Implementation of an RFID RC522 and IoT-Based Automatic Door Security System in an Electrical Engineering Laboratory

[1*]Yudi Wijanarko, [2]Niksen Alfarizal, [3]Muhammad Regi Pratama
[1,2]Electrical Engineering Department, State Polytechnic of Sriwijaya, Indonesia
Email: [1]wijanarko_yudi@polsri.ac.id, [2]Niksenbae90@gmail.com,
[3]muhammadregipratama96@gmail.com

Article Info

Article history:
Received May 15th, 2025
Revised Jun 14th, 2025
Accepted Jul 30th, 2025

Keyword:
ESP32
Internet Of Things (IoT)
RFID RC522
Smart Door Lock
Smart Room

ABSTRACT

The development of smart home technology has encouraged the development of more efficient and integrated automatic security systems, Using RFID technology with the Internet of Things (IoT) is one method that can be applied. This research aims to implement an automatic door security system based on RFID RC522 connected to the IoT network in the Electrical Engineering Laboratory. The research method used is Research and Development (RnD) through the process of designing, making, and testing system prototypes. The system is controlled by an ESP32 microcontroller, uses an RC522 RFID module for authentication, and utilizes relays and solenoid door locks as locking mechanisms. Test results show that the maximum effective RFID reading distance is 5 cm, with a fast and accurate response at a distance of 1 to 4 cm. The system can log all access activities directly through the IoT platform and distinguish between valid and invalid cards. In terms of power consumption, the door lock solenoid has the largest power usage when active at 7.2 W, while other components remain efficient. The implementation of this system is proven to be able to improve the security aspects and ease of access monitoring in the laboratory room automatically and connected.

Corresponding Author:
Yudi Wijanarko,
Electrical Engineering Department,
State Polytechnic of sriwijaya,
Jl Srijaya Negara Bukit Besar Palembang, South Sumatra, Indonesia
Email: wijanarko_yudi@polsri.ac.id

DOI: http://dx.doi.org/10.24014/ijaidm.v8i2.37007

1. INTRODUCTION

The rapid development of digital technology has significantly influenced various sectors, including industry, education, and everyday life. In the field of education, particularly in engineering programs, laboratories play an essential role as facilities for practical learning and scientific experimentation [1]. The Electrical Engineering Laboratory, for example, enables students to explore fundamental concepts in electricity, electronics, and control systems through hands-on activities that involve sensitive and high-value equipment. Therefore, ensuring security becomes a primary concern in laboratory management. Uncontrolled access may lead to equipment damage, misuse of facilities, and asset loss, making it necessary to implement an access control system that restricts usage to authorized individuals only.

Conventional locking systems that rely on physical keys are now considered inefficient and offer low security because they are easy to lose, duplicate, or misuse. Similarly, password-based systems are not fully reliable, as they remain vulnerable to data theft and various security breaches [2]. Although biometric technologies such as fingerprint and facial recognition offer high accuracy, the relatively high implementation and maintenance costs make them less suitable for certain institutions. Thus, a secure, efficient, cost-effective, and easily integrable access control solution is needed.

Radio Frequency Identification (RFID) and the Internet of Things (IoT) present promising alternatives for enhancing modern security systems [3]. RFID enables contactless user identification, allowing authentication to be carried out more quickly and conveniently than manual methods. Meanwhile, IoT expands system capabilities through real-time data communication, remote monitoring, and internet-based network integration [4]. The combination of these technologies produces an automatic authentication system equipped with centralized access logging and monitoring, making it highly suitable for laboratory environments that require both efficiency and a high level of security.

Several recent studies have examined the integration of RFID and the IoT in security and access control systems. Aisyah et al.(2022) developed an RFID-based door lock prototype that demonstrated reliable user authentication, although the system did not yet support internet-based remote monitoring. Diantoro and Rohmatullahama (2023) designed an IoT-based restricted access security system for industrial environments; however, its implementation remained limited to a local system without real-time activity logging. Nova Amalia and Muhammad (2024) proposed an RFID–IoT-based door security system, but their research primarily focused on basic locking functions and did not address power efficiency or multiuser integration capabilities. Fakhruddin et al.(2024) developed a home door security system using IoT with an ESP32 and the Blynk application, but the system was not tailored for laboratory environments, which typically involve more complex usage requirements. In addition, the study by Zulkarnaen and Al Koriah (2024), which combined RFID and IoT for home door access, emphasized sensor variation rather than conducting a comprehensive performance evaluation in multi-access scenarios.

Based on previous studies, the integration of RFID and IoT holds significant potential for developing smart and efficient access control systems. However, some studies still encounter challenges related to cost, data security, and adaptability to dynamic educational environments. Therefore, this study focuses on the design and implementation of an RFID- and IoT-based smart door-lock system for an Electrical Engineering laboratory, aiming to provide secure, efficient, and real-time monitored access control.

1. Identifying system performance in the user authentication process using RFID cards.
2. Evaluating power consumption efficiency and the effectiveness of IoT integration in real-time access monitoring.
3. Delivering secure, efficient, and easy-to-implement access control solutions in educational laboratory environments.

The novelty of this research lies in its low-cost system architecture, which enables centralized internet-based monitoring while addressing the limitations of previous studies that relied solely on local control and lacked optimal scalability.

