Jurnal ICT : Information and Communication Technologies, 16 (2) (2025) 412-424

Published by: Marq & Cha Institute

Jurnal ICT : Information and Communication Technologies

Journal homepage: www.ejournal.marqchainstitute.or.id/index.php/JICT

Mekro Bisnis Center IoT-Based Housing Security System with Automatic Barrier Using e-KTP Verification and Sound Indicators

Muhammad Aidil Dzikri[1], Maulia Rahman[2]
[1,2] Informatika, Universitas Potensi Utama, Medan, Indonesia

Article Info

Article history

Received : Oct 25, 2025
Revised : Oct 28, 2025
Accepted : Oct 30, 2025

Keywords:

Automatic Access Control;
e-KTP,
Internet of Things;
Residential Security;
RFID.

Abstract

Residential security is an essential aspect of ensuring the comfort and safety of residents. However, the use of conventional systems such as manual security guards and barrier gates without identity verification is still commonly found, including at the Mekro Business Center Housing Complex. Problems arising from these systems include inefficiency, the potential for unauthorized access, and limitations in manual surveillance by security personnel. To address these issues, an automated system is needed to manage residential access in real-time and enhance overall security. This study aims to develop a security system based on the Internet of Things (IoT) using an automatic barrier gate equipped with e-KTP verification via RFID and a sound indicator for real-time notifications. The system was designed using the Fishbone Diagram approach as a reference in designing the components and workflow of the security system. The tools used include an ESP32 microcontroller, RFID RC522 module, infrared sensor, buzzer, and DFPlayer Mini speaker, all integrated with the Blynk application and a monitoring website. The testing process was conducted experimentally using the blackbox method through a miniature physical prototype simulation in six different scenarios. Out of 35 total tests, the system responded correctly 30 times under online conditions, achieving a 100% success rate in scenarios involving authorized access, unauthorized access, intrusion attempts, emergency access, and control via the application. All tests under offline conditions failed due to the lack of internet connectivity. The results show that this system can improve the efficiency and reliability of automatic access control in residential environments and support the performance of security personnel.

Corresponding Author:

Muhammad Aidil Dzikri
Informatika
Universitas Potensi Utama,
Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia
Email : muhammadaidildzikri25@gmail.com

1. Introduction

Technological advances in the era of globalization encompass machinery, communications, and electronics. Modern technology has transformed the way we live, including maintaining residential security. Security has become a crucial issue due to the rise in crime, such as theft and robbery.

The rise in crime in residential areas is a serious concern. In the Medan area, 562 cases of aggravated theft (curat) and 128 cases of violent theft (curas) were recorded in 2023, with residential areas being the primary target. The lack of a security system is a major contributing factor to crime in this area. (Antara News, 2023)

The lack of security systems, such as CCTV and security guards, is often the cause of incidents. One example occurred in the Rorinata Housing Complex in Sunggal. In this case, a gang of thieves successfully broke into a resident's home and stole a motor vehicle. The lack of security surveillance, such as the absence of CCTV and security guards, was the primary reason for this incident (Tribun Medan, 2024).

Conventional security systems, such as manual security, are no longer effective. Internet of Things (IoT)-based innovations offer solutions by connecting devices for monitoring and rapid response. RFID technology allows e-KTPs to be used as tags for automatic identity verification, providing enhanced security. Research by Firmansyah and Cahyono (2022) demonstrated the effectiveness of IoT with its real-time notification feature via Telegram.

Audible indicators also enhance security by providing early warnings when suspicious activity is detected. Research by Fakhruddin (2024) supports the efficiency of IoT with an ESP32 microcontroller in managing security.

Furthermore, interviews with the management of the Mekro Business Center Housing Complex revealed that the current security system still uses a manual method, with the gate open from 6:00 a.m. to 12:00 a.m. Residents or guests must report to the security post, but this system has significant shortcomings. The gate is not always strictly monitored, allowing guests to enter without prior notification, and outsiders such as scavengers or beggars to enter without permission, especially when the guards are on duty or on break.

Although there have been no criminal incidents in the past five years, the Mekro Business Center Housing management recognizes that the manual security system has loopholes that could be exploited by malicious parties. The use of technology such as automatic barriers is considered to strengthen the security system, expedite the verification process, and still allow collaboration with security guards as the primary supervisors.

2. Research Methodolgy

The stages in designing a system can be seen in the fishbone diagram in Figure 1.

