ISSN: 2963-2536 (media online)

Proceedings of Malikussaleh International Conference on Multidisciplinary Studies (MICoMS)

Organized by center of Excellence of Technology Natural Polymer and Recycle Plastics

International Conference Proceedings 00023 (2024) DOI: https://doi.org/10.29103/micoms.v4.2024

Development and Implementation of an ESP32 Microcontroller and Monitoring System for Smart Door Lock Using RFID Sensor for E-KTP ID and Fingerprint Based on the Internet of Things

Attariq Ziad [1]*, Eva Darnila [2], Kurniawati [3]

[1] Department of Informatics, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, Attariq.200170193@mhs.unimal.ac.id
[2] Department of Informatics, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, eva.darnila@unimal.ac.id
[3] Department of Informatics, Universitas Malikussaleh, Bukit Indah, Lhokseumawe, 24353, Indonesia, kurniawati@unimal.ac.id
* Correspondence: attariq.200170193@mhs.unimal.ac.id

Abstract: This study aims to improve the effectiveness and efficiency of door security systems by integrating RFID technology, fingerprint recognition, and the Internet of Things (IoT). This system not only enables automatic locking but also provides real-time access control and monitoring through a web-based application. The technology supports high-level security through dual authentication methods, using E-ID cards and fingerprint sensors. Additionally, the implementation of IoT allows users to monitor and manage door access remotely, offering added flexibility and convenience. The system's trial shows high reliability in reading RFID and fingerprint data, with significant accuracy in various conditions. The results of this study contribute to the development of modern security solutions that can be applied in various environments, such as residential homes, offices, and public facilities, with the potential to reduce overall crime rates.

Keywords: Smart door lock, E-KTP, Fingerprint, ESP32, Monitoring system.

1. Introduction

Security is a fundamental necessity in the modern digital era, essential for individuals, groups, and communities. Doors, as the primary access points to rooms and buildings, serve not only as physical barriers but also as the first line of defense to safeguard valuable belongings and personal data. However, traditional manual locking systems are often inadequate in meeting contemporary security demands. Risks such as key loss, unauthorized duplication, and mechanical damage highlight the fundamental weaknesses of conventional locks, underscoring the need for more advanced and effective security solutions.

The rising crime rates further emphasize the urgency of implementing sophisticated security systems. For example, in Lhokseumawe, criminal cases significantly increased from 665 in 2021 to 778 in 2022, with theft being one of the most prevalent crimes [1]. These statistics demonstrate that traditional security systems are no longer sufficient to prevent increasingly complex threats, making it imperative to develop innovative, technology-based solutions to enhance safety and efficiency.

An effective approach to address these challenges is the implementation of smart door lock systems based on advanced technologies. These systems replace conventional manual locks with automated mechanisms utilizing Radio Frequency Identification (RFID) and biometric fingerprint authentication. In this study, E-KTP, Indonesia's official electronic identification card, is selected as the primary authentication medium due to its high-security features, such as unique biometric data stored within a secure chip [2], [3]. This technology not only enhances security but also simplifies access for users. For instance, smart locks eliminate the need to carry multiple keys and reduce the risks of key loss or duplication, offering a more practical alternative to traditional locking systems [4],[5].

The integration of Internet of Things (IoT) further extends the functionality of smart door locks. IoT allows devices to communicate and connect in real-time through the internet, enabling users to monitor and control door access remotely via web-based applications [6], [7]. This feature provides not only enhanced physical security but also greater transparency and control over access management.

This research aims to design and develop a smart door lock system based on the ESP32 microcontroller, utilizing RFID to read E-KTP data and fingerprint authentication to grant access. The system is also equipped with an IoT-based monitoring application that records door access activities in real-time. By combining security, efficiency, and convenience, this system is expected to improve residential safety in Lhokseumawe, reduce crime rates, and enhance user experience.

