International Journal of Applied Mathematics and Computing
E-ISSN: 3047-146X
P-ISSN: 3048-1988
IJAMC

*Research Article*

# Implementation of an RFID Card-Based Automatic Door Lock System Using NodeMCU with Integration of Telegram Notifications and IoT Services

**Frencis Matheos Sarimole[1*], Satria Wira Yudha[2], Sutisna[3], Roid Adip Akmal[4]**

[1]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: frencis@stikomcki.ac.id
[2]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: satriawirayudha@stikomcki.ac.id
[3]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia;
email: sutisna@stikomcki.ac.id
[4]Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika Jakarta, Indonesia
*****Corresponding Author: frencis@stikomcki.ac.id

**Abstract:** In the digital era, the demand for practical and efficient security systems has significantly increased, particularly in the context of access control for restricted rooms or buildings. This research aims to develop an automatic door locking system utilizing an RFID card and a NodeMCU ESP32 microcontroller integrated with Internet of Things (IoT) technology through real-time notifications using the Telegram application. The system is designed to replace conventional locking methods that often present various weaknesses, such as key loss, physical duplication, and lack of remote access capabilities. The development method employed is the Research and Development (R&D) approach, consisting of needs analysis, system design, hardware and software implementation, followed by testing and evaluation. The main components used in the system include the RC522 RFID reader for user identification, Espressif manufactures the ESP-32 microcontroller, which is equipped with Wi-Fi and Bluetooth modules to enable wireless internet connections. NodeMCU ESP32 as the control center and internet connector, a relay module as an electronic switch, and a solenoid door lock as the actuator. The results show that the system is capable of accurately reading RFID card UIDs, granting access to registered cards, activating the solenoid to unlock the door, and sending access status notifications to Telegram in an average of less than three seconds. The system also effectively denies access to unregistered cards and sends warning messages accordingly. Therefore, this system enhances the security and efficiency of room access control and has the potential to be adopted as a prototype solution in the development of smart homes or modern access control systems.

**Keywords:** IoT; NodeMCU ESP32; RFID; Solenoid; Telegram Bot.

**Received: 11 August 2025**
**Revised: 20 September 2025**
**Accepted: 16 October 2025**
**Published: 30 October 2025**
**Curr. Ver.: 30 October 2025**



## 1. Introduction

In today's era of digitalization and automation, the demand for intelligent and efficient security systems continues to increase, particularly in managing physical access to homes, offices, and other institutions. Conventional security systems that rely solely on mechanical keys or manual security measures are increasingly considered inadequate due to their vulnerability to criminal activities such as theft, key duplication, and key loss. Along with technological advancements, various Internet of Things (IoT)-based solutions have emerged, enabling real-time monitoring and control, even from remote locations (Cholilalah & Arifin, 2019; Budiyanti, 2021; Salim & Mursalim, 2025). This development has encouraged innovation in the design of automatic door locking systems that are more secure, practical, and integrated (Saghoa et al., 2018; Setiawan et al., 2022).

Radio Frequency Identification (RFID) is one of the wireless identification technologies widely used in various applications, including security systems. This study implements an IoT-based automatic room door system utilizing RFID microcontroller technology (Ridho et al., 2024). RFID operates by reading data stored on tags or cards without requiring direct physical contact (Asshiddiqi et al., 2022). This technology offers speed and convenience in user authentication and can be applied to regulate access to specific rooms or facilities (Fadila & Djaksana, 2021). The combination of RFID and microcontrollers such as NodeMCU provides significant opportunities to develop automatic locking systems that not only electronically unlock doors but are also capable of connecting to the internet and performing intelligent data processing (Ridho et al., 2024; Fadila & Djaksana, 2021).

NodeMCU, as an ESP-based microcontroller equipped with Wi-Fi and Bluetooth connectivity capabilities, has become an ideal choice for IoT-based projects (Wicaksono & Rahmatya, 2020). ESP32, introduced by Espressif Systems, is a microcontroller that serves as the successor to the ESP8266 (Nugroho et al., 2021). In this study, it is assumed that the automatic entrance door will close after a person enters or exits the room (Prafanto et al., 2021). By utilizing NodeMCU, the automatic door locking system can be connected to the internet, enabling integration with various online services (Makatita et al., 2024). One of the services that can be integrated is Telegram, an instant messaging application that supports bots and automated notifications. By leveraging this feature, the system can send real-time notifications to users whenever door access attempts are successful or unsuccessful (Ridho et al., 2024).