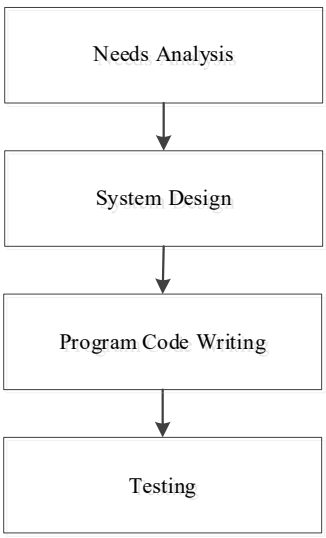

Figure 1 Fishbone Diagram

This diagram illustrates the essential steps involved in designing an IoT-based security system, including requirements analysis, system design, coding, testing, and evaluation. Each stage plays a crucial role in ensuring the system's effective functioning. These stages are further explained below.

1. Needs Analysis
   Needs Analysis: In this stage, researchers collect research-related data and determine the software and hardware tools to be used in system development. This needs analysis includes the hardware and software requirements needed to build and test the system. The following are the software tools used for system implementation and development:
   a. Windows 11 Operating System
   b. Arduino IDE as a programming platform.
   c. Blynk for remote control and monitoring.

   The following are the hardware tools required for system implementation and development:
   - Laptop as a device for system development and programming
   - e-KTP as a user verification tool.
   - ESP32 microcontroller as the main controller.
   - RFID RC522 for verification.
   - Servo motor to open and close the barrier.
   - Infrared sensor (IR obstacle) to detect vehicle presence.
   - Additional components such as a 0.96-inch OLED display, buzzer, small 8-ohm speaker, DFPlayer Mini, MicroSD card, LED lights, 220-ohm resistor, push button, double-sided PCB, magnetic sensor, and jumper cables.

     In addition, the author had one crucial requirement: collecting references. The author collected references in the form of theories used in related research, which served as sources for the author's research. In this case, these included journals on automatic barrier gates, residential security, and the ESP32 microcontroller, as well as prototype-based automated system design. These references served as the basis for system development and design.
2. System Design
   In the system design stage, the researcher created the system using several Unified Modeling Language (UML) design models, namely:
   • Use Case Diagram: Describes user interaction with the system.
   • Activity Diagram: Describes the system's operational processes.
   • Sequence Diagram: Describes the sequence of interactions between components.

   Furthermore, the system is designed to integrate IoT, where the ESP32 microcontroller can communicate with hardware such as RFID and servo motors, and connect to the Blynk application to enable remote control and monitoring. As a testing phase, a miniature physical prototype was created to test and simulate the automatic barrier system, including all components integrated as needed.
3. Writing Program Code
   In this stage, the system design will be implemented into program code that can be recognized by a computer. Programming begins using the C++ language through the Arduino IDE platform. The program code is designed to control each hardware function, such as RFID card reading, servo motor movement, and sending sound notifications. Implementation is carried out using the C++ language on the Arduino IDE platform to ensure the system functions according to the design.
4. Testing
   This testing was conducted to ensure that the prototype built functioned properly and was free from design and programming errors. This prototype was the result of research conducted by 30 authors to design and build a miniature system. The testing conducted by the authors was as follows:

a. Prototype Testing and Implementation.
The authors conducted a series of tests on the prototype, including testing each component on a miniature scale to ensure that everything functioned as expected. This testing was conducted on the hardware and software used in the prototype, involving the device through a smartphone application, Blynk. This smartphone was then connected to the internet, allowing the authors to remotely control the Esp32 microcontroller, which was also connected to the internet. In this case, the authors used the Blackbox Testing method, which refers to the operation of the system based on its functional elements. This was to ensure that the prototype built could function properly and meet its intended purpose in real-world conditions.

5. Results
At this stage, conclusions were drawn from the development of a prototype IoT-based security system for protecting residential access using e-KTP verification and voice indicators. This research was conducted in a simulated environment with a prototype that used hardware and software that represented real-world conditions at the Mekro Business Center Housing Complex, without direct on-site implementation. The prototype test results showed that the system successfully integrated RFID-based e-KTP verification, voice notification, and automatic barrier control features as designed. However, the testing revealed that the stability of the IoT connection under unstable network conditions and the system's response to real-time notifications still needed improvement. Overall, this prototype was effective in enhancing access security and supporting surveillance. However, further development is needed to improve the system's reliability to ensure it is more ready for implementation in a real-world residential environment.

3. Results and Discussion

3.1. Discussion

This research aims to design and develop an IoT-based residential security system that integrates RFID-based e-KTP verification and audio indicators to provide real-time notifications of threats and unauthorized access. This system is designed to improve the effectiveness of residential security and reduce reliance on manual security.

One of the main problems faced by conventional security systems in the Mekro Business Center Housing Complex is the lack of efficiency and effectiveness in preventing crime. Data shows that in the Medan area, there were 562 cases of aggravated theft (curat) and 128 cases of violent theft (curas) in 2023, with residential areas as the primary target (Antara News, 2023). The lack of security systems such as CCTV and security guards is a major factor contributing to the high crime rate in residential areas.