2. LITERATURE REVIEW

Research on RFID and IoT-based access control systems has been conducted extensively in recent years, in line with the increasing need for security and efficiency in digital systems. Several relevant studies were used as references in this research to review technological developments and identify research gaps that can be further explored [5].

Research on the integration of RFID and IoT technologies in access control systems has been widely conducted in recent years. Study in, investigated the development of an RFID ID-12–based door lock prototype [6]. The study began with the configuration of the RFID reader module, which was connected to a microcontroller, followed by tests on reading distance and authentication accuracy. The results showed that the system was able to read cards reliably and provide accurate lock–unlock responses. The main advantage of this study lies in its high reading accuracy. However, its limitation is the absence of remote access monitoring, as the system was not connected to an IoT platform.

In a subsequent study, a restricted-access security system was designed that integrated RFID with IoT connectivity in an industrial environment. Their research included hardware design, local server development, and user access testing in controlled areas [7]. The system successfully identified RFID cards and recorded access activities. Its strength is the improved access security within industrial facilities. Nevertheless, the data storage mechanism remained local, preventing real-time monitoring of access activities.

Furthermore, research in developed an RFID–IoT–based door security system. The research began with configuring the RFID module and microcontroller connected to Wi-Fi, followed by performance testing of the automatic locking mechanism [8]. The results indicated that the system operated reliably in terms of authentication and could be monitored through the internet. However, the study did not address power efficiency, leaving the system’s suitability for long-term operation undetermined.

IoT-based security systems were also developed using an ESP32 microcontroller integrated with the Blynk application [9]. The study involved integrating sensors, control components, and an IoT platform. The findings showed that users could remotely monitor door conditions and control a solenoid lock via smartphone. The system’s strength is its monitoring flexibility, but the study was intended for home applications and did not consider multiuser scenarios commonly encountered in laboratory environments.

Meanwhile, research in introduced an innovative approach by combining RFID wristbands with IoT-based voice recognition technology. Their research included prototype development, voice sensor configuration, and dual-authentication testing [10]. The results demonstrated improved security through multi-layered authentication. However, the system was not tested under high-access-load conditions, leaving its stability in multiuser situations unverified.

Based on these studies, it can be concluded that the integration of RFID and IoT offers significant potential for enhancing security, efficiency, and flexibility in access control systems. However, most prior studies still encounter limitations related to real-time monitoring, power efficiency, implementation costs, and scalability within educational environments. These gaps form the basis of the present research, which aims to develop a low-cost RFID–IoT–based door lock system capable of real-time access monitoring and suitable for implementation in electrical engineering laboratories.

3. RESEARCH METHOD

This research uses the Research and Development (RnD) method, which is an approach that aims to assess, design, manufacture, and test the validity of the products developed [11].

This research was conducted through the stages of designing, building, and testing a prototype smart home system, the explanation of which can be seen in more detail in the following figure.

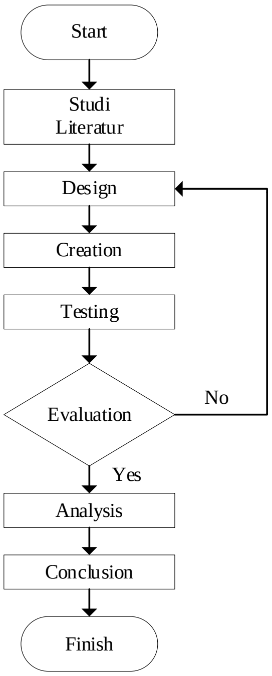


Figure 1. Research Flowchart

In Figure 1 shows an explanation of how this research begins by reviewing the literature to collect the relevant theoretical basis. Then the system design is carried out. After the design is complete, the tool is made and tested for function. The test results are evaluated, if not appropriate, improvements are made by returning to the design stage. If it is appropriate, the data is analyzed and conclusions are drawn to answer the research objectives, as for the components used in this study include, among others:

3.1 RFID Reciver RC522

RFID is a practical and suitable identification technology to be applied to automation systems. This is because RFID utilizes radio waves to identify an object. This technology has been widely utilized in various applications, such as room or occupancy security systems, toll road payment systems, and so on [12]. The RC522 RFID requires a minimum voltage of between 2.5 to 3.3 Volts to operate. This module is capable of detection at a distance of about 5 cm by using a contactless chip, namely the MFRC522 IC as a reader and data writer. Because it is contactless, communication with the system is done wirelessly at a frequency of 13.56 MHz with data transfer rates reaching 848 kbps [13]. RC522 RFID module can be seen in Figure 2.

To clarify the technical characteristics of the MFRC522 RFID module used in the system, the Table 1 shows its technical specifications. This information includes the working voltage, current consumption in active and standby conditions, as well as the operating frequency which is a reference in system design and performance testing.