In addition to Telegram, the system can be further enhanced by integrating it with IoT platforms such as Blynk, ThingSpeak, or Firebase (Fakhruddin, 2024; Setiawan et al., 2022). These platforms enable users to monitor access logs, configure the system remotely, and store data in real time on cloud servers (Fakhruddin, 2024; Kusumah et al., 2023). This provides added value in terms of flexibility and scalability for implementing technology-based security systems.

The development of an automatic door locking system based on RFID, NodeMCU, and integration with Telegram and IoT services has significant potential to address modern security needs. Besides improving user efficiency and convenience, the system also offers better control over who is authorized to access specific rooms or areas (Ridho et al., 2024; Asshiddiqi et al., 2022). Furthermore, with notification and remote monitoring features, users can quickly respond to potential security threats as they arise (Fakhruddin, 2024; Setiawan et al., 2022).

Based on this background, the authors are interested in designing and implementing an automatic door locking system that combines RFID technology as an authentication tool, an ESP32-based NodeMCU as the main controller, and integration with the Telegram application and IoT services to enhance real-time monitoring and notification functions. It is expected that this research will contribute significantly to the development of intelligent technology-based security systems that can be widely implemented, particularly in residential and office environments.

## 2. Literature Review

### Automatic Door Lock System

An automatic door lock system is a device designed to control entry and exit access digitally without requiring physical keys. The system utilizes electronic mechanisms controlled by a microcontroller to lock or unlock doors based on signals received from input devices such as RFID cards, fingerprint scanners, or PIN codes. In this study, an RFID-based automatic door locking system is implemented to enhance security and operational efficiency (Ridho et al., 2024; Fadila & Djaksana, 2021).

### Radio Frequency Identification (RFID)

**Figure 1.** Radio Frequency Identification (RFID).

RFID is an automatic identification technology that uses radio waves to read data stored on tags or cards. An RFID card contains a chip and an antenna capable of transmitting information to an RFID reader when it is within the reader's operating range. RFID technology is widely applied in access control systems due to its ability to perform user authentication without requiring direct physical contact (Asshiddiqi et al., 2022; Ridho et al., 2024).

**NodeMCU ESP32**

**Figure 2.** NodeMCU ESP32.

NodeMCU ESP32 is a microcontroller development board equipped with Wi-Fi and Bluetooth connectivity capabilities, making it highly suitable for Internet of Things (IoT) applications. Compared with its predecessor, the ESP8266, the ESP32 offers higher processing performance, a greater number of input/output pins, and improved power efficiency. In this study, the ESP32 functions as the main controller of the door locking system, integrating the RFID module, locking mechanism, and cloud-based or Telegram services (Nugroho et al., 2021; Wicaksono & Rahmatya, 2020).

**Telegram Notification**

Telegram is a cloud-based instant messaging application that supports the creation of bots for sending and receiving automated messages. Through the Telegram Bot API, the system can send notifications directly to users whenever door access activities occur. This feature provides real-time monitoring capabilities and enhances security by allowing users to receive immediate updates regarding successful or failed access attempts (Ridho et al., 2024).

**Internet of Things (IoT)**

The Internet of Things (IoT) refers to a concept in which physical devices are connected to the internet and can communicate and exchange data automatically. In the context of this study, IoT is utilized to connect the door locking system with cloud services, enabling remote monitoring and control of the door from different locations (Kusumah et al., 2023; Cholilalah & Arifin, 2019). This technology enhances the flexibility, scalability, and effectiveness of digital security systems (Budiyanti, 2021; Salim & Mursalim, 2025).

## 3. Materials and Method

**Data Type and Source**

This study uses primary data obtained directly through observation and testing of an RFID- and NodeMCU ESP32-based automatic door locking system prototype. The collected data include RFID card identification (UID) readings, system responses during the authentication process, activation times for door locking and unlocking mechanisms, and the speed and reliability of notification delivery through the Telegram application. All data were obtained from testing the developed system under operational conditions that were aligned with the objectives of the study.