Security systems that still rely on manual security have various weaknesses, such as limited access monitoring and the lack of an early warning system to detect suspicious activity. Manual security also requires human labor, which can cause delays in responding to security threats.

Furthermore, security systems that are not integrated with modern technology make access monitoring slow and inefficient. This system also lacks early warning features such as an audible indicator that can provide real-time notification of unauthorized access. As a result, residents of the Mekro Business Center Housing Complex are more vulnerable to criminal activity.

Based on these issues, this study proposes the implementation of an IoT-based security system that incorporates RFID-based e-KTP technology to automatically control entry and exit. Furthermore, the system will be equipped with an audible indicator as an early warning that can provide real-time notification of security threats. Thus, it is hoped that this system will be able to improve the security of the Mekro Business Center Housing Complex more effectively and efficiently.

a. Circuit Block Diagram

In general, the design of an automatic barrier system using an ESP32 microcontroller with Internet of Things (IoT) technology features authentication using an RFID-based e-KTP and can be

controlled through the Blynk application. This system enables the automatic opening and closing of the barrier using a predetermined authentication method. In this feature, the ESP32 microcontroller serves as a pre-programmed control center. This system has two settings: manual and automatic.

1. In the manual setting, the user uses a push button to directly open or close the barrier.
2. In the automatic setting, the system reads data from the e-KTP or RFID sensor and controls a servo motor to automatically open or close the barrier. Access information is displayed on an OLED LCD screen, and audible notifications are provided via a buzzer.

With this system, the authentication and access management processes can be more secure and efficient. To facilitate the design, a block diagram was created, as shown in Figure 2 below:

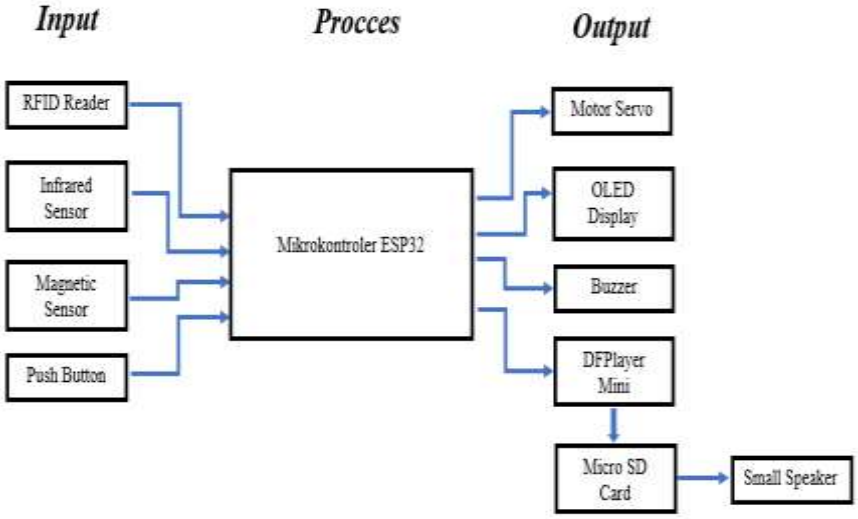

Figure 2. Circuit Block Diagram

The explanation and function of each block are as follows:

a. ESP32 Microcontroller: Serves as the control center for the entire circuit system. The ESP32 receives data from various sensors and input modules, then processes it to control the output devices.
b. RFID Reader: Serves to read data from the e-KTP (electronic ID card) and sends it to the microcontroller for processing as part of the access verification system.
c. Servo Motor: Serves as an actuator that automatically moves the barrier based on commands from the microcontroller after successful authentication.
d. Infrared Sensor: Serves to detect the presence of objects around the barrier and prevent it from closing if there are obstacles, thereby increasing user safety.
e. 0.96" OLED Module: Functions to display access status information, such as e-KTP validation, barrier status, and error indications if problems occur.
f. Buzzer: Provides audible notifications to indicate success or failure in the authentication process. For example, a short beep indicates access is accepted and a long beep indicates access is denied.
g. Magnetic Sensor: Functions to detect unauthorized access to the barrier. If the barrier is opened without permission, this sensor will send a signal to the microcontroller to provide a real-time warning and activate an alarm.
h. Push Button: Used as a manual control to directly operate the system, such as opening or closing the barrier in an emergency.
i. Small Speaker: Functions to play audio as an audible notification of automatic barrier access, whether access is accepted or denied.
j. DFPlayer Mini: An audio file player module that can be used to output sound from the system. This module receives commands from the ESP32 to play audio files stored on a MicroSD card.

k. MicroSD Card: Functions as an audio file storage medium used by the DFPlayer Mini to provide audible notifications.

b. Use Case Diagram

A Use Case Diagram is a model for the behavior of the information system to be created. A use case describes the interaction between one or more actors and the information system being developed. The following is a design of the processes involved in the IoT-based Mekro Business Center residential security system, which includes an automatic barrier using e-KTP verification and a sound indicator.

