JIEE Časopispriemyselnejelektrotechniky
Journal of Industrial Electrical Engineering
ISSN 2454-0900
www.jiee.eu

Centralized access system based on ESP32

[1]*Daniel GAJDOŠ*, [2]*Tibor VINCE*

[1,2]Department of Theoretical and Industrial Electrical Engineering, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Slovak Republic

[1]daniel.gajdos@student.tuke.sk, [2]tibor.vince@tuke.sk

***Abstract* — This article is aimed at bringing information about what an access system is. It will also offer the reader the very design and implementation of such a system, which will familiarize him more closely with the given issue, and provide him with an insight into what is necessary for the system to be operational.**

***Keywords* — access system, card reader, control system, ESP32**

I. Introduction

In modern times, the rapid advancement of technology has had a profound impact on our daily lives. These advancements have permeated various aspects of life, replacing outdated and inefficient methods with more advanced and effective solutions. The integration of these technologies has brought about numerous benefits, such as increased convenience, speed, safety, sustainability, cost-effectiveness, and uninterrupted functionality. Access systems could be an integral part of these technological developments. In the following chapters, we will delve deeper into the world of access systems to explore their significance and implications.

Access systems primarily serve the purpose of authenticating individuals based on their credentials. The authentication process determines whether access should be granted or denied to a given object. Each person is assigned a unique identifier, which allows for their clear identification within the system. These systems have found wide-ranging applications, particularly in scenarios where efficient verification of a large group of people is required within a short timeframe. Presently, access systems are commonly utilized by companies, hotels, as well as institutions such as schools, libraries, theaters, and government buildings.

The paramount objective of these systems is to ensure the security of the protected object. Consequently, it is imperative that they function flawlessly, with robust security measures in place to safeguard against unauthorized access and the interception of transmitted data. In the following chapters, we will embark on the design and implementation of one such access system, aiming to uphold its reliability and integrity.

II. Design of an Access System

When designing the access system for the smaller hotel with 8 rooms, we have opted for an alternative that incorporates a dedicated reader and a separate system for managing and verifying individuals. This choice is influenced by the hardware used in the reader's construction. It is worth noting that there are systems available that integrate evaluation, user configuration, and other settings directly into the reader itself, eliminating the need for additional management systems and hardware. Such systems may be more suitable for scenarios where only one or two readers are required. However, when dealing with a larger number of readers, a more efficient approach involves a centralized system where configurations can be set once for all readers instead of individually for each one. The overall structure of the system is depicted in Fig. 1 , providing a more comprehensive understanding of its components and their interactions.

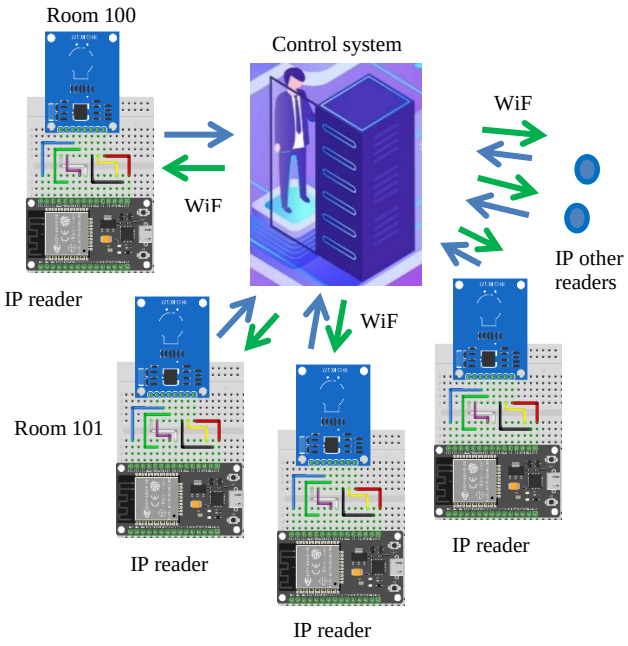

Fig. 1 Design of the structure of the access system in the hotel

In our designed access system, each room is equipped with its own dedicated reader, and communication between the control system and the readers is established through a WiFi network. This configuration allows for seamless communication and data transfer between the control system and the individual readers.

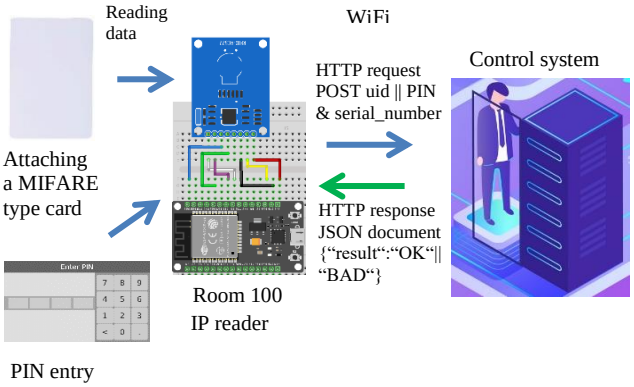

Fig. 2 Communication between the reader and the control system after attaching or entering credentials

Fig. 2 provides a closer approximation of how the entire access system should function. When a person wishes to authenticate, they can do so by presenting their card or entering their assigned PIN code. The reader processes this information and sends it to the control system for evaluation. The control system then assesses the information and responds back to the reader in JSON format with the appropriate response. This two-way communication enables efficient authentication and response handling within the access system.

