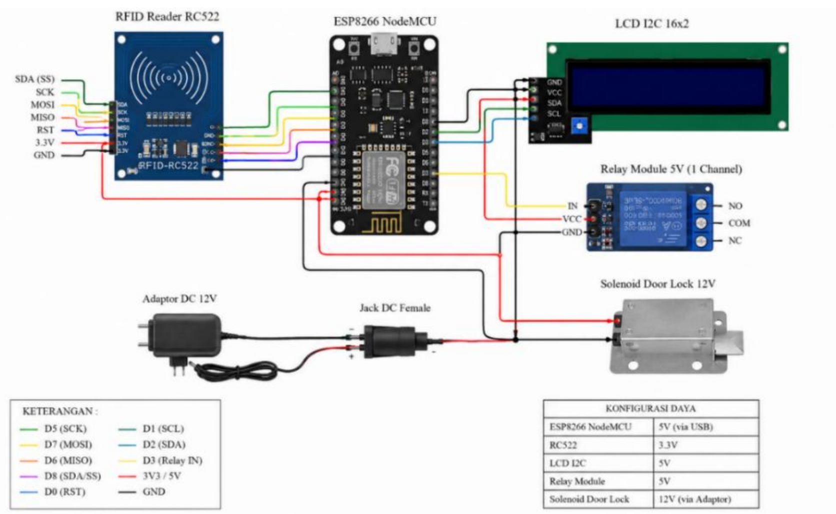


Fig. 3. Hardware Circuit Configuration of the Proposed RFID-Based Automatic Door Access Control System

The output and power-control sections of the circuit consist of a 5 V single-channel relay module, a 12 V solenoid door lock, and a 12 V DC power supply. The relay input is connected to a GPIO pin of the ESP8266, allowing the microcontroller to control the switching operation according to the RFID authentication result. When a registered UID is successfully authenticated, the ESP8266 generates a control signal that activates the relay, enabling the 12 V power supply to energise the solenoid door lock and unlock the door. After the predefined access period has elapsed or the locking command is executed, the relay is deactivated, and the solenoid returns the door to its locked condition. As shown in **Fig. 3**, the system uses different operating voltage levels according to the electrical requirements of each component: the RFID RC522 operates at 3.3 V, the ESP8266 NodeMCU and relay module use appropriate low-voltage supplies, and the external 12 V DC adapter powers the solenoid door lock. This separation is important because the ESP8266 cannot directly supply the voltage and current required by the solenoid lock. Overall, the circuit configuration demonstrates the integration of the communication, processing, display, switching, actuation, and power-supply subsystems into a complete hardware platform for the proposed RFID-based automatic door access control system.

2.5 System Testing

The developed prototype was evaluated using Black-Box Testing to determine whether the overall system and its individual hardware components met the predefined functional requirements. This testing approach focuses on evaluating the relationship between system inputs and outputs without examining the program's internal structure or the embedded software's detailed logic. During testing, various input conditions were applied to the system, using both registered and unregistered RFID cards, and the corresponding system responses were observed. The evaluation covered the complete operational sequence, beginning with RFID card detection and UID reading, followed by authentication processing, relay activation, solenoid door-lock operation, and the display of authentication information on the 16×2 I2C LCD. This approach was selected because it provides a practical method for determining whether the integrated prototype performs its intended functions from the user and system operation perspectives.

Each major hardware component was tested individually and collectively to verify its functional performance and integration with the proposed access control system. The RFID RC522 was evaluated based on its ability to detect RFID cards and accurately transmit UID data to the ESP8266 NodeMCU, while the microcontroller was tested to determine whether it could correctly process the received UID and distinguish between authorised and unauthorised users. The relay module and 12 V solenoid door lock were evaluated by observing their switching, locking, and unlocking responses following the authentication process. In addition, the 16×2 I2C LCD was tested to verify its ability to display the appropriate system and authentication status in real time. The complete system was subsequently evaluated under different access conditions to ensure that all components operated in a coordinated manner throughout the authentication-to-actuation process. The results obtained from these functional tests provide the basis for assessing the operational reliability and effectiveness of the developed RFID-based automatic door access control prototype, as discussed in the following section.