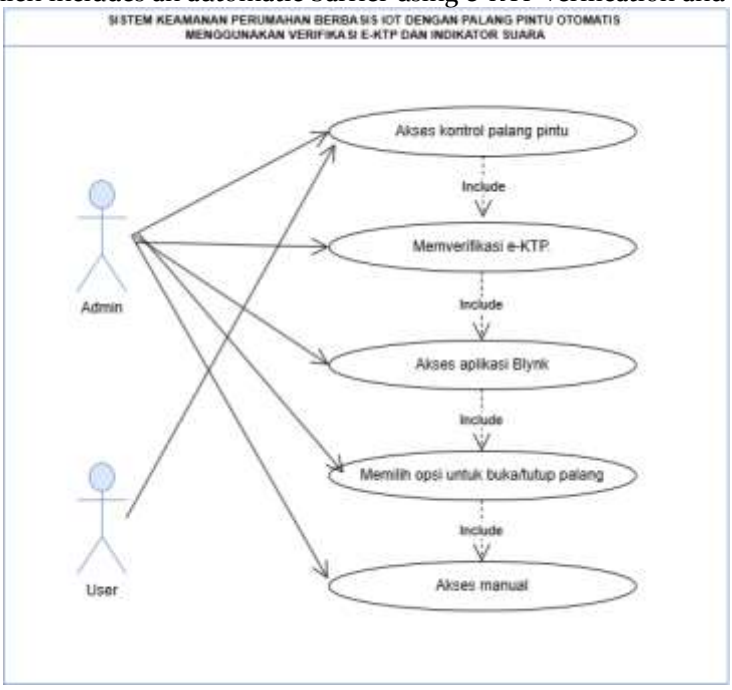

Figure 3. Use Case Diagram

3.2. Result

a. Blynk App

The initial display when creating a new project in the Blynk application can be seen in Figure 4

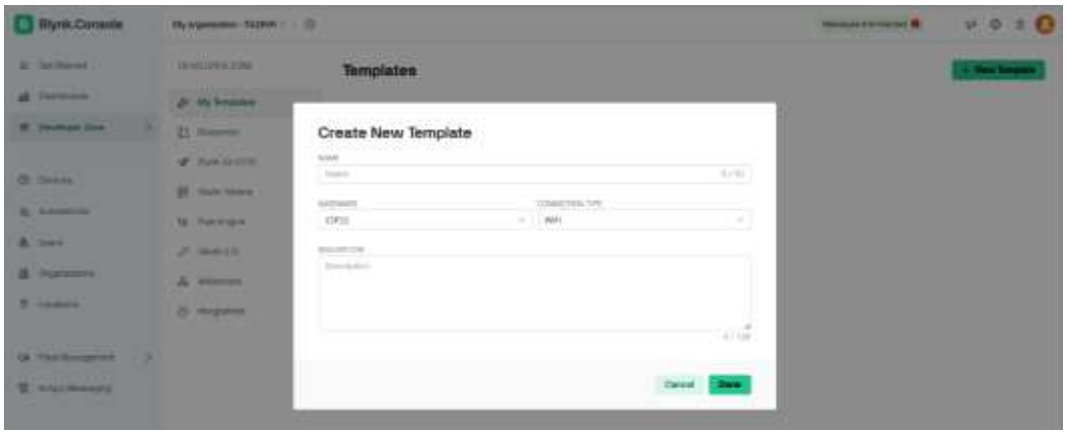

Figure 4. New Project in Blynk

After the new template is successfully created, select New Device. Once successfully created, the display will appear as shown in Figure 5.

Figure 5. Initial Blynk Project Display

The Blynk interface can be customized to suit your needs, such as adding buttons, LEDs, and access information. Figure 6 shows the interface used in this system.

Figure 6. Security System Project Display in the Blynk Application

Caption for Figure IV.3:

1. The Lock LED functions as an indicator of the gate's locked status (access is closed).
2. The Open LED functions as an indicator when the gate is open.
3. The Alarm LED will illuminate if unauthorized access occurs or the gate is forced open, displaying a warning notification on Blynk.
4. The Access ON/OFF button is used by the housing administrator to open or close the gate remotely.
5. The Full Name, Resident Identification Number, and Access Status columns display data from the e-KTP card detected by the RFID system.

b. Website

The login page is the main gateway to access the system. Users are required to enter their registered username and password to log in. This authentication process aims to maintain access security so that unauthorized individuals cannot access the management system. This is shown in Figure 7 below.