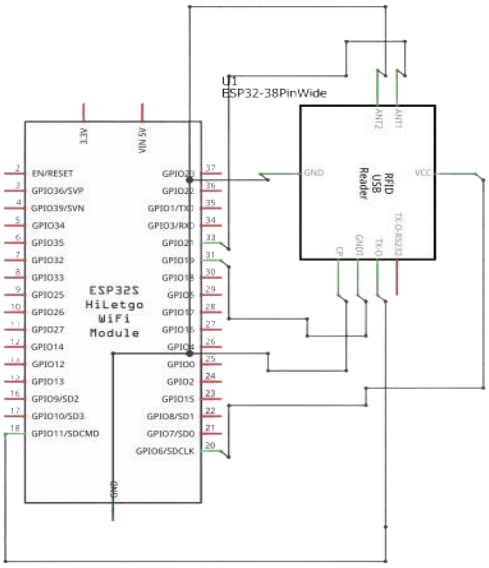


Figure 2. RC522 RFID Module

Table 1. Technical Specifications of MFRC522 RFID Chip

No	Parameters	Specifications
1	Operating Voltage	3.3V DC
2	Current Consumption (Active)	13-26 mA (when reading cards)
3	Current Consumption (Standby mode)	10 µA – 100 µA (power saving)
4	Frequency of Operation	13.56 MHz

As shown in Table 1, the power consumption of the MFRC522 chip is calculated based on the fundamental electrical principle $P = V \times I$, P=V×I. Under operating conditions, the chip functions at a voltage of 3.3 volts with an active-mode current requirement ranging from 13 mA to 26 mA. By substituting these values into the equation, the minimum power consumption occurs when the current is 13 mA, resulting in 3.3 V × 13 mA = 0.0429 W 3.3 V×13 mA=0.0429 W, or 42.9 mW. Conversely, the maximum power consumption is obtained when the current reaches 26 mA, producing 0.0858 W 0.0858 W, or 85.8 mW. Based on these calculations, it can be concluded that the MFRC522 has relatively low power requirements, with consumption ranging from 42.9 mW to 85.8 mW in active mode, thereby supporting energy efficiency in systems that implement this chip.

3.2 RFID Tag

For data storage needs, researchers use the Mifare Classic 1K, which is commonly applied to electronic wallet systems, transportation tickets, identity cards, and various similar systems. The Mifare Classic has a sector-based security structure, which is divided into 16 sectors, and works at a frequency of 13.56 MHz. This RFID tag has a data storage life of up to 10 years and supports re-writes up to 200,000 times. Figure 3 shows the physical form of a 1 kilobyte capacity Mifare Classic RFID tag card [14].

Figure 3. Tag MIFARE

3.3 Mikrokontroller ESP 32

ESP32 is a microcontroller developed by Espressif Systems, a technology company based in Shanghai, China [15]. One of the advantages of ESP32 is that it has been integrated with WiFi and Bluetooth features, making it easier to develop IoT systems that require wireless connectivity [16]. This module can also be utilized in various other applications, such as control systems, monitoring, and so on. The ESP32 is equipped with a deep sleep feature that enables energy savings by disabling the module when it is not operating [17]. ESP32 is a microcontroller that comes natively with Wi-Fi and Bluetooth modules, designed to deliver high performance in Radio Frequency (RF) communication while maintaining low power consumption efficiency [18].

Figure 4. Mikrokontroller ESP 32

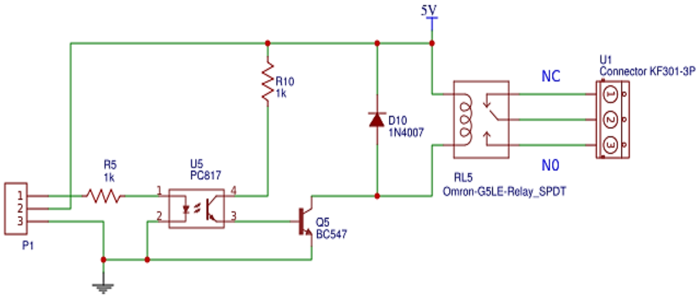
The ESP32 microcontroller in Figure 4 offers the advantages of low cost and power consumption. This device has been equipped with a WiFi module integrated directly on the chip, and supports dual-mode Bluetooth connections with energy-saving features, thus providing more flexibility in its use. In addition, the NodeMCU ESP32 module is a compact prototyping board that is easy to program using the Arduino IDE or Python programming language [19].

3.4 Relay

Relays are electronic components that are used as switches to control electrical circuits, especially when the required current or voltage exceeds the capabilities that can be handled directly by a microcontroller [20]. In electrical systems, relays are operated by utilizing a low-voltage electric current from a microcontroller or other control circuit to activate electromagnets inside the device. Figure 5 shows how a transistor works as an electronic switch to activate a relay. Voltage is applied to the base of the transistor through a current-limiting resistor to ensure that the incoming current remains within safe limits.

3.5 Solenoid Door Lock

Lock for door solenoid is a security system that operates electrically using a solenoid, which is an electromagnetic device that regulates the locking motion through an electric current [21]. When electrified, The solenoid generates a magnetic field that pushes the locking lever, which allows the door to be opened or locked. In Figure 6, the system supports two modes of operation, namely fail-safe, where the door will open when power is cut off, and fail-secure, where the door remains locked even without a power source. This technology offers efficiency and reliability in automatic access control systems.