By integrating three core technologies, RFID, fingerprint authentication, and IoT. This study offers a more comprehensive approach compared to traditional security systems. In addition to providing stronger protection against theft and other threats, the system is designed to be flexible and applicable in various environments, such as households, offices, and public facilities. Through this approach, the research aims to contribute meaningfully to the development of innovative, effective, and relevant security solutions for modern society.

2. Materials and Methods

2.1. E-KTP

E-KTP is Indonesia's official electronic identity card equipped with a chip that stores biometric data, such as fingerprints and digital photographs [8], [9]. This biometric data makes E-KTP a secure and hard-to-forge authentication tool, and it is also compatible with advanced technological systems. The reason for utilizing E-KTP in this study as key access for door locking systems lies in its several advantages. First, it enhances security due to the unique biometric information it contains, such as fingerprints. Second, it serves as an official identity card widely held by many individuals. Users do not need to carry physical keys or additional devices, as the E-KTP itself suffices. In this research, E-KTP is used as the primary authentication medium in a smart lock system, integrated with RFID and fingerprint recognition to create a comprehensive security solution.

2.2. Fingerprint

Fingerprint recognition is a biometric technology that uses the unique patterns of ridges and valleys on a person's fingertip to authenticate identity [10], [11]. These patterns are unique to each individual and remain consistent throughout life, even in the case of identical twins [12]. This makes fingerprint recognition one of the most reliable authentication methods, as the patterns are difficult to forge or duplicate.

In this study, the AS608 fingerprint sensor is used, offering several key features:

- High Resolution: With a resolution of 500 dpi, the sensor ensures precise and accurate fingerprint readings.
- Fast Authentication: The process takes less than one second, making it efficient for real-time applications.
- User Convenience: Users can simply place their finger on the sensor to unlock the door, eliminating the need for physical keys or remembering access codes.
- Fingerprint recognition enhances the security of the door lock system by providing an additional layer of authentication, ensuring that only registered users can access the door.

2.3. Sensors

2.3.1. RFID (Radio Frequency Identification)

RFID is a wireless technology used to identify and authenticate objects by transmitting data through electromagnetic waves [13], [14]. The system consists of two main components: the RFID tag, which stores unique data, and the RFID reader, which retrieves this data without requiring direct contact.

In this study, RFID technology is integrated to read data from E-KTP cards. Its functionality includes:

- High-Speed Authentication: RFID enables quick data reading, reducing delays in access control.
- Contactless Operation: The technology eliminates the need for physical interaction, enhancing durability and ease of use.
- IoT Integration Capability: RFID data is transmitted in real-time to a web-based monitoring platform, providing users with remote access and control over the system.

This integration ensures secure and efficient authentication while allowing seamless communication with IoT-enabled platforms.

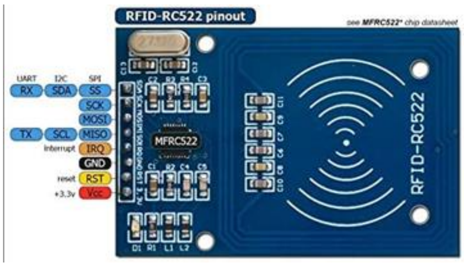


Figure 1. RFID sensor

2.3.2. Fingerprint Sensors

Fingerprint sensors are electronic devices that capture unique fingerprint patterns and convert them into digital data. The AS608 fingerprint sensor, used in this study, is notable for its high-speed processing and accuracy [15]. The sensor matches the scanned fingerprint with a pre-stored template in the system's database to ensure secure authentication. By combining RFID and fingerprint sensors, the system provides multi-layered security, ensuring that unauthorized users cannot gain access even if one layer of security is breached.

Figure 2. Fingerprint sensor

2.4. IoT (Internet of Things)

The Internet of Things (IoT) is a technological framework that connects devices, enabling them to communicate and exchange data over the internet [16], [17]. By automating processes and providing remote control capabilities, IoT enhances operational efficiency, user convenience, and system security. In the context of door-lock systems, IoT facilitates real-time monitoring, remote management, and automated access control. This technology addresses the limitations of conventional locks, such as vulnerability to human error and physical manipulation, by introducing advanced mechanisms that optimize security and functionality.