3. Result & Discussion

This section presents and discusses the implementation and functional evaluation results of the developed RFID-based automatic door access control system. The analysis focuses on the performance and integration of the main hardware components, including the RFID RC522 reader, ESP8266 NodeMCU, 5 V relay module, 12 V solenoid door lock, and 16×2 I2C LCD. The developed prototype was evaluated using Black-Box Testing to verify that each component and the overall system operated according to the predefined functional requirements. The evaluation covered the complete operational process, including RFID card detection, UID reading and validation, authentication data processing, relay switching, door locking and unlocking, and real-time status display. The obtained results are discussed to assess the functional performance, reliability, and effectiveness of the integrated prototype in providing automatic and secure room access control.

3.1 Prototype Implementation

Fig. 4 presents the physical implementation of the proposed RFID-based automatic door access control system after the hardware components were assembled and integrated into a functional prototype. The implemented system consists of the RFID RC522 reader, ESP8266 NodeMCU, relay module, solenoid door lock, power supply circuitry, and supporting electronic connections installed on the prototype platform. The RFID reader is positioned in the upper section of the prototype to facilitate the detection and reading of RFID cards, while the ESP8266 NodeMCU functions as the main processing unit responsible for receiving UID data, performing user authentication, and generating control signals based on the authentication results. The electronic components are interconnected according to the hardware circuit configuration presented in **Fig. 3**, enabling communication and control among the identification, processing, switching, and actuation subsystems. The physical implementation demonstrates that the proposed hardware architecture can be successfully realised as an integrated prototype, rather than remaining limited to a conceptual design or circuit simulation.

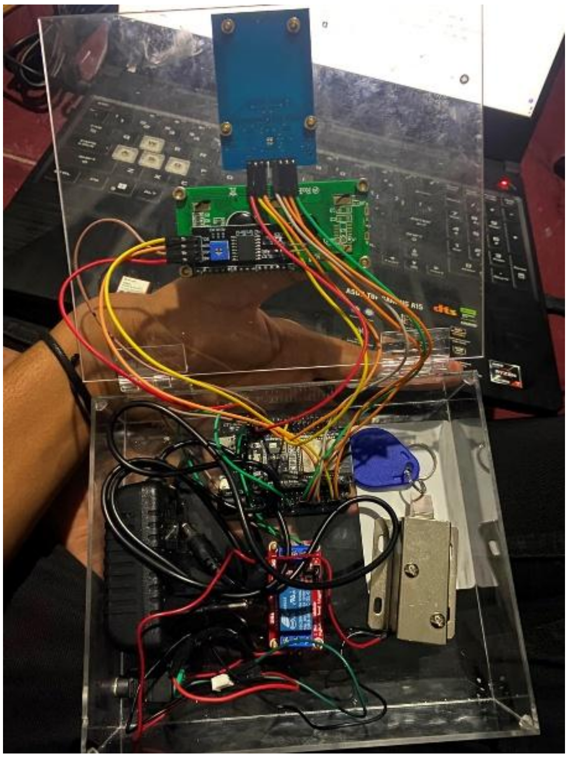


Fig. 4. Prototype Implementation of the Proposed RFID-Based Automatic Door Access Control System

During system operation, the RFID RC522 detects the RFID card and transmits the UID to the ESP8266 NodeMCU for authentication. When the detected UID matches the registered identification data, the ESP8266 generates an output signal to activate the relay module, which then controls the 12 V power supply to the solenoid door lock, unlocking the door. Conversely, when an unauthorised RFID card is detected, the relay remains inactive, and the solenoid maintains the locked position. The implementation shown in Figure 4 confirms the successful physical integration of the authentication, processing, switching, and electronic locking components into a single operational platform. Furthermore, the prototype provides an appropriate experimental platform for evaluating the functional performance of the developed system through Black Box Testing. Although the current prototype uses exposed wiring and a laboratory-scale assembly suitable for development and functional validation, future improvements could include a compact printed circuit board, optimised cable management, protective enclosures, and enhanced electrical isolation to improve the system's durability, safety, and suitability for practical installation.