Gambar 5. Wiring Diagram Relay

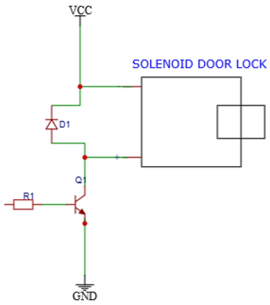


Figure 6. Solenoid Door Lock 12v

3.6 Internet of Things (IoT)

The modern technology known as the IoT aims to ensure that objects remain active and connected through internet connectivity [22]. Through this concept, various physical devices can communicate with each other, enabling more efficient automation processes in everyday life. The presence of IoT makes various human activities easier to carry out in an integrated and practical manner, thus providing an increase in convenience, efficiency, and productivity in various fields. In the future, the internet may surpass human computing capabilities, such as remotely controlling electronic devices. Every object has an IP address that allows it to be tracked [23].

According to Gartner, one of the technology trends that will have a major impact on the development of Information Technology in the next five years is the IoT. IoT itself is an approach that involves various devices, objects, applications, and services in the surrounding environment to create new solutions and achieve common goals. Each device in this network has an IP address as an identity that allows it to be recognized and monitored [24].

According to technical standardization, the IoT can be defined as a global-scale infrastructure designed to meet various needs of society and combine technological and social elements to solve various problems [25]. Various devices used in everyday life, such as transportation equipment, household appliances, and industrial machinery, can now be integrated with the internet, making the monitoring process more practical and can be done remotely. According to Betts [26]. After all components are available and successfully assembled, the next step is to analyze the RFID reading distance, whose process flow can be seen in the flowchart diagram below.

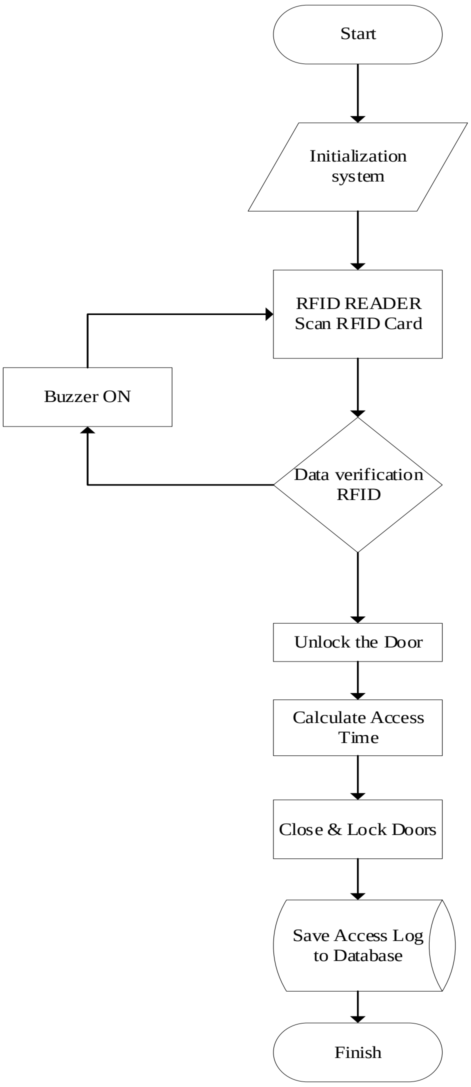


Figure 7. Flowchart of the Research Flow

Figure 7 describes the workflow of the RFID-based Smart Door Lock system, which begins with the system initialization process after the device is activated. Next, the RFID reader will scan the card that is affixed. If the card data does not match, the system will turn on the buzzer as a sign of denial of access. However, if the data is valid, the door will open automatically and the system starts calculating the user access duration. After the access time is up, the door will be locked again, and all access data will be stored into the database for recording and monitoring purposes. The process is then terminated once all steps are completed.

4. RESULTS AND ANALYSIS

The results of the implementation and testing of the Smart Door Lock system based on the IoT with the RC522 RFID module used in the Electrical Engineering Laboratory are presented in this section. The testing process aims to assess the performance of the system from various aspects, such as RFID reading distance, user identity validation, power consumption of each component, and monitoring capabilities via IoT connection. All data is organized in the form of a table and followed by a systematic explanation to facilitate the reader's understanding of the performance of the system that has been designed.

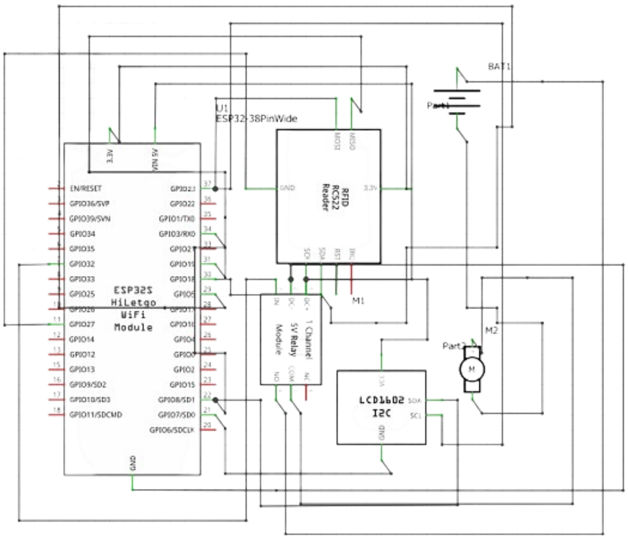


Figure 8. Wiring Diagram of Smart Door Lock System with RC522 RFID Module

To support the process of analyzing the results of the system implementation, Figure 8 shows a circuit schematic that illustrates the configuration and connection between electronic components in the IoT-based Smart Door Lock system. This system uses the RC522 RFID module as a user authentication tool, with the ESP32 microcontroller as the control center as well as a link to the internet network for remote monitoring purposes. The system status display, such as the success or failure of RFID card verification, is shown through the LCD in real-time. Meanwhile, the relay module serves to regulate the flow of current from the 12V battery to the door lock solenoid, which will lock or open the door according to the authentication results. This circuit is designed to be ideally used on laboratory doors or confined spaces that require an automated security system.