**Research Method**

This study employed the Research and Development (R&D) method, which aims to produce a product in the form of an Internet of Things (IoT)-based automatic door locking system prototype. This method was selected because the research focuses not only on analyzing a phenomenon but also on the design, development, implementation, and evaluation of a system that can be applied in real-world environments. The research stages consisted of requirements analysis, system design, system implementation, system testing, and system evaluation.

**Requirements Analysis**

The requirements analysis stage was conducted to identify problems associated with conventional door locking systems. The analysis focused on various weaknesses of physical keys, such as the risks of loss, forgery, and duplication. In addition, user requirements for a security system that is more practical, secure, and capable of real-time monitoring were identified. The analysis results indicated that the developed system should incorporate RFID-

based authentication, automated control using NodeMCU ESP32, and Telegram-based notification features to improve security and facilitate room access monitoring.

**System Design**

The system design stage covered both hardware and software design. Hardware design involved configuring the connections among the NodeMCU ESP32, RFID RC522 module, relay, solenoid door lock, and internet network used for data communication. On the software side, the design process included developing a system flowchart, control logic, and program code using Arduino IDE. In addition, Telegram Bot API configuration was performed to enable automatic access notifications for users. The outcome of this stage was a comprehensive system design that served as the foundation for implementation.

**System Implementation**

The implementation stage involved assembling all components according to the previously developed design. The NodeMCU ESP32 was programmed to read RFID card UIDs, verify user data, control the relay and solenoid as door locking and unlocking mechanisms, and send notifications to Telegram based on the user's authentication status. At this stage, Wi-Fi network configuration and Telegram Bot integration were also performed using a previously generated authentication token. After the integration process was completed, each component was tested incrementally to ensure that all system functions operated according to the design specifications.

**System Testing**

System testing was conducted using an experimental approach by evaluating the developed prototype under various operational scenarios. The testing process aimed to assess the performance, reliability, and stability of the system in performing its primary functions. The first test focused on RFID card reading functionality to ensure that the system could correctly recognize registered UIDs. Subsequently, relay and solenoid activation tests were conducted to measure the system response time from the moment an RFID card was scanned until the door was unlocked or locked. Additional testing was performed on the Telegram notification feature to verify that access information was delivered to users in real time.

In addition to functional testing, endurance testing was conducted through repeated door opening and closing simulations over a specified period. This test aimed to identify potential performance degradation, response delays, or actuator malfunctions resulting from continuous use. To evaluate the security aspect, several testing scenarios were performed, including the use of unregistered RFID cards, unauthorized access simulations, and repeated card scans within a very short time interval (multiple tapping). These tests were intended to determine the system's ability to prevent unauthorized access. The parameters observed in this study included RFID card reading accuracy, system response time, door locking and unlocking activation duration, Telegram notification delivery success rate, system stability during repeated operation, and system reliability under unauthorized access scenarios.

**System Evaluation**

The evaluation stage was conducted based on the results obtained from system testing. The evaluation focused on the RFID authentication success rate, system response speed, effectiveness of Telegram notifications, and system reliability under various operational and network conditions. The evaluation results were used to determine the feasibility of implementing the system in real-world environments and to formulate recommendations for future development. Potential improvements include the addition of an access log feature, implementation of multi-factor authentication, and database integration for dynamic RFID user management. Through systematic development and testing procedures, the proposed automatic door locking system is expected to provide an effective and practical security solution while supporting the implementation of Internet of Things technology in access control applications.

## 4. Results and Discussion

**System Implementation**

The implementation was carried out by assembling all the main components of the system, namely: 1) The NodeMCU ESP32 was programmed through the Arduino IDE using the C# programming language and functioned as the central system controller. 2) The RFID RC522 module was connected to the ESP32 through SPI communication to read card UIDs. 3) The relay functioned as an electronic switch that received signals from the ESP32 to activate the solenoid. 4) The solenoid door lock was connected to a 12V power supply and controlled through the relay, allowing the door to open automatically for 5 seconds when a

valid RFID card was detected. 5) The Telegram Bot was used as a notification delivery medium for users. Every door access event, whether successful or unsuccessful, was recorded and sent via Telegram messages to designated users.