2.4.1. Previous Research

IoT has been widely explored by researchers for its potential to revolutionize access control systems. Nurwijayanti and Basyir developed an RFID and IoT-integrated automated door-lock system designed to address the inefficiencies of traditional locks. Their system successfully automated door operations, provided access reports, and significantly improved both security and operational efficiency [18]. Similarly, Najib et al. implemented an IoT-based system using E-KTP and RFID technology. The system demonstrated robust performance, achieving an optimal reading distance of 4 cm and meeting the "perfect" TIPHON standards for throughput and delay, making it an effective solution for IoT-based home security [19].

Yulisman et al. further enhanced IoT applications by designing an automatic door-lock system using E-KTP integrated with a web-based platform. This system simplified access control, allowed real-time monitoring, and achieved a success rate of 88.7%, demonstrating its reliability and user-friendliness [20]. Alvayen and Karnadi extended IoT functionality by integrating it with RFID and the Blynk application, enabling users to remotely monitor and control doors. Their system also provided real-time notifications, ensuring efficient management of access activities [21].

In educational and professional environments, Wiranata et al. developed an IoT-enabled RFID door-lock system that utilized Telegram for remote operation. This innovation allowed real-time monitoring of faculty presence and secure access control via internet-based commands. The versatility of IoT demonstrated in this study highlights its applicability in diverse use cases, from academic institutions to residential and commercial settings [22].

The findings from these studies underscore the transformative impact of IoT in door-lock systems. IoT enables real-time communication, centralized data management, and remote accessibility, offering significant improvements over traditional locking mechanisms. Building on these advancements, the present study integrates IoT with RFID and fingerprint sensors using the NodeMCU ESP32 microcontroller and Laravel-based web monitoring. This approach aims to deliver a comprehensive, secure, and user-friendly smart door-lock system tailored for modern security demands.

2.5. System Schematic

Below is a schematic description of the smart door lock monitoring system using RFID sensors for e-KTP id and fingerprint.

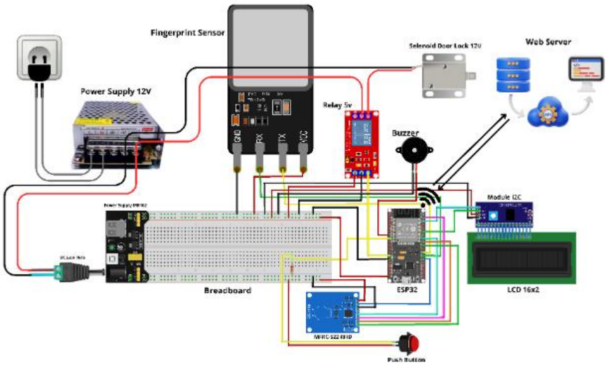


Figure 3. System Schematic

This Internet of Things (IoT) system is a smart door lock that uses fingerprint and RFID sensors for authentication. A 12V power supply powers the main components, including relays and the solenoid door lock. The fingerprint sensor and RFID (E-KTP ID/RFID card) send data to the ESP32, which controls the 5V relay to open or close the door when access is permitted. A buzzer as an audible indicator provides access notification.

The ESP32 controls the system, including the 16x2 LCD via the I2C module to display the authentication status. Push buttons allow opening the door from inside the room. Through Wi-Fi connection, the ESP32 connects to a web server for real-time remote monitoring and control. With dual authentication, voice notification, push button, and web access, the system offers flexible and practical security.

2.6. Fingerprint Identifications

The fingerprint identification process involves two primary phases: the learning phase and the identification phase. During the learning phase, the system captures and processes fingerprint data to build a reference database. The process begins with segmentation, where the fingerprint's relevant area is isolated, eliminating unnecessary background details. Unique features are then extracted using the Local Binary Pattern (LBP) method, which analyzes texture patterns within the fingerprint image. These extracted features are associated with user profiles and stored in the system's database as templates for future identification.