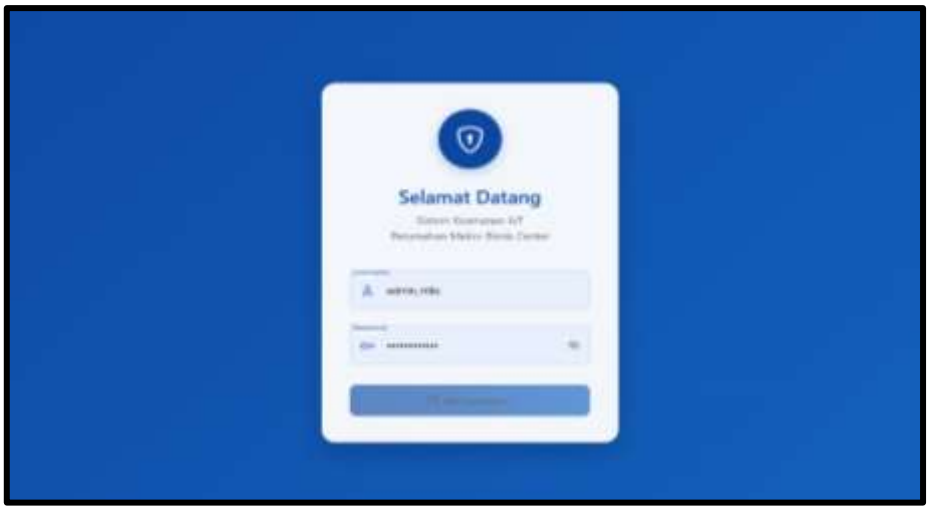

Figure 7. Login Display on the Housing Security System Website

After logging in as a user (security guard), users will be directed to a dashboard page that displays summary information such as total access today, number of registered residents, approved and denied access, and weekly statistics graphs. This dashboard display is for informational purposes only and does not provide data management features. This can be seen in Figure 8.

Figure 8. User Dashboard Display on the Website

Unlike users, admins have broader access. The admin dashboard displays the same data as users, but is equipped with navigation buttons to access management features such as card management, a list of unregistered cards, and resident data settings. This display makes it easier for admins to control overall system access.

Figure 9. Admin Dashboard Display (Housing Manager)

The access history page displays a complete list of all access activities performed through the system, whether using RFID, Blynk, or push buttons. Each history record records the full name, NIK (National Identity Number), access time, and status (accepted, rejected, or unauthorized). To maintain data security, the NIK and card ID stored in the database are encrypted so they cannot be accessed arbitrarily. This page can be accessed by both users and admins, as shown in Figure 10 below.

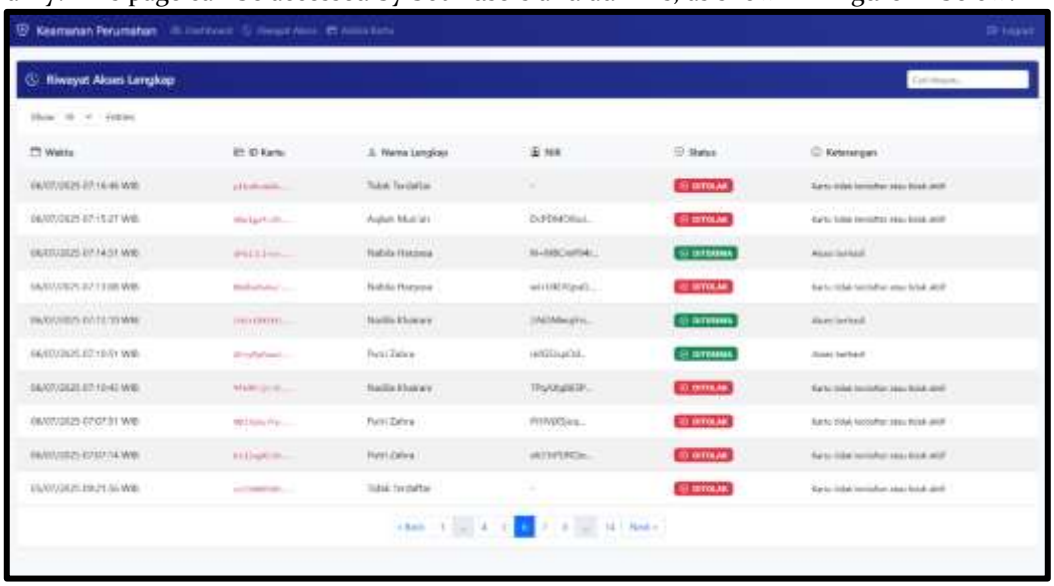

Figure 10: Access History Page Display on the Website

Furthermore, the card management page can only be accessed by admins and is used to register new resident e-KTP cards, edit user data, or delete access from cards that are no longer in use. This feature is crucial in ensuring that only verified cards can be used to open the automatic barrier. To maintain data security, the NIK and card ID are encrypted and can only be viewed by the admin through the card management page. This can be seen in Figure 11 below.