3.2 Functional Testing

The functionality of the developed RFID-based automatic door access control system was evaluated using the Black Box Testing method to determine whether each hardware component and the overall integrated system operated according to the predefined functional requirements. This testing approach focuses on evaluating the relationship between system inputs and their corresponding outputs without examining the program's internal structure. During the testing process, each major hardware component, including the RFID RC522 reader, ESP8266 NodeMCU, 5 V relay module, 12 V solenoid door lock, and 16×2 I2C LCD, was evaluated based on its intended function. The testing procedure covered the complete operational sequence of the system, beginning with RFID card detection and UID reading, followed by authentication processing, relay switching, solenoid door-lock actuation, and the display of authentication status. Both authorised and unauthorised RFID cards were used as input conditions to evaluate whether the developed prototype could correctly distinguish between valid and invalid access requests. The functional testing results of the individual components and the integrated system are summarised in **Table 2**.

The authentication process begins when an RFID card is presented to the RFID RC522 reader. The reader detects the card, reads its Unique Identifier (UID), and transmits the identification data to the ESP8266 NodeMCU through the SPI communication interface. The ESP8266 then processes the received UID and compares it with the registered UID data stored in the program memory. This comparison process represents the primary decision-making stage of the proposed access control system because the subsequent operation of the relay, solenoid door lock, and LCD depends on the authentication result. When the received UID matches the registered data, the ESP8266 recognises the RFID card as an authorised credential and proceeds with the access-granting process. Conversely, when the UID does not match the stored identification data, the system flags the card as unauthorised and prevents activation of the electronic locking mechanism.

When an authorised RFID card is successfully authenticated, the ESP8266 outputs a signal via its GPIO pin to activate the 5 V relay module. The relay subsequently serves as an electronic switching interface, enabling the external 12 V DC power supply to operate the solenoid door lock. As a result, the solenoid locking mechanism is activated, and the door is unlocked for a predefined period, allowing the authorised user to enter the restricted area. Simultaneously, the 16×2 I2C LCDs an "Access Granted" message to provide immediate visual feedback regarding the authentication result. After the predefined access period has elapsed, the ESP8266 deactivates the relay, interrupts the electrical power supplied to the solenoid, and returns the door to its locked condition. This operational sequence demonstrates that the authentication, processing, switching, actuation, and display functions operate in a coordinated manner following successful user authentication.

Conversely, when an unauthorised RFID card is presented to the reader, the ESP8266 detects that the received UID does not correspond to the registered identification data. Under this condition, the microcontroller does not generate the control signal required to activate the relay module. Consequently, the relay remains inactive, the solenoid door lock maintains its locked position, and physical access to the restricted area is prevented. At the same time, the LCDs display an "Access Denied" message, indicating that the authentication process was unsuccessful. This response demonstrates the developed prototype's ability to distinguish between authorised and unauthorised RFID credentials and to generate the appropriate system output based on the authentication result.

Overall, the Black Box Testing results demonstrate the functional integration of the major hardware components within the developed prototype. The RFID RC522 successfully performs identification by reading and transmitting the UID, while the ESP8266 NodeMCU handles authentication and controls subsequent system responses. The relay module provides the required switching mechanism between the low-voltage control circuit and the 12 V solenoid door lock, whereas the LCD provides real-time visual feedback regarding the authentication status. The successful responses observed under both authorised and unauthorised access conditions indicate that the developed system performs the intended authentication-to-actuation process in accordance with the proposed system design. These results also demonstrate that the prototype can provide a functional and practical approach to local RFID-based automatic door access control without requiring continuous Internet connectivity.