**System Testing**

Testing was conducted to evaluate the functionality and stability of the system comprehensively. The testing included:

a) RFID Card Reading Function Test

This scenario aimed to test whether the system could recognize registered cards and reject unauthorized cards. RFID cards were placed on the RC522 module, and the system was required to respond by activating the solenoid and sending notifications to Telegram.

b) Door Locking and Unlocking Response Test

The test examined whether the solenoid activated to unlock the door for 5 seconds after a valid card was accepted and then automatically relocked the door. The average response time from card tapping until the door opened was approximately 1.2 seconds.

c) Telegram Notification Delivery Test

This test verified the system's ability to send notifications through Telegram. The results showed that notifications were delivered on average in less than 3 seconds after an action was performed.

d) System Stability Test

The system was tested under repeated usage conditions (≥20 card taps) to determine whether any performance degradation or functional failures occurred. The results indicated that the system remained stable and experienced no disruptions.

e) Failed Access Condition Test

A simulation was performed using an unregistered card. The system successfully denied access and sent a rejection notification to Telegram.

Based on all testing results, the developed system was able to function according to the specified requirements. The system was capable of automatically controlling door access using RFID cards, providing real-time access information, and demonstrating adequate durability and responsiveness in actual usage scenarios.

**Final Testing Results**

This chapter presents the final testing results of the RFID card and NodeMCU ESP32-based automatic door locking system operated without a Wi-Fi connection. Testing was conducted to ensure that the system could continue operating locally, securely, and reliably under offline conditions.

a) Validation of Basic RFID System Functions

Testing was conducted to determine whether the system could recognize RFID cards, verify user data, and automatically control the door lock actuator without relying on a network connection. Test Scenarios: Use of RFID cards registered in EEPROM. Use of unknown RFID cards. Repeated testing for durability validation.

Results: a) Authorized RFID cards successfully unlocked the door automatically. b) Unknown cards were rejected, and the system displayed the status "Access Denied" through the LCD or LED indicator. c) The average system response time from card tapping until the door opened was approximately ±1.1 seconds.

b) Local Data Storage Testing

Since the system did not use a Wi-Fi network, user UID data were stored directly in local memory, such as EEPROM or a microSD module. Test Results: a) Stored UID data could be read and recognized by the system without disruption. b) The EEPROM was capable of storing up to 50 UIDs without issues. c) Data deletion and addition could be performed through the system's control button (admin button).

c) System Resistance to Electrical and Environmental Disturbances

This test aimed to determine whether the system remained stable under power disturbances or variations in ambient temperature. Results: a) When the voltage dropped below 4.8V, the system became unstable and frequently failed to read RFID cards. b) Under normal 5V conditions, the system operated stably for 48 hours continuously. Exposure to room temperature heat (35°C) did not significantly affect performance.

d) Evaluation of Offline Research Objectives

The initial objective of this research was to develop an RFID-based automatic locking system capable of operating independently without an internet connection. The evaluation results of the objectives are presented below:

**Table 1**. Evaluation of Offline Research Objectives.

| Objective | Status | Result |
|---|---|---|
| Develop an RFID-based automatic door locking system | Achieved | The system is capable of automatically opening and closing the door using an RFID card. |
| Integrate the system with NodeMCU ESP32 | Achieved | The ESP32 functions as the central controller for the system logic. |
| Store and read user data locally | Achieved | EEPROM is utilized as local storage for user UID data. |
| Provide an independent security system without network connectivity | Achieved | The system remains fully operational without a Wi-Fi connection. |

e) Testing Example

**Table 2.** Testing Example.

| Scenario | Input | System Response | Response Time |
|---|---|---|---|
| Valid RFID card tapped | UID: A1B2C3D4 | Relay activated, door unlocked, green LED turned on | ±1.1 seconds |
| Unrecognized RFID card tapped | UID: X9Y8Z7 | Red LED turned on, buzzer activated, door remained locked | ±1.0 second |
| Door remains open for more than 5 seconds | Timeout | System automatically relocked the door | 5 seconds |

The testing results showed that the system could operate effectively even without an internet network connection. The system remained capable of performing its primary function as an RFID-based access controller, equipped with relay control for automatically opening and closing doors. Local data storage makes this system highly suitable for use in areas with limited Wi-Fi connectivity, such as remote locations, warehouses, or restricted-access rooms.