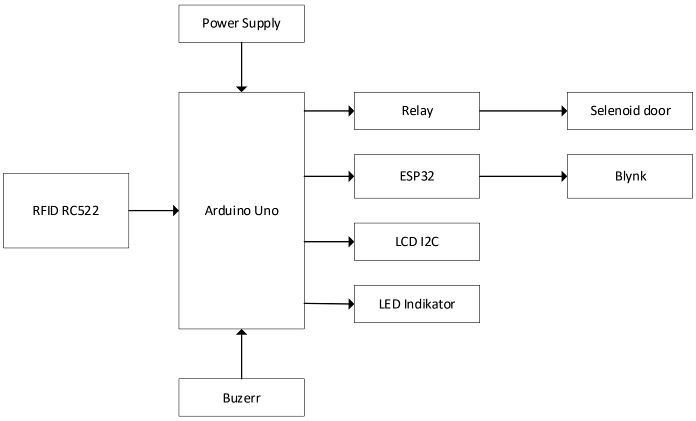


Figure 9. Block Diagram of Smart Door Lock System Using RFID

Figure 9 shows the block diagram of the Smart Door Lock system, which is operated by an ESP32 microcontroller and based on the IoT. This system obtains power from the power supply, which then distributes energy to all components. The RC522 RFID module functions to read data from the RFID card as a form of user authentication. Once the data is received, the ESP32 processes the information and, if verified, activates the relay module, which will serve to control the solenoid lock, which will allow the door to be opened.The authentication and operational status of the system is displayed via an I2C LCD, while indicator LEDs provide visual information, and a buzzer sounds as a warning in case of unauthorized access. In addition, the system is also integrated with the Blynk application to enable remote monitoring and control via the internet network.

4.1. RFID Reading Distance Testing

This test aims to evaluate the extent of the RC522 RFID module's ability to detect RFID cards accurately. The test results show that the maximum distance that can be used to read the card is 5 cm. At that distance or less, the system is able to read cards quickly and accurately. Conversely, if the distance exceeds 5 cm, the reading process tends to fail. This finding is in line with the technical specifications of the RC522 RFID module.

Table 2. RFID Reading Distance Test Results

No	Card to Reader Distance (cm)	Reading Status	Description
1	1	Successful	Very fast reading
2	2	Successful	High Accuracy
3	3	Successful	Slightly slowed response
4	4	Successful	Still within optimal range
5	5	Successful	Maximum limit of stable readings
6	6	Failed	Out of effective range

In Table 2, tests were conducted to determine the maximum distance that is still possible for the RFID-RC522 to read cards or tags accurately. The test results show that the module is able to optimally detect cards at a distance range of 1 to 4 cm with a fast and accurate response. However, when the tag was brought closer at a distance of 6 cm, the reading process was unsuccessful, indicating that the maximum effective distance of the RFID RC522 is 5 cm. This finding is in line with the technical specifications of the module, which is designed for operation at short distances.

4.2. Valid and Invalid Card Testing

The purpose of this test is to evaluate the system's ability to identify and distinguish between valid and invalid RFID cards. The test results show that when a valid card is used, the system recognizes it and automatically activates the actuator to open the door. Conversely, if an unregistered card is used, the system will deny access and activate the buzzer as a warning sign. The resulting response shows that the system works according to the previously designed program logic.

Table 3. Valid and Invalid Card Testing Results

No	Card ID	Card Status	System Response	Description
1	12345678	Valid	Open Door	Access Received
2	87654321	Invalid	Buzzer On	Access Denied
3	13579246	Valid	Open Door	Access Received
4	11223344	Invalid	Buzzer On	Card Not Accepted

In Table 3. Presents test results related to RFID cards that have been registered (valid) and those that have not been registered (invalid) in the system. When a valid card is used, the system will automatically open the door. Conversely, if an unregistered card is used, access will be denied and a buzzer will sound as a sign of rejection. This test proves that the system is able to accurately distinguish between users who have access rights and those who do not, and provide appropriate responses to each condition.

4.3. System Power Consumption Evaluation

Evaluation of power consumption is done to find out how much energy each main component in the system requires. Based on the calculation using the formula $P = V \times I$, it is known that the component with the highest power consumption is the door lock solenoid when it is in door opening condition, which reaches 7.2 Watts. On the other hand, the RFID module and ESP32 microcontroller show lower and more efficient power usage, both when in standby mode and when reading data.