3.2 System Testing

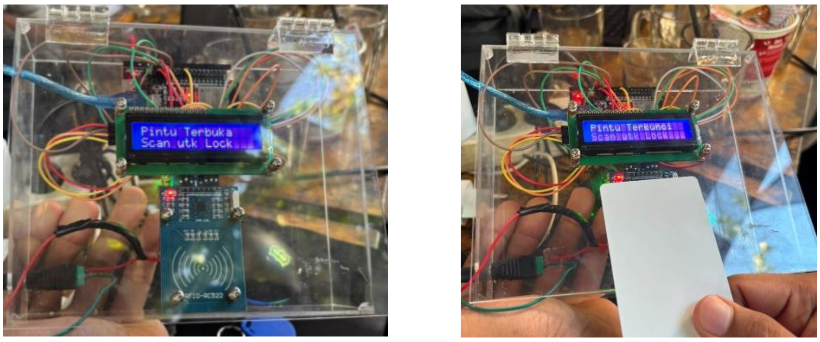
Table 2 presents the functional testing results of the main hardware components integrated into the proposed RFID-based automatic door access control system. The test results indicate that all components successfully performed their intended functions in accordance with the predefined system requirements. The RFID RC522 successfully detected the presented RFID cards and read their Unique Identifier (UID) data, which were subsequently transmitted to the ESP8266 NodeMCU for authentication processing. The ESP8266 successfully received and processed the UID data by comparing it with the registered identification data stored in the program memory. The successful performance of these two components confirms that the identification and authentication stages operated correctly and provided the necessary input for the subsequent access control process. Therefore, the RFID RC522 and ESP8266 NodeMCU demonstrated effective functional integration as the primary identification and processing components of the developed system.

Table 2. Functional Testing Results

Component	Testing Parameter	Result
RFID RC522	Reading the RFID card UID	Successful
ESP8266 NodeMCU	Processing RFID authentication	Successful
Relay Module	Switching operation	Successful
Solenoid Door Lock	Locking and unlocking mechanism	Successful
LCD I2C	Displaying authentication status	Successful

The testing results also demonstrate the successful operation of the output and actuation components. The relay module correctly performed the switching operation in response to the control signals generated by the ESP8266, thereby enabling the 12 V solenoid door lock to perform the required locking and unlocking. When an authorised RFID card was detected, the relay was activated, and the solenoid mechanism unlocked the door, while the system maintained the locked condition when unauthorised access was detected. Furthermore, the 16×2 I2C LCD successfully displayed the corresponding authentication status, providing immediate visual feedback regarding the system operation. The successful performance of all components demonstrates that the developed prototype effectively integrates the identification, authentication, processing, switching, actuation, and display functions. Overall, the results presented in **Table 2** confirm that the proposed RFID-based automatic door access control system operated in accordance with its intended functional design. However, since the current evaluation was limited to functional Black Box Testing, further quantitative testing involving RFID reading distance, authentication response time, repeated access trials, long-term operational stability, and system performance under different environmental conditions is recommended to provide a more comprehensive evaluation of the developed prototype.

Fig. 5 presents the functional testing results of the proposed RFID-based automatic door access control system under two different operational conditions: successful door unlocking and door locking. In the first condition, shown as “RFID Opened,” the system responds to the authentication process by activating the electronic locking mechanism and displaying the message “Pintu Terbuka / Scan utk Lock” on the 16×2 I2C LCD, indicating that the door has been successfully unlocked and the system is ready to receive the next RFID input for the locking process. This condition demonstrates the successful integration of the RFID RC522 reader, ESP8266 NodeMCU, relay module, solenoid door lock, and LCD. The RFID RC522 reads the UID of the presented card and transmits the identification data to the ESP8266 for processing. When the detected UID matches the registered data, the ESP8266 generates a control signal to activate the relay module, allowing the solenoid door lock to unlock. Simultaneously, the LCD provides immediate visual feedback regarding the current status of the door, confirming that the authentication, processing, actuation, and display functions operate in a coordinated manner.