In the identification phase, the system verifies newly scanned fingerprints by comparing them to the stored templates in the database. Similar to the learning phase, the fingerprint undergoes segmentation and feature extraction to isolate and analyze its unique characteristics. The extracted features are then matched against the stored templates using a comparison algorithm to determine the best match. If a match is found, access is granted; otherwise, it is denied, and the failed attempt is logged. This two-phase process ensures high accuracy and reliability, making the system well-suited for secure and efficient access control in IoT applications (Fanggidae et al., 2019).

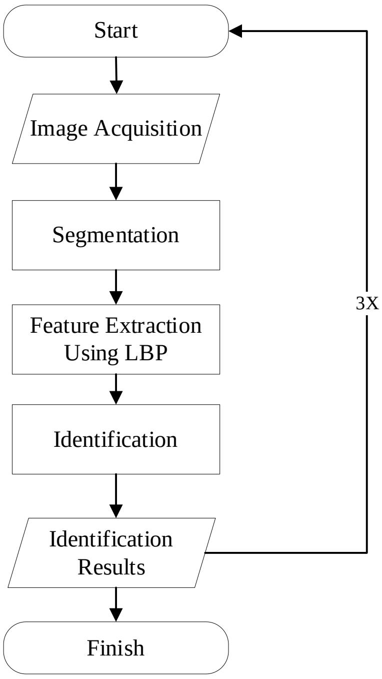


Figure 4. Fingerprint Identifications

3. Results and Discussion

3.1. Objectives

The objectives of this research design are as follows:

- To develop a door security system utilizing E-KTP cards and fingerprint authentication as door access controls.
- To monitor and manage the smart door lock system through E-KTP-based controls.

3.2. Benefits

The benefits of this research design are as follows:

- For researchers: This study serves as an opportunity to enhance skills relevant to the professional field and expand knowledge in developing Internet of Things (IoT) projects.
- For users: The results of this study aim to provide enhanced security against criminal activities, particularly theft and unauthorized entry through doors.

3.3. Results

3.3.1. System Implementation Results

The RFID and fingerprint-based smart door lock system can be implemented in residential settings by integrating various hardware and software components. This system uses the ESP32 as the main microcontroller, which is connected to an RFID reader (RC522), a 16x2 LCD display to show the status, a relay to control the solenoid lock, and a buzzer and manual button as backups. The backend of the system is connected to a PostgreSQL database via Prisma, allowing automatic and real-time access logging. Node.js (Express.js) functions as the server to manage access logic and user verification based on registered identities. Only authorized users can unlock the door, with access being restricted to prevent misuse.

3.3.2. Device Testing

Sensor Testing as a Crucial Step in Developing a Smart Door Lock Prototype Using RFID and Fingerprint Sensors:

3.3.3. RFID

The RFID sensor will be evaluated for its accuracy in reading E-KTP cards. If the card read by the RFID sensor is already registered, the solenoid will unlock the door. During the RFID testing, experiments were conducted using 3 valid cards and 2 invalid and unregistered cards.

Table 1. RFID Testing

Card ID (E-KTP)	User Status	Test Results	Solenoid Response
1234567890123456	Registered	Valid Card, Registered in the System	Unlocking (Solenoid Active)
3201012201900001	Registered	Valid Card, Registered in the System	Unlocking (Solenoid Active)
3505056708001234	Registered	Valid Card, Registered in the System	Unlocking (Solenoid Active)
3172011511960003	Not Registered	Valid Card, But Not Registered in the System	Door Remains Locked (Solenoid Inactive)
3604024507990002	Not Registered	Valid Card, But Not Registered in the System	Door Remains Locked (Solenoid Inactive)

In the RFID sensor testing and solenoid response, it was concluded that the solenoid will unlock if the card read by the sensor is valid and registered. If the card read by the sensor is invalid or not registered, the solenoid will remain locked. In this test, the RFID sensor was able to read the card from a distance of 1-2 cm from the sensor.