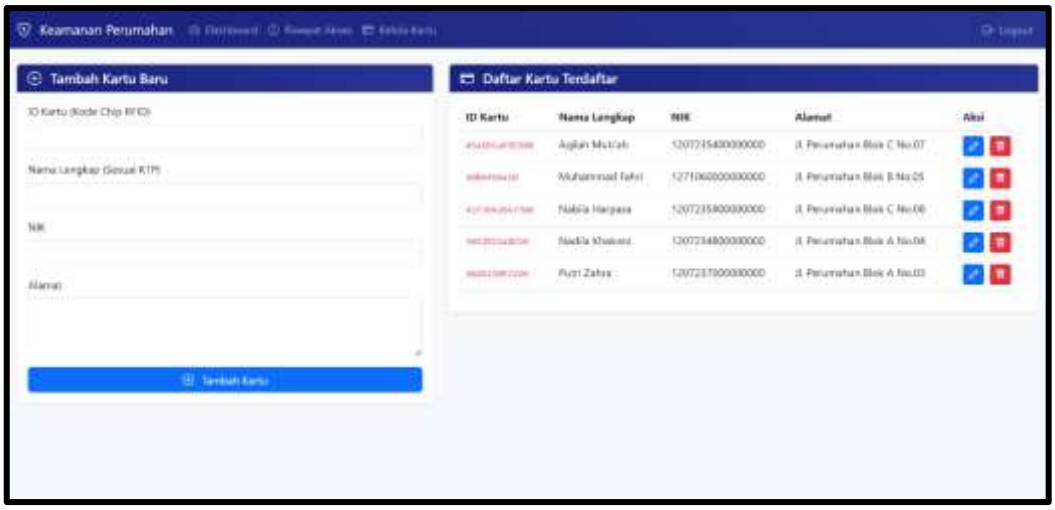

Figure 11: Card Management Page Display by Admin

This "Unregistered Cards" page is also specifically for admins, displaying a list of e-KTP cards that have been affixed but not yet registered in the system. This feature makes it easier for administrators to identify invalid cards and can be used to verify data before they are officially registered. This can be seen in Figure 12 below.

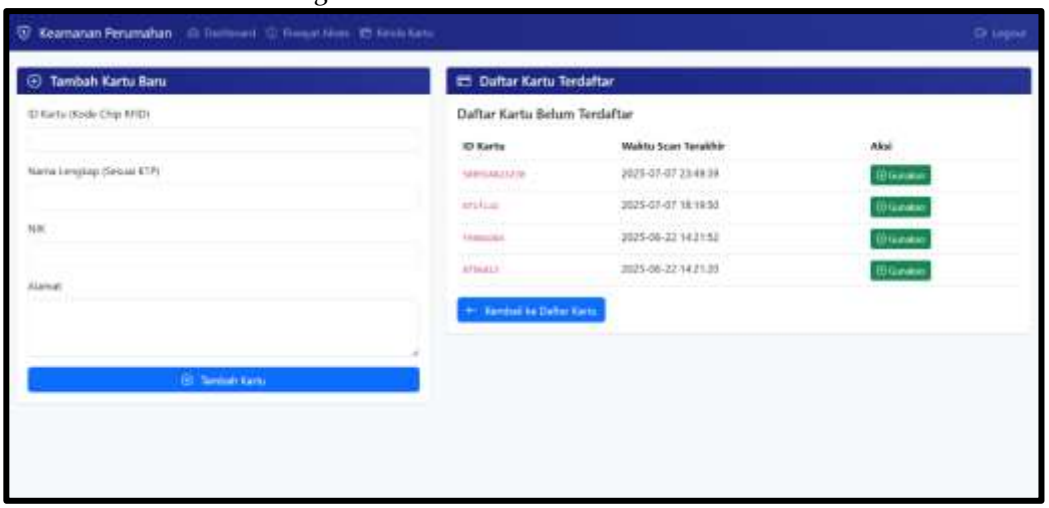

Figure 12. Unregistered Cards Page Display by Admin

c. Design Implementation Results

The following displays the results of the Mekro Business Center residential security system based on the Internet of Things (IoT) with an automatic barrier using e-KTP verification and an audible indicator. This system is designed to automatically manage residents' entry and exit. It can be monitored via the Blynk application and website, and is equipped with real-time security notifications. The resulting design can be seen in Figures 13 and 14

Figure 13: Design Result Display (Front View)

Figure 14: Design Result Display (Top View)

The system designed by the researchers has been successfully implemented and according to plan. The system operates by using an infrared sensor that detects an object approaching the barrier. When an object is detected, the system displays a message on the OLED screen and plays a welcoming sound to prompt the user to attach their e-KTP to the RFID. If the affixed card is registered, the system automatically opens the barrier using a servo motor, the green LED lights up, and the buzzer sounds briefly to indicate access is accepted. Conversely, if the card is not registered, the system will deny access, the red LED will illuminate, and a long buzzer will sound as a warning.