Table 4. System Power Consumption Evaluation

No	Component	Voltage (V)	Current (mA)	Power (Watt)	Operation Status
1	RFID RC522	3.3 V	13 – 26 mA	0.0429 – 0.0858 W	When reading cards
2	ESP32	3.3 V	40 – 240 mA	0.132 – 0.792 W	Until WiFi is active
3	Solenoid Door Lock	12 V	400 – 600 mA	4.8 – 7.2 W	When unlocking
4	Buzzer	3.3 V	10 – 20 mA	0.033 – 0.066 W	When access is denied

The power evaluation results in Table 4. Shows that the energy consumption of each component varies according to its operational condition. The RC522 RFID module consumes quite low power when active, which is between 0.0429 to 0.0858 Watts. The ESP32 microcontroller has more diverse power consumption, depending on its activity, ranging from idle conditions to when using a Wi-Fi connection. Meanwhile, the door lock solenoid is the component with the highest power consumption, reaching 7.2 Watts when driving the door opening mechanism. From these findings, it can be concluded that the system has good energy efficiency, especially when it is in standby.

4.4. Access Monitoring Through IoT

The system is supported by an IoT-based access monitoring feature, which allows every access activity to be recorded and sent to the server in real-time. The data sent includes the time of the event, RFID card ID, card validity status, as well as the system's response to the access. Through this capability, laboratory managers can remotely monitor access usage, increase security levels, and ensure that all access history is neatly and accurately documented.

Table 5. Access Monitoring Through IoT

No	Access Time	Card ID	Card Status	System Action	Status Sent to Server
1	08-05-2025 08:15	12345678	Valid	Open Door	Sent
2	08-05-2025 08:20	11223344	Invalid	Access Denied	Sent
3	08-05-2025 09:01	13579246	Valid	Open Door	Sent
4	08-05-2025 09:30	00001111	Invalid	Access Denied	Sent

In the IoT-based access monitoring section, Table 5 displays user activity data that is recorded directly and sent to the server in real-time. Every time the system is accessed, information such as access time, card ID, card status, and system actions will be automatically recorded and sent. With this feature, laboratory managers can remotely monitor and obtain access history with accurate details. This capability provides significant support for a more effective and transparent security monitoring system.

5. DISCUSSION

The test results indicate that the RFID RC522 and IoT-based access control system developed in this study operates stably with consistent performance across all testing stages. The RFID module is capable of reading cards within a range of 1 to 5 cm, achieving the highest success rate at a distance of 1–4 cm. These findings are consistent with previous work using an RFID- and Arduino-based smart door lock prototype, which also reported that RFID tag detection is most effective at short distances and highly dependent on module sensitivity and card orientation relative to the antenna[27]. Thus, the RFID reading performance observed in this study falls within the typical operational range for HF RFID devices.

The system also demonstrates reliable capability in distinguishing between registered and unregistered cards. Both solenoid activation and alarm triggering occur immediately after the microcontroller processes the card data. This outcome supports previous findings showing that authentication using unique RFID card identifiers provides rapid validation in IoT-based access control systems[28]. A key distinction of the present study is the integration of real-time monitoring through an IoT platform, allowing administrators to observe access activities directly.

Power consumption evaluation indicates that the solenoid door lock is the most energy-demanding component, whereas the ESP32 and RFID module operate more efficiently, particularly in standby mode. This pattern is consistent with results reported for a smart door prototype combining RFID, a keypad, and motion sensors, where door actuators were identified as the primary source of energy consumption, while sensors consumed minimal power when idle[29]. These findings emphasize that actuator efficiency is a critical factor in optimizing the overall performance of automated access control systems. Compared to conventional IoT-based smart home designs, the proposed system provides additional capabilities, including comprehensive access activity logging and multiuser support, making it more suitable for educational laboratory environments[30]. The ability to document access activities represents a significant advantage in managing spaces that are utilized by multiple users.

The findings suggest that integrating RFID and IoT technology significantly enhances the security, manageability, and operational efficiency of access control systems. Owing to its straightforward architecture and relatively low implementation cost, the proposed system is well-suited for deployment in laboratory environments that require strict, reliable, and well-documented access supervision.

6. CONCLUSION

This research successfully developed an RFID RC522 and IoT-based automatic door security system in the Electrical Engineering Laboratory, capable of reading cards from a distance of up to 5 cm with high accuracy and distinguishing between authorized and unauthorized access. The solenoid door lock was the component with the highest power consumption, while the ESP32 and RFID module worked efficiently. IoT integration enabled real-time access monitoring, improving security and operational efficiency. Compared to previous research, this system excels due to its low cost, energy efficiency, and support for practical remote monitoring in educational laboratories. Overall, this system achieves the research objectives of providing secure, efficient, and internet-connected access control, with potential for further development through cloud-based access management and data security.

ACKNOWLEDGEMENTS

The authors would like to thank everyone who helped and supported the completion of this research, both with facilities, technical guidance, and inspiration. Thanks also go to colleagues at the Electrical Engineering Laboratory who have helped in the testing and data collection process. All forms of assistance are very meaningful in realizing the implementation of this RFID and IoT-based automatic door security system.