## 5. Conclusion and Recommendations

### Conclusion

Based on the design, implementation, and testing results of the RFID Card and NodeMCU-Based Automatic Door Lock System with Telegram Notification Integration and IoT Services, several conclusions can be drawn as follows: 1) The system is capable of identifying registered RFID cards with high accuracy, ensuring that only authorized users can unlock the door. 2) The integration of the NodeMCU with IoT services functions as intended, where every door access activity can be transmitted as a real-time notification through the Telegram application. 3) The testing results indicate that the system can operate consistently without requiring a permanent Wi-Fi connection by utilizing a local data storage mechanism before synchronization is performed when network connectivity becomes available. 4) The hardware and software designs effectively complement each other to create a security solution that is efficient, responsive, and user-friendly.

### Recommendations

To further enhance the system and accommodate broader application requirements, the following recommendations are proposed: 1) Implementation of Backup Power Sources: A backup power supply system, such as rechargeable batteries, should be added to ensure continuous operation during power outages. 2) Integration of Additional Sensors: Fingerprint recognition or facial recognition sensors can be incorporated to enhance security by providing multiple layers of authentication. 3) Development of a Mobile Application: A dedicated Android/iOS application can be developed to manage RFID card registrations, monitor access history, and perform device firmware updates directly. 4) Network Connectivity Optimization: The use of GSM/4G communication modules may be considered to enable direct notification delivery without relying on local Wi-Fi network availability.

## References


Asshiddiqi, F. F., Triayudi, A., & Aldisa, R. T. (2022). Pembangunan smart detection absensi berbasis kartu RFID dan ESP32. *Jurnal Sistem Komputer dan Informatika, 4*(1), 204–211. https://doi.org/10.30865/json.v4i1.4912

Budiyanti, R. T. (2021). *Buku ajar Internet of Things.*

Cholilalah, A. I. H., & Arifin, R. (2019). *Fundamental Internet of Things (IoT): Teori dan aplikasi.*

Erwin, E. M. Y., & Pratama, F. (2023). Rancang bangun sistem monitoring suhu dan kelembaban ruang server berbasis IoT menggunakan Arduino pada PT Bintaro Serpong Damai. *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan), 7*(1), 15–22. https://doi.org/10.47970/siskom-kb.v7i1.453

Fadila, F., & Djaksana, Y. M. (2021). Prototype sistem pengaman pintu menggunakan elektronik kartu tanda penduduk (E-KTP) berbasis NodeMCU ESP8266. *Prosiding Seminar Informatika dan Sistem Informasi, 6*, 60–75. http://openjournal.unpam.ac.id/index.php/SNISIS/article/view/14908

Fakhruddin, A. (2024). Rancang bangun sistem keamanan pintu rumah berbasis Internet of Things dengan ESP32 dan aplikasi Blynk. *E-Link: Jurnal Teknik Elektro dan Informatika, 19*(1), 53–61. https://doi.org/10.30587/e-link.v19i1.7600

Holc, J. P., et al. (2017). *Internet of Things: Konsep dan implementasi.*

Kiswanta, K. (2018). Rancang bangun panel kontrol selenoid valve sistem terbuka berbasis program dan manual pada untai uji beta (UUB). *EPIC Journal of Electrical Power, Instrumentation and Control, 2*(1). https://doi.org/10.32493/epic.v2i1.1299

Koru, N., Patiran, A. Z., & Baisa, L. Y. (2024). Internet of Things (IoT) sistem monitoring suhu, kelembapan dan intensitas cahaya pada ruang penyimpanan obat. *5*(2), 538–542.