Once the object passes the infrared sensor and is no longer detected, the barrier will close automatically, and the OLED display will return to the home page. If the barrier is opened by force, the magnetic sensor will activate a continuous buzzer alarm, and a notification will be sent to the Blynk app. All access activity is also recorded and can be viewed on the website by both the user (security guard) and the administrator (housing manager).

4. Conclusion

Based on the results of observations and testing of the housing security system conducted by researchers, the following conclusions can be drawn: The integration of RFID-based e-KTP with IoT successfully provides more secure and efficient access control. The trial results showed that the system can automatically distinguish between authorized and unauthorized access and attempted burglaries. This minimizes the risk of crime because every access is recorded and only residents with registered e-KTPs can enter. IoT-based sound indicators have proven effective as early warnings. The buzzer system and DFPlayer Mini provide real-time notifications when unauthorized access or attempted burglaries

are detected. This way, residents and security guards can immediately respond to threats. The implementation of an automated system with IoT-based gates can replace some manual guard functions. Entry and exit access can be controlled automatically, while security guards continue to act as additional supervisors. This makes the monitoring process faster, more efficient, and less dependent on security officers. IoT-based security systems have been proven to reduce reliance on manual guarding. With the integration of e-KTP, sound indicators, the Blynk application, and website monitoring, response to threats is faster, more structured, and more documented. This system improves the security of the Mekro Business Center housing compared to conventional methods that only rely on security guards and manual barriers.

References

Alfan, A. N., & Ramadhan, V. (2022). Prototype Detektor Gas dan Monitoring Suhu Berbasis Arduino Uno. *Jurnal PROSISKO, 9*(2), 61-69.

Alfina, O., & Harahap, F. (2019). Pemodelan UML Sistem Pendukung Keputusan dalam Penentuan Kelas Siswa-Siswa Tunagrahita. *METHOMIKA: Jurnal Manajemen Informatika & Komputerisasi Akuntansi, 3*(2), 143-150.

Arinal, V., Nuari, F. A., Sanip, W., Taufik, M., & Sarikah, D. (2024). Implementasi Alat Deteksi Plat Nomor Kendaraan untuk Otomatisasi Palang Pintu pada Lingkungan Perumahan RT 05/05 Gondrong dengan Machine Learning. *Kohesi: Jurnal Multidisiplin Saintek, 2*(10), 91-112.

Azlan, M. U., & Zainal, M. S. (2024). An IoT Based Home Security System With ESP32, Video Monitoring, and Blynk Integration. *Enhanced Knowledge in Sciences and Technology, 5*(1), 238-244.

Badri, F., Sari, I. P., & Pratama, R. A. (2023). Simulasi Rancang Bangun Palang Pintu Otomatis Berbasis RFID (Radio Frequency Identification). *Jurnal Teknologi dan Rekayasa Sistem, 12*(3), 45–52.

Daulay, B. H., Jannah, M., & Pasaribu, S. A. (2024). Sistem Keamanan Pintu Menggunakan E-KTP Berbasis Sensor RFID (Radio Frequency Identification). *Jurnal Mahkota Informatika, 1*(1), 31-41.

Fakhruddin, A. (2024). Rancang Bangun Sistem Keamanan Pintu Rumah Berbasis Internet of Things dengan ESP32 dan Aplikasi Blynk. *Jurnal Teknik Elektro dan Informatika, 19*(1), 53–59.

Firmansyah, M., & Cahyono, Y. (2022). Sistem Keamanan Pintu Rumah Menggunakan e-KTP dan Notifikasi dengan Telegram Berbasis IoT. *Prosiding Seminar Nasional Informatika dan Sistem Informasi, 7*(1), 136–143.

Janis, J. W. (2020). Rancang Bangun Aplikasi Online Sistem Pemesanan Jasa Tukang Bangunan Berbasis Lokasi. *Jurnal Teknik Informatika, Universitas Sam Ratulangi Manado, 15*(1), 1-12.

Johan, T. M., & Herizal. (2022). Rancang Bangun Palang Pintu Otomatis Berbasis Arduino Menggunakan Kartu RFID. *Jurnal Teknologi Sistem Otomasi, 8*(2), 78–85.

Kurniawan, D. (2021). Rancang Bangun Sistem Akses Kontrol Keluar Masuk Perumahan Menggunakan Sensor Fingerprint Berbasis Mikrokontroler ATmega328. *Jurnal Teknologi dan Rekayasa Sistem, 4*(2), 120-130.