REFERENCES

[1] R. Wulandari, “The Impact Of Technological Developments In Education,” vol. 09, 2023, [Online]. Available: https://journal.upy.ac.id/index.php/JPI/index (in Indonesian)

[2] Robby Kurniawan Harahap, Alief Vickry Thaha Maulidzart, Antonius Irianto Sukowati, Dyah Nur’ainingsih, Widyastuti, and Desy Kristyawati, “Securing RFID in IoT Networks With Lightweight AES and ECDH Cryptography Approach,” Jurnal Nasional Teknik Elektro dan Teknologi Informasi, vol. 13, no. 3, pp. 186–194, Aug. 2024, doi: 10.22146/jnteti.v13i3.11824.

[3] S. A. Siregar, P. M. Simanullang, M. Hamni, S. Rezeki, M. Aqil, and F. Jeriko, “Utilization of Radio Frequency Identification (RFID) in the Student Multi-Access System,” Online, 2023.(in Indonesian)

[4] Z. Musliyana, A. Rivaldo Koto, D. R. Yusian, and D. Payana, “Implementation Of Internet Of Things (Iot) In Android-Based Control Of Household Electrical Devices,” Journal of Informatics and Computer Science, vol. 9, no. 2, 2023.(in Indonesian)

[5] H. Maulana, P. Pendidikan Teknik Elektro, F. Tarbiyah dan Keguruan Universitas Islam Negeri Ar-Raniry Banda Aceh Aceh Jln Syeikh Abdul Rauf Darussalam Banda Aceh, and B. Aceh, “Design Of Rfid And Keypad-Based Smart Door Lock,” Jurnal Pendidikan Teknologi informasi, vol. 8, no. 2, pp. 80–88, 2024.(in Indonesian)

[6] S. Aisyah, Y. Ali, K. Saharja, and A. Sani, “Smart Door Lock System Development Prototype Using Rfid Technology ID-12,” Jurnal Riset Informatika, vol. 4, no. 4, pp. 379–384, Sep. 2022, doi: 10.34288/jri.v4i4.118.

[7] K. Diantoro and F. Rohmatullahama, “Designing a Limited Access Security System with RFID Technology at PJB Muara Tawar” remik, vol. 7, no. 1, pp. 388–398, Jan. 2023, doi: 10.33395/remik.v7i1.11932. (in Indonesian)

[8] R. Bangun Sistem Keamanan Pintu Menggunakan Modul RFID Berbasis IoT and N. Amalia, “Designing a Door Security System Using IoT-Based RFID Modules,” vol. 1, no. 2, [Online]. Available: https://jurnal.komputasi.org/index.php/jst/article/view/20/ (in Indonesian)

[9] A. Fakhruddin, D. Irawan, A. Soffiana, and J. Teknik, “Designing An Internet Of Things-Based Home Door Security System With Esp32 And The Blynk Application,” vol. 19, pp. 53–59, 2024.(in Indonesian)

[10] A. Koriah, P. Teknik Informatika, S. N. Syaikh Zainuddin Anjani Jalan Raya Mataram, and L. Timur, “Design A Home Door Security System With Voice Recognition And Iot-Based Rfid Bracelets.” (in Indonesian)

[11] Ade Rahayu, “Research and Development (R&D) Methods : Pengertian, Jenis dan Tahapan,” DIAJAR: Jurnal Pendidikan dan Pembelajaran, vol. 4, no. 3, pp. 459–470, Jul. 2025, doi: 10.54259/diajar.v4i3.5092. (in Indonesian)

[12] H. N. Ahmad and T. Ardiyansyah, “Utilization Of Rfid (Radio Frequency Identification) For The Security Of Microcontroller-Based ATMEGA328 Cabinet Doors,” 2012. (in Indonesian)

[13] I. Muzaki, I. Amal, and M. Alfarisi, “Smart Lock Door Using Rfid Rc522 Based On Arduino Nano Microcontroller.” [Online]. Available: http://ejournal3.undip.ac.id/index.php/transient

[14] D. Nataliana, F. Hadiatna, and A. Fauzi, “Designing an RFID Tag Security System using the Caesar Cipher Method in Electronic Payment Systems,” ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, vol. 7, no. 3, p. 427, Sep. 2019, doi: 10.26760/elkomika.v7i3.427.

[15] H. Kusumah and R. A. Pradana, “Application Of Esp32-Based Microcontroller And Internet Of Things Trainer Interfacing In Interfacing Courses”.

[16] A. Sanaris and I. Suharjo, “Prototype of an Automatic Clothes Dryer Control Device Using NodeMCU ESP32 and Telegram Bot Based on the Internet of Things (IoT) Prototype of an Automatic Clothes Dryer Control Device Using NodeMCU ESP32 and Telegram Bot Based on the Internet of Things (IoT),” Gejayan.(in Indonesian)

[17] E. Julianto Prihantoro et al., “Perancangan Smart Klinik Berbasis Mikrokontroler Nodemcu ESP32,” JEECOM, vol. 3, no. 2, 2021.