3.3.4. Fingerprint Sensor

In the fingerprint sensor testing, the accuracy of the fingerprint reading is evaluated. If the fingerprint read by the sensor is registered in the system, the solenoid will unlock the door. In this test, 3 valid fingerprints and 2 invalid and unregistered fingerprints were used. The system is expected to unlock the door when it detects the valid, registered fingerprints and remain locked when it detects the invalid or unregistered fingerprints.

Table 2. Fingerprint Sensor Testing

Fingerprint ID	**Status Pengguna**	**User Status**	Solenoid Response
001	Registered	Valid Fingerprint, Registered in the System	Unlocking (Solenoid Active)
002	Registered	Valid Fingerprint, Registered in the System	Unlocking (Solenoid Active)
003	Registered	Valid Fingerprint, Registered in the System	Unlocking (Solenoid Active)
004	Not Registered	Valid Fingerprint, But Not Registered in the System	Door Remains Locked (Solenoid Inactive)
005	Not Registered	Valid Fingerprint, But Not Registered in the System	Door Remains Locked (Solenoid Inactive)

In the fingerprint sensor testing, the accuracy of the fingerprint reading is evaluated. If the fingerprint read by the sensor is registered in the system, the solenoid will unlock the door. In this test, 3 valid fingerprints and 2 invalid and unregistered fingerprints were used. The system is expected to unlock the door when it detects the valid, registered fingerprints and remain locked when it detects the invalid or unregistered fingerprints.

3.4. System Development

The developed prototype involves several components such as a 12V power supply to provide electricity, NodeMCU as the microcontroller, an RFID RC522 sensor to read ID cards, a fingerprint sensor to read fingerprints, a push button to open the door from inside the room, a solenoid to lock and unlock the door, a buzzer that sounds when the E-KTP card and fingerprint are placed near the sensor, and a 16x2 LCD to display information related to the system. All these components will be integrated and controlled via an internet connection, allowing remote control and monitoring through a website as well as real-time notifications via a Telegram bot. Here is the assembly of the components:

1. NodeMCU – RFID
   Pin D3 on NodeMCU connects to the RST pin on the RFID modul.
   Pin D4 on NodeMCU connects to the SDA pin on the RFID module
   Pin D5 on NodeMCU connects to the SCK pin on the RFID module
   Pin D6 on NodeMCU connects to the MISO pin on the RFID module
   Pin D7 on NodeMCU connects to the MOSI pin on the RFID module
   Pin GND on NodeMCU connects to the GND pin on the RFID module
   Pin 3V on NodeMCU connects to the 3.3V pin on the RFID module

2. NodeMCU LCD I2C (16x2)
   Pin GPIO 21 on ESP32 connects to the SDA pin on the LCD I2C
   Pin GPIO 22 on ESP32 connects to the SCL pin on the LCD I2C
   Pin GND on ESP32 connects to the GND pin on the LCD I2C
   Pin 5V on ESP32 connects to the VCC pin on the LCD I2C
3. NodeMCU - Fingerprint Sensor
   Pin GPIO 17 (TX) on ESP32 connects to the RX pin on the fingerprint sensor
   Pin GPIO 16 (RX) on ESP32 connects to the TX pin on the fingerprint sensor
   Pin GND on ESP32 connects to the GND pin on the fingerprint sensor
   Pin 3.3V on ESP32 connects to the VCC pin on the fingerprint sensor
4. NodeMCU - Relay Module untuk Solenoid
   Pin GPIO 5 on ESP32 connects to the IN pin on the relay module
   Pin GND on ESP32 connects to the GND pin on the relay module
   Pin 5V on ESP32 connects to the VCC pin on the relay module
5. NodeMCU – Buzzer
   Pin GPIO 13 on ESP32 connects to the positive pin of the buzzer
   Pin GND on ESP32 connects to the negative pin of the buzzer
6. NodeMCU - Push Button
   Pin GPIO 15 on ESP32 connects to one of the pins on the push button
   The other pin on the push button connects to GND
7. NodeMCU - Power Supply
   Pin GND on ESP32 connects to the GND on the power supply
   Pin 5V on ESP32 connects to the 5V on the power supply for the breadboard