Manurung, S., Parlina, I., Anggraini, F., Hartama, D., & Jalaluddin. (2021). Penggunaan Sistem Arduino Menggunakan RFID untuk Keamanan Kendaraan Bermotor. *Jurnal Penelitian Inovatif (JUPIN), 1*(2), 139-148.Mubarok, F. H. A., & Subali, M. (2020). Sistem Keamanan Pintu Portal pada Perumahan dengan RFID Menggunakan NodeMCU Berbasis Website. *Seminar Nasional Teknologi Informasi dan Komunikasi STI&K (SeNTIK), 4*(1), 311-321.

Muhammad, S. (2023). Krisis keamanan harus jadi fokus utama kapolrestabes Medan yang baru. *ANTARA News Sumatera Utara*. Diakses dari https://sumut.antaranews.com/berita/555879/krisis-keamanan-harus-jadi-fokus-utama-kapolrestabes-medan-yang-baru.

Mufida, E., Anwar, R. S., & Gunawan, I. (2020). Rancangan Palang Pintu Otomatis pada Apartemen dengan Akses e-KTP Berbasis Arduino. *INSANtek – Jurnal Inovasi dan Sains Teknik Elektro, 1*(2), 52–63.

Nugraha, A. A., Tjahjono, G., & Ray, F. F. G. (2020). Rancang Bangun Sistem Pengaman Menggunakan RFID. *Jurnal Spektro, 3*(2).

Nugroho, G. W., & Effendi, R. (2022). Rancang Bangun Sistem Pengukuran Luas Permukaan Kulit Menggunakan Konveyor dan Sensor Optik Berbasis Arduino. *Jurnal Teknik ITS, 11*(1).

Pokenika, A. J., Alam, T. H. I., & Soekarta, R. (2023). Rancang Bangun Buka Pintu Otomatis Menggunakan E-KTP (Kartu Tanda Penduduk) Sebagai RFID Berbasis Arduino. *FRAMEWORK, 1*(2), 108-116.

Pratama, R. A., & Nada, N. Q. (2024). Pengembangan Sistem Palang Pintu Perumahan Berbasis RFID untuk Meningkatkan Keamanan Lingkungan. *Jurnal Sistem Kendali dan Teknologi Otomasi, 14*(1), 87–95.

Purnama, A., & Sitohang, S. (2022). Rancangan Bangun Sistem Keamanan Rumah Berbasis IoT. *Jurnal Comasie, 6*(1), 78-87.

Purnama Sari, I., & Badri, F. (2023). Penerapan Palang Pintu Otomatis Jarak Jauh Berbasis RFID di Perumahan. *Jurnal Rekayasa dan Aplikasi Teknik Informatika, 10*(4), 123–131.

Robiyanto, R., Putra, W. P., & Raswa. (2023). Implementasi Sistem pada Automasi Barrier Gate Palang Pintu Parkir Menggunakan ESP32 dan RFID. *Coding: Jurnal Komputer dan Aplikasi, 11*(3), 457-466.

Sasmita, S. D., Wibowo, S. A., & Prasetya, R. P. (2021). Penerapan IoT (Internet of Thing) Smart Flower Container pada Tanaman Hias Aglaonema Berbasis Arduino. *JATI (Jurnal Mahasiswa Teknik Informatika), 5*(2).

Sulaeman, W., Alimudin, E., & Sumardiono, A. (2022). Sistem Pengaman Loker dengan Menggunakan Deteksi Wajah. *Journal of Energy and Electrical Engineering (JEEE), 3*(2).

Syukhron, I., Rahmadewi, R., & Ibrahim. (2021). Penggunaan Aplikasi Blynk untuk Monitoring dan Kontrol Jarak Jauh pada Sistem Kompos Pintar Berbasis IoT. *ELECTRICIAN – Jurnal Rekayasa dan Teknologi Elektro, 15*(1).

Tambunan, A., & Prasandi, A. (2024). Lagi-lagi, komplotan maling bobol rumah warga di Perumahan Rorinata di Sunggal, motor raib. *Tribun Medan, 2*(1). Diakses dari https://medan.tribunnews.com/2024/09/22/lagi-lagi-komplotan-maling-bobol-rumah-warga-di-perumahan-rorinata-di-sunggal-motor-raib.

Tantowi, D., & Kurnia, Y. (2020). Simulasi Sistem Keamanan Kendaraan Roda Dua dengan Smartphone dan GPS Menggunakan Arduino. *Jurnal ALGOR, 1*(2), 9-15.

Virgiawan, A., Amini, S., & Purwanto. (2021). Perancangan Keamanan Ruangan dengan Sensor PIR dan Magnetic Door Switch Berbasis Web. *Skanika, 4*(2), 126-132.