[18] M. Rizal, P. Negeri, U. Pandang, M. S. Hadis, R. Angriawan, and A. Arifin, “Evaluasi Kinerja Bluetooth Pada Modul Esp32 Di Lingkungan Line Of Sight; Journal of Embedded Systems Security and Intelligent Systems ·

April 2020 CITATIONS 4 READS 74 4 authors, including: Evaluasi Kinerja Bluetooth Pada Modul Esp32 Di Lingkungan Line Of Sight." [Online]. Available: https://ojs.unm.ac.id/JESSI/index

[19] D. Wara and B. Suprianto, "Pengembangan Trainer Internet Of Things Berbasis Mikrokontroler Esp32 Pada Mata Pelajaran Pemrograman, Mikroprosesor Dan Mikrokontroler Di Smk Negeri 2 Surabaya."

[20] G. Nazhrullah and Aria Kharisma, "Relay Proteksi Arus Lebih Berbasis Mikrokontroller Arduino," PoliGrid, vol. 4, no. 1, Nov. 2023, doi: 10.46964/poligrid.v4i1.9.

[21] A. Z. Hasibuan and S. Asih, "Pemanfaatan Internet Of Thing Untuk Pengendalian Solenoid Doorlock Dalam Sistem Keamanan Rumah Cerdas," 2023. [Online]. Available: www.ellislab.com

[22] Ayu Syahfitri, "Internet of Things (IoT), Sejarah, Teknologi, dan Penerapannya," Uranus : Jurnal Ilmiah Teknik Elektro, Sains dan Informatika, vol. 3, no. 1, pp. 113–120, Jan. 2025, doi: 10.61132/uranus.v3i1.667.

[23] B. Yanto, B. Basorudin, S. Anwar, A. Lubis, and K. Karmi, "Smart Home Monitoring Pintu Rumah Dengan Identifikasi Wajah Menerapkan Camera ESP32 Berbasis IoT," Jurnal Sisfokom (Sistem Informasi dan Komputer), vol. 11, no. 1, pp. 53–59, Mar. 2022, doi: 10.32736/sisfokom.v11i1.1180.

[24] S. Arafat, M. Kom, and Kom, "Internet of Things (IoT)-Based Home Door Security System with ESP8266," Oktober-Desember, 2016.

[25] D. Adidrana, H. Suryoprayogo, and A. Rahman Hakim, "Perancangan Sistem Smart Door Lock Menggunakan Internet of Things (Studi Kasus: Institut Teknologi Telkom Jakarta)," DES 2022 Journal of Informatics and Communications Technology, vol. 4, no. 2, pp. 102–108, doi: 10.52661.

[26] R. I. Pratama, F. Ardianto, B. Alfaresi, A. Sofijan, and E. Ariyanto, "Implementasi internet of things (iot) web server smarthome," Jurnal Digital Teknologi Informasi, vol. 5, no. 2, p. 59, Sep. 2022, doi: 10.32502/digital.v5i2.4370.

[27] Thariq Arifun Nathiq, "Rancang Bangun Smart Doorlock Kamar Mesin dan Anjungan Berbasis RFID dan Arduino," Venus: Jurnal Publikasi Rumpun Ilmu Teknik , vol. 2, no. 4, pp. 14–40, Jun. 2024, doi: 10.61132/venus.v2i4.376.

[28] D. Andriyan, R. Andri Yusda, and M. Dwi Sena, "JUTSI: Jurnal Teknologi dan Sistem Informasi Rancang Bangun Smart Door Lock Berbasis IoT Untuk Smart Office," vol. 4, no. 1, 2024, doi: 10.33330/jutsi.v4i1.3004.

[29] M. Rizal Fachri, P. Studi Pendidikan Teknik Elektro, and U. Islam Negeri Ar-Raniry Banda Aceh, "Analisis Prototype Smart Door Lock Berbasis RFID, Keypad dan Sensor Gerak," vol. X, no. 1, 2025.

[30] A. N. M. Andreas and R. Arijanto, "Rancang Bangun Smart Home IoT dengan Integrasi Kunci Rfid dan Otomasi Elektronik," bit-Tech, vol. 7, no. 2, pp. 235–243, Dec. 2024, doi: 10.32877/bt.v7i2.1729.

BIBLIOGRAPHY OF AUTHORS

Yudi Wijanarko, S.T., M.T., is a permanent lecturer in the Electrical Engineering Department of Politeknik Negeri Sriwijaya (POLSRI) Palembang in the Applied Sciences Group in the Electronics Engineering Study Program which focuses on the field of Electrical Engineering or Engineering which has expertise in the fields of Electronic Devices, Analog Systems, Design Projects and Renewable Energy. He has served as Head of D3 Electronic Engineering Study Program (2012-2016); and Head of Electrical Engineering Department (2016-2020).

Niksen Alfarizal, S.T., M.Kom., is a permanent lecturer in the D3 Electronic Engineering Study Program, Department of Electrical Engineering, Politeknik Negeri Sriwijaya who currently serves as the Head of the Study Program and is active in teaching and research, especially in the development of microcontroller-based systems, Internet of Things (IoT), instrumentation, and control systems. He has produced various scientific works published in national and international journals.

Muhammad Regi Pratama, is an active 8th semester student in the Bachelor of Applied Electrical Engineering Study Program, Department of Electrical Engineering, Politeknik Negeri Sriwijaya. During the study period, he was active in academic activities and research projects related to the development of microcontroller-based systems, the Internet of Things (IoT), and technology applications for security and automation systems.