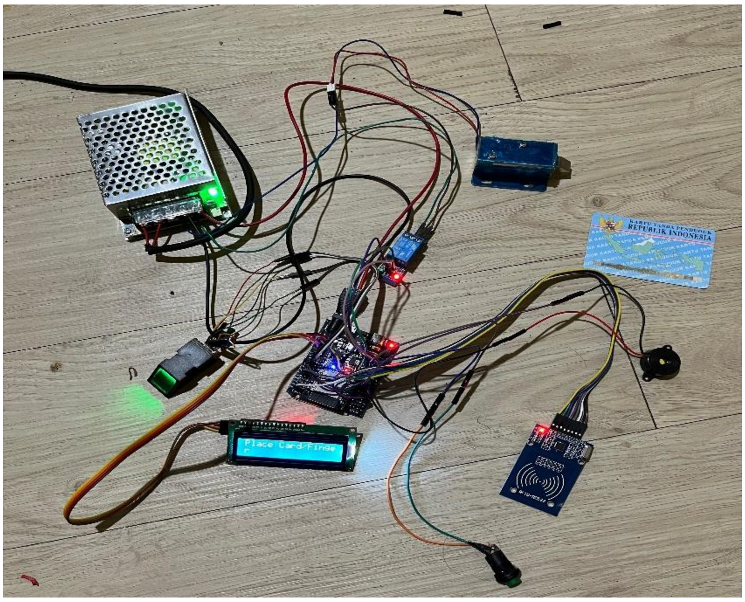
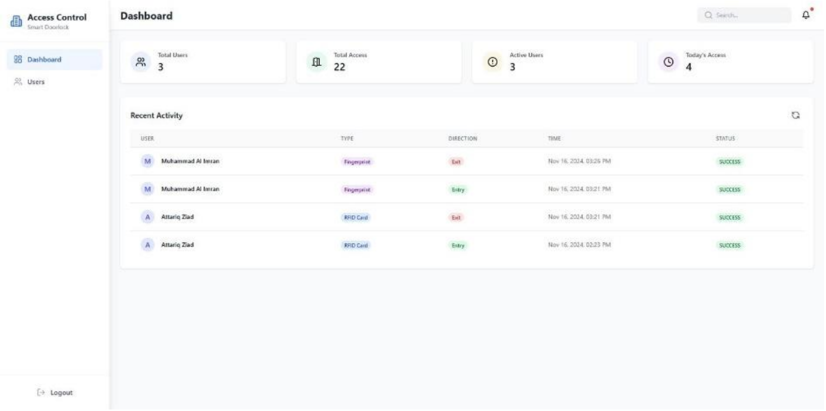


Figure 5. Prototype

After creating the prototype, the next step is to develop the website-based information system, for the website's appearance:



Dashboard

Total Users 3

Total Access 22

Active Users 3

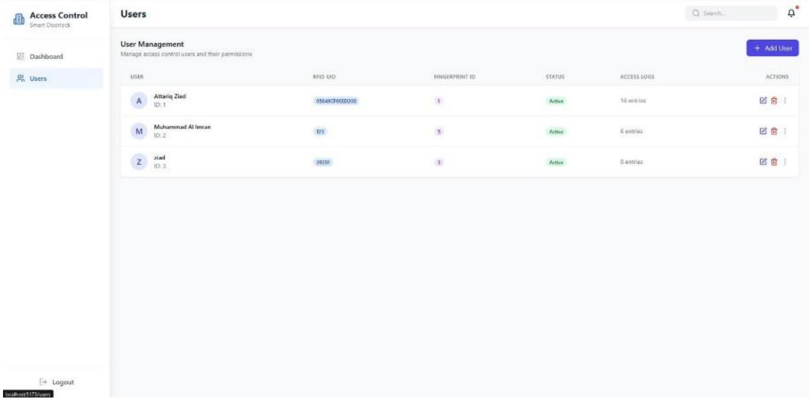
Today's Access 4

Recent Activity

USER	TYPE	DIRECTION	TIME	STATUS
M Muhammad Al Imran	Fingerprint	Exit	Nov 16, 2024, 03:26 PM	SUCCESS
M Muhammad Al Imran	Fingerprint	Entry	Nov 16, 2024, 03:21 PM	SUCCESS
A Attariq Ziad	RFID Card	Exit	Nov 16, 2024, 03:21 PM	SUCCESS
A Attariq Ziad	RFID Card	Entry	Nov 16, 2024, 02:23 PM	SUCCESS

Figure 6. Dashboard

On the dashboard display, there is a user activity table that records various important information. It contains data such as the user's name, authentication method (fingerprint or RFID card), access direction (entry or exit), access time, and access success status. This table functions as a history log, providing complete information about who accessed, when, and how the process took place. This page allows the admin to monitor and manage access in real-time.



Users

User Management

Manage access control users and their permissions

USER	RFID UID	FINGERPRINT ID	STATUS	ACCESS LOGS	ACTIONS
A Attariq Ziad ID: 1	05849CF6EED200	1	Active	16 entries	
M Muhammad Al Imran ID: 2	123	5	Active	6 entries	
Z ziad ID: 3	39201	3	Active	0 entries	

Figure 7. User

This page is the User Management interface of the Smart Door lock Access Control system, used to manage user data. The table on this page records the main information of each user, such as name, unique ID, RFID card number, fingerprint ID number, account status (active or inactive), and the number of recorded access logs. Additionally, there are action buttons in the last column of the table for editing or deleting user data. The navigation on the left provides access to the Dashboard menu for monitoring system activity overall and the Users menu for managing user data. At the top, there is an "Add User" button that makes it easy for the admin to add new users to the system. For a clearer view, the "Add User" button can be seen in Figure 7 below:

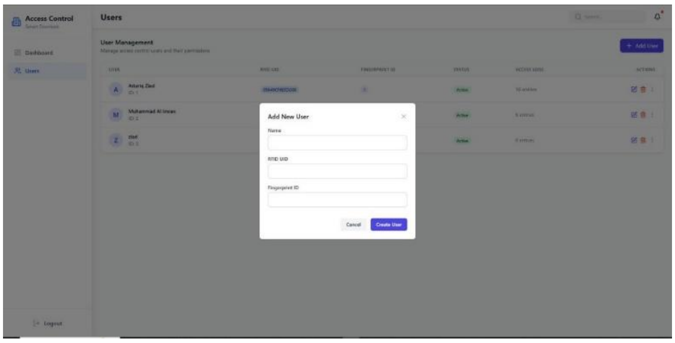


Figure 8. Add user

This page is designed to make it easier for the admin to add new users to the system. The form consists of several main input elements, namely:

1. Name: An input field to enter the full name of the user who will be registered in the system. This name will serve as the user's primary identity in the user list.
2. RFID ID: This field will be automatically populated after an RFID card (such as an ID card or other access cards) is placed on the RFID sensor. The system will read the unique card number and record it as the user's RFID ID.
3. Fingerprint ID: This field will also be automatically populated after the user places their fingerprint on the fingerprint scanner. The system will generate a unique identification number for the fingerprint and record it as the user's Fingerprint ID.

After all the information is filled out, the admin can press the Submit button to save the new user's data into the system. This form ensures that each user has accurate and unique information to access the system using their RFID card or fingerprint

4. Conclusions

The conclusion of this research shows that the Internet of Things (IoT)-based smart door lock system designed using ESP32 microcontroller, RFID sensor for E-KTP identification, and fingerprint sensor succeeds in improving door access security effectively. The integration of RFID and fingerprint sensors provides a double layer of authentication that strengthens the locking system, while making it easier for registered users to open the door without the need for a physical key. In addition, the web-based monitoring feature enables real-time access monitoring, which increases user flexibility and control in managing the security of residences or public places. With these advantages, this IoT-based smart door lock system is expected to be a practical and efficient security solution and contribute to reducing crime rates through better protection of door access.