RFID Opened RFID Locked

Fig. 5. Functional Testing Results of the RFID-Based Automatic Door Access Control System

The second condition, shown as "RFID Locked," demonstrates the system response during the door-locking process when the RFID card is presented again to the reader. After the card is detected and processed, the ESP8266 controls the relay and solenoid mechanism to return the door to its locked condition, while the LCDs display the corresponding locking status. The experimental observations shown in Figure 5 confirm that the developed prototype can successfully perform the complete access control sequence, including RFID card detection, UID processing, user authentication, relay switching, solenoid actuation, and real-time status display. The consistency between the input conditions and the resulting system responses supports the functional testing results presented in Table 2, in which all hardware components successfully performed their intended functions. Overall, the results demonstrate that the proposed system can reliably execute the authentication-to-actuation process and provide clear visual feedback to users during locking and unlocking operations. However, these findings primarily demonstrate the functional feasibility of the developed prototype; additional quantitative evaluations, including authentication response time, RFID reading distance, repeated-cycle reliability, false acceptance and rejection rates, and long-term operational stability, would be valuable for further assessing the system's performance and practical applicability.

The novelty of this study lies in the development and functional validation of an integrated, low-cost, and locally operated RFID-based automatic door access control system that combines the ESP8266 NodeMCU, RFID RC522 reader, 5 V relay module, 12 V solenoid door lock, and 16×2 I2C LCD within a unified authentication-to-actuation architecture. Unlike previous studies that predominantly emphasise IoT-based remote monitoring, web-based access management, database connectivity, or individual access control components, the proposed system focuses on reliable standalone operation without dependence on continuous Internet connectivity. The system integrates the complete operational sequence, including RFID card detection, UID-based user authentication, embedded data processing, electronic switching, physical door locking and unlocking, and real-time visual feedback, followed by functional validation using the Black Box Testing method. Therefore, the principal contribution of this study is not merely the use of RFID and ESP8266 technologies but the systematic implementation and evaluation of a complete, network-independent access control prototype that provides a simple, practical, and expandable platform for room security applications and future developments involving access logging, database integration, enhanced authentication mechanisms, and IoT-based remote monitoring.

4. Conclusion

This study successfully developed and functionally evaluated an RFID-based automatic door access control system using the ESP8266 NodeMCU as the main processing and control unit. The developed prototype integrates an RFID RC522 reader for UID-based user identification, an ESP8266 NodeMCU for authentication processing and system control, a 5 V relay module for electronic switching, a 12 V solenoid door lock for physical access control, and a 16×2 I2C LCD for providing real-time system status information. The proposed system was implemented as a locally operated and network-independent access control architecture that performs the complete authentication-to-actuation process, including RFID card detection, UID reading and validation, authentication decision-making, relay switching, physical door locking and unlocking, and visual feedback to the user without requiring continuous Internet connectivity.

The functional performance of the developed prototype was evaluated using the Black Box Testing method under both authorised and unauthorised access conditions. The experimental results demonstrated that all integrated hardware components successfully performed their intended functions in accordance with the predefined system requirements. The RFID RC522 successfully detected RFID cards and transmitted the corresponding UIDs to the ESP8266 NodeMCU, while the microcontroller correctly processed the authentication data and generated appropriate control signals based on the authorisation status. When an authorised RFID card was detected, the system successfully activated the relay and solenoid door lock to provide physical access while simultaneously displaying the corresponding door status on the LCD. Conversely, when an unauthorised RFID card was presented, the system maintained the locked condition and provided appropriate visual feedback. These results confirm the successful functional integration of the identification, authentication, processing, switching, actuation, and display subsystems within a single operational prototype.