Kurniati, S., Syam, S., & Bantoruan, F. L. (2021). Sistem pemanas induksi dengan menggunakan solenoid coil dan mikrokontroler. *Jurnal Media Elektro, 10*(1), 44–52. https://doi.org/10.35508/jme.v0i0.3902

Kurniawan, B. S. M. C. (2021). Rancang bangun sistem monitoring suhu dan kelembapan ruang server pada PT Untung Bersama Sejahtera Surabaya (pp. 50–62).

Kurniawan, Y., & Zulkifli, Z. (2019). Rancang bangun pembangkit listrik menggunakan solenoida dengan pemanfaatan fluks magnet. *RELE (Rekayasa Elektrikal dan Energi), 2*(1), 9–13. https://doi.org/10.30596/rele.v2i1.3111

Kusumah, R., Islam, H. I., & Sobur, S. (2023). Sistem monitoring suhu dan kelembaban berbasis Internet of Things (IoT) pada ruang data center. *Journal of Applied Informatics and Computing, 7*(1), 82–88. https://doi.org/10.30871/jaic.v7i1.5199

Makatita, N. F., Dwicahya, & Hakim, A. (2024). MQTT protocol-based ESP-32 smarthome with multi-sensor recognition. *Journal of Electrical, Electronics, Information, Communication Technology, 6*(1), 29–36.

Mambang. (2021). *Buku ajar teknologi komunikasi internet (Internet of Things).* https://www.researchgate.net/publication/360289401

Mukhtar, A., Hermana, R., Burhanudin, A., & Setyoadi, Y. (2023). *Sensor dan aktuator: Konsep dasar dan aplikasi*. CV Widina Media Utama.

Perbandingan kinerja Arduino Uno dan ESP32 terhadap pengukuran arus dan tegangan. (2021). *Jurnal Otomasi, Kontrol dan Instrumentasi, 13*(1), 35–47. https://doi.org/10.5614/joki.2021.13.1.4

Prafanto, A., Budiman, E., Widagdo, P. P., Putra, G. M., & Wardhana, R. (2021). Pendeteksi kehadiran menggunakan ESP32 untuk sistem pengunci pintu otomatis. *JTT (Jurnal Teknologi Terapan), 7*(1), 37–43. https://doi.org/10.31884/jtt.v7i1.318

Ridho, I. I., Maulani, J., & Muharir, M. (2024). Implementasi IoT pintu otomatis berbasis microcontroller RFID menggunakan MQTT dan Bot Telegram. *Smart Comp: Jurnalnya Orang Pintar Komputer, 13*(2), 247–251. https://doi.org/10.30591/smartcomp.v13i2.5796

Saghoa, Y. C., Sherwin, R. U. A., & Sompie, N. M. T. (2018). Kotak penyimpanan uang berbasis mikrokontroler Arduino Uno. *Jurnal Teknik Elektro dan Komputer, 7*(2), 167–168.

Salim, M., & Mursalim. (2025). *E-book Internet of Things (IoT)*.

Setiawan, D., Jaya, H., Nurarif, S., Syahputra, T., & Syahril, M. (2022). Implementasi ESP32-CAM dan Blynk pada WiFi door lock system menggunakan teknik duplex. *Jurnal Sains Sosial Research, 5*(1), 159–166. https://doi.org/10.54314/jssr.v5i1.807

Sunardi, Yudhana, A., & Furizal. (2023). Tsukamoto fuzzy inference system on Internet of Things-based for room temperature and humidity control. *IEEE Access, 11*, 6209–6227. https://doi.org/10.1109/ACCESS.2023.3236183

Syihabuddin, A., & Abidin, Z. (2020). Sistem monitoring dan evaluasi nilai siswa berbasis dashboard berdasarkan key performance indicator (Studi kasus: SMP Kartika II-2 Bandarlampung). *Jurnal Teknologi dan Sistem Informasi, 1*(2), 17–25. https://doi.org/10.33365/jtsi.v1i2.360

Wicaksono, M. F., & Rahmatya, M. D. (2020). Implementasi Arduino dan ESP32 CAM untuk smart home. *Jurnal Teknologi dan Informasi, 10*(1), 40–51. https://doi.org/10.34010/jati.v10i1.2836