References

[1] Syahputra, D. (2022). Angka Kriminalitas di Lhokseumawe Naik di 2022, Didominasi Pencurian dengan Kekerasan. INews Aceh.

[2] Pratama, Heroik M., and Nurul Amalia. Adoption of Voting Technology: A Guide for Electoral Stakeholders in Indonesia. International Institute for Democracy and Electoral Assistance (International IDEA), 2020.

[3] Budiman, Shahril, and Kedah Darul Aman. "DECLARATION OF ORIGINALITY..

[4] Ho, Grant, et al. "Smart locks: Lessons for securing commodity internet of things devices." Proceedings of the 11th ACM on Asia conference on computer and communications security. 2016.

[5] Hazazi, Hussein. Understanding and Improving the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User. Diss. The University of North Carolina at Charlotte, 2024.

[6] Sahani, Mrutyunjaya, et al. "Web-based online embedded door access control and home security system based on face recognition." 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. IEEE, 2015.

[7] Pavithra, D., and Ranjith Balakrishnan. "IoT based monitoring and control system for home automation." 2015 global conference on communication technologies (GCCT). IEEE, 2015.

[8] Faisal, Mohammad Adrian, and Erwin Sitompul. "Door Security System Using e-KTP RFID Reading and Passive Infrared Sensor." (2019).

[9] Soemartono, Triyuni. "The Dynamic of e-KTP Evaluation Program in DKI Jakarta." BISNIS & BIROKRASI: Jurnal Ilmu Administrasi dan Organisasi 20.2 (2014): 5.

[10] Jain, Anil, and Sharath Pankanti. "Fingerprint classification and matching." Handbook for Image and Video Processing (2000): 821-836.

[11] Allen, Robert, Pat Sankar, and Salil Prabhakar. "Fingerprint identification technology." Biometric systems: Technology, design and performance evaluation. London: Springer London, 2005. 22-61.

[12] Tucker-Drob, Elliot M., and Daniel A. Briley. "Continuity of genetic and environmental influences on cognition across the life span: a meta-analysis of longitudinal twin and adoption studies." Psychological bulletin 140.4 (2014): 949.

[13] Finkenzeller, Klaus. RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. John wiley & sons, 2010.

[14] Jia, Xiaolin, et al. "RFID technology and its applications in Internet of Things (IoT)." 2012 2nd international conference on consumer electronics, communications and networks (CECNet). IEEE, 2012.

[15] Katuk, Norliza, and Ikenna Rene Chiadighikaobi. "An enhanced block pre-processing of PRESENT algorithm for fingerprint template encryption in the internet of things environment." *International Journal of Communication Networks and Information Security* 13.3 (2021): 474-481.

[16] Ammar, Mahmoud, Giovanni Russello, and Bruno Crispo. "Internet of Things: A survey on the security of IoT frameworks." Journal of Information Security and Applications 38 (2018): 8-27.

[17] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.

[18] Nurwijayanti, K. N., & Abdul Basyir. (2021). IoT-based Automated Door-Lock System Integrated with RFID for Improved Security

[19] Najib, A. A., Munadi, R., & Karna, N. B. A. (2021). RFID with E-KTP Integration for IoT Home
Security Systems

[20] Yulisman, N. I., Sabna, E., & Fonda, H. (2021). IoT-Based Smart Door Lock with E-KTP for Enhanced Home Security

[21] Alvayen, S., & Karnadi, K. (2022). Real-Time Monitoring and Access Control with IoTIntegrated RFID Systems

[22] Wiranata, A., Rizalitaher, A. S., & Daulay, W. A. A. (2023). Educational Application of IoTEnabled RFID for Remote Door Control and Monitoring