Overall, the developed system demonstrates the functional feasibility of a low-cost, practical, and integrated RFID-based automatic door access control solution. The principal contribution of this study lies in the implementation and functional validation of a complete local authentication-to-actuation architecture that combines RFID-based UID authentication, embedded processing, electronic switching, physical door control, and real-time user feedback without dependence on continuous Internet connectivity. Nevertheless, the current evaluation was limited to functional Black Box Testing; therefore, the findings primarily demonstrate the operational feasibility of the developed prototype rather than comprehensive security or long-term reliability performance. Future research should include quantitative evaluations of authentication response time, RFID reading distance, repeated locking and unlocking cycles, false acceptance and rejection rates, power consumption, and long-term operational stability. Further developments may also incorporate secure user database management, digital access logging, enhanced RFID authentication mechanisms, compact printed circuit board design, improved electrical protection and system enclosure, as well as IoT-based remote monitoring to extend the proposed prototype toward more robust and practical real-world access control applications.

Acknowledgement

The author would like to express sincere gratitude to the Faculty of Engineering, Universitas Serambi Mekkah, for providing the facilities, resources, and academic support necessary for the completion of this research. Appreciation is also extended to the academic supervisors and colleagues for their valuable guidance, constructive suggestions, and technical assistance throughout the design, development, implementation, and testing of the RFID-based automatic door access control system. The author further acknowledges all individuals who directly or indirectly contributed to the successful completion of this study and the preparation of this article.

References

Adams, D., & Giap, Y. C. (2024). Prototype of an automatic door and fire alarm system based on IoT. Bit-Tech, 6(3), 363–370. DOI

Araújo, D. dos S., & Lemes, M. T. (2025). IFGAccess: Sistema de controle de acesso web utilizando RFID e o microcontrolador ESP8266. Revista Eletrônica de Iniciação Científica em Computação, 23, 55–62. DOI

Basyir, A., & Nurwijayanti, K. N. (2022). Perancangan sistem keamanan pintu ruangan otomatis berbasis RFID pada Internet of Things (IoT). Jurnal Ilmiah MATRIK, 24(1), 21–27.

Singh, S., Sazid, M., Kumar, V., & Kaur, M. N. (2024). Smart door lock using ESP8266 using IoT. SSRN Electronic Journal. DOI

Kassim, S. O., Idriss, A. S., & Ahmed, A. I. (2023). Implementation of a sustainable security architecture using Radio Frequency Identification (RFID) technology for access control. International Journal of Sustainable Development and Planning, 18(4), 1059–1067.

Caballero-Gil, P., Caballero-Gil, C., & Molina-Gil, J. (2022). RFID authentication protocol based on a novel EPC Gen2 PRNG. Sensors, 22(16), 6266.

Wang, Y., Liu, R., Gao, T., Shu, F., Lei, X., Wu, Y., Gui, G., & Wang, J. (2023). A novel RFID authentication protocol based on a block-order-modulus variable matrix encryption algorithm. IEEE Internet of Things Journal.

Khando, K., Islam, M. S., Gao, S., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267.

Pal, S., Hitchens, M., Rabehaja, T., & Mukhopadhyay, S. (2021). Security requirements for the Internet of Things: A systematic approach. Sensors, 21(17), 5897.

Ferrag, M. A., Shu, L., Choo, K.-K. R., & Yang, X. (2021). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. IEEE Access, 9, 32031–32053.

Hameed, S., Khan, F. I., & Hameed, B. (2021). Understanding security requirements and challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2021, Article 9629381.

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2021). Internet of Things security: A survey. Journal of Network and Computer Applications, 182, 103027.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2021). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things Journal, 8(8), 6477–6501.

Tewari, A., & Gupta, B. B. (2021). Security, privacy and trust of different layers in the Internet-of-Things (IoTs) framework. Future Generation Computer Systems, 108, 909–920.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2021). A survey of machine- and deep-learning methods for Internet of Things security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2022). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146–164.

Ishaq, K., & Bibi, S. (2023). IoT-based identification systems: A systematic literature review. IEEE Access, 11, 84931–84950.

Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., & Castedo, L. (2024). Security analysis of commercial RFID tags for Internet of Things applications. Sensors, 24, Article 3175.

Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., Nasser, N., & Ali, A. (2022). A machine-learning approach to blockchain-based smart home network security. IEEE Network, 35(3), 223–229.

Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2022). Biometrics for Internet of Things security: A review. Sensors, 21(18), 6163.