III. CARD READER IMPLEMENTATION

The card reader module implementation utilizes an ESP32 development board, which is connected to the MFRC522 reader through the SPI bus. The ESP32 development board is equipped with a web server that listens on port 80, specifically designed for the HTTP protocol. The reader program supports two authentication modes. The first mode involves card authentication, where the user presents their card for verification. In case the card is forgotten, the second mode allows authentication using a PIN code. To provide a user-friendly interface, visuals have been designed for both authentication methods using HTML and CSS languages. Fig. 3 depicts the reader environment for card authentication.

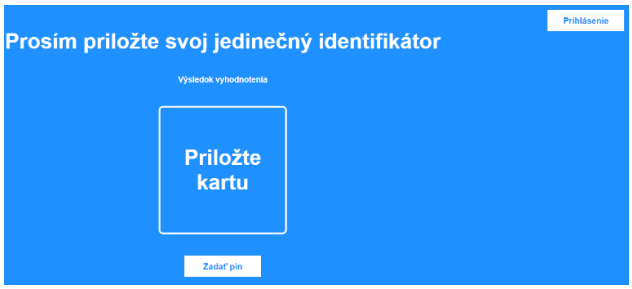

Fig. 3 Authentication using a card

In this particular scenario, if the user decides to authenticate using a PIN code instead of a card, they need to click on the "Enter PIN" button. Upon clicking the button, the system transitions to a new environment, as depicted in Fig. 4.

Fig. 4 Authentication using PIN code

IV. CONTROL SYSTEM IMPLEMENTATION

The system was implemented on a local server using the EASYPHP DEVSERVER program, which includes the Apache server, MYSQL database server, and PHP module. As part of the implementation, the necessary table structure was created. There are a total of 5 tables, with one table containing registered users and the remaining tables used to store records and access rights of individuals assigned to specific rooms.

The system was developed using HTML and CSS, which determined the structure and design of the user interface. PHP was responsible for the dynamic functionality of the system, including communication with the database and the authentication process. Prior to accessing the system settings, users are required to authenticate with a username and password. The application form for authentication can be seen in Fig. 5

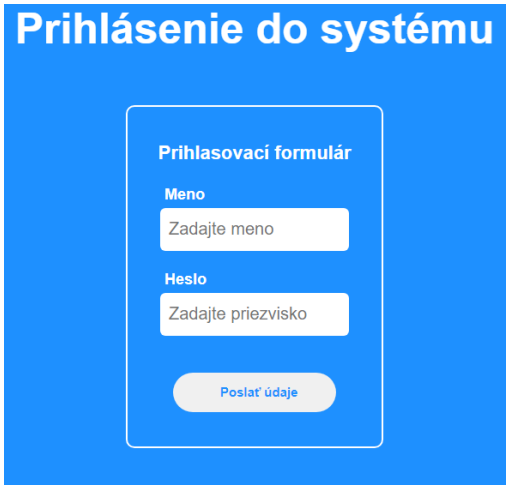

Fig. 5 System login screen

After successfully logging into the system, users have access to two menus: the records menu and the rights menu for setting access privileges. The records menu provides an overview of all access attempts made to individual rooms. Each record includes information such as the name and surname of the authenticated person, the type of authentication used, and the timestamp of the access attempt. A table displaying the records can be seen in Fig. 6.

Tabuľka obsahujúca záznamy

Meno	Priezvisko	identifikátor	Použitý identifikátor	Dátum	Čas	Vyhodnotenie
Jan	Rychly	23219123413	karta	18. 1. 2023	10:23:16	prístup povolený
neevidovany	neevidovany	989208178	karta	18. 1. 2023	10:22:41	prístup zamietnuty
Jan	Rychly	23219123413	karta	17. 1. 2023	21:48:16	prístup povolený
neevidovany	neevidovany	989208178	karta	17. 1. 2023	21:48:11	prístup zamietnuty
neevidovany	neevidovany	989208178	karta	12. 1. 2023	11:24:22	prístup zamietnuty
neevidovany	neevidovany	548	PIN	12. 1. 2023	11:24:15	prístup zamietnuty

Fig. 6 Table containing records

In the rights setting menu, users can assign specific rooms to individuals by entering their card identifier and a unique PIN code. The form for assigning rooms requires users to input all necessary information, which will then be saved in the database. The system ensures that the same identifier is not assigned to multiple individuals, and it also allows for the assignment of multiple rooms to a single person. The form for adding a person to the system can be seen in Fig. 7.

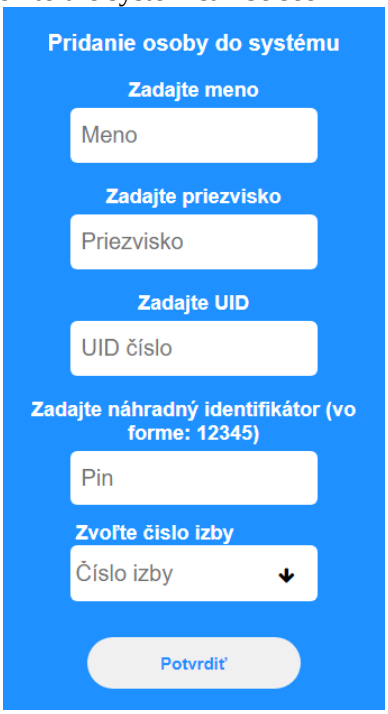

Fig. 7 Adding a person form

In the rights setting menu, users have access to a table displaying the assigned rooms and other relevant information. From this table, users can perform individual record deletions or make specific modifications as needed. The system is designed to handle any errors that may occur during these operations.

The overall process, starting from the authentication of a person to the evaluation by the control system, is illustrated in the activity diagram shown in Fig. 8. This diagram outlines the sequence of activities that occur when a person presents their card for authentication and it undergoes evaluation by the control system. The process would be similar when entering the PIN code, but the diagram specifically focuses on the scenario involving card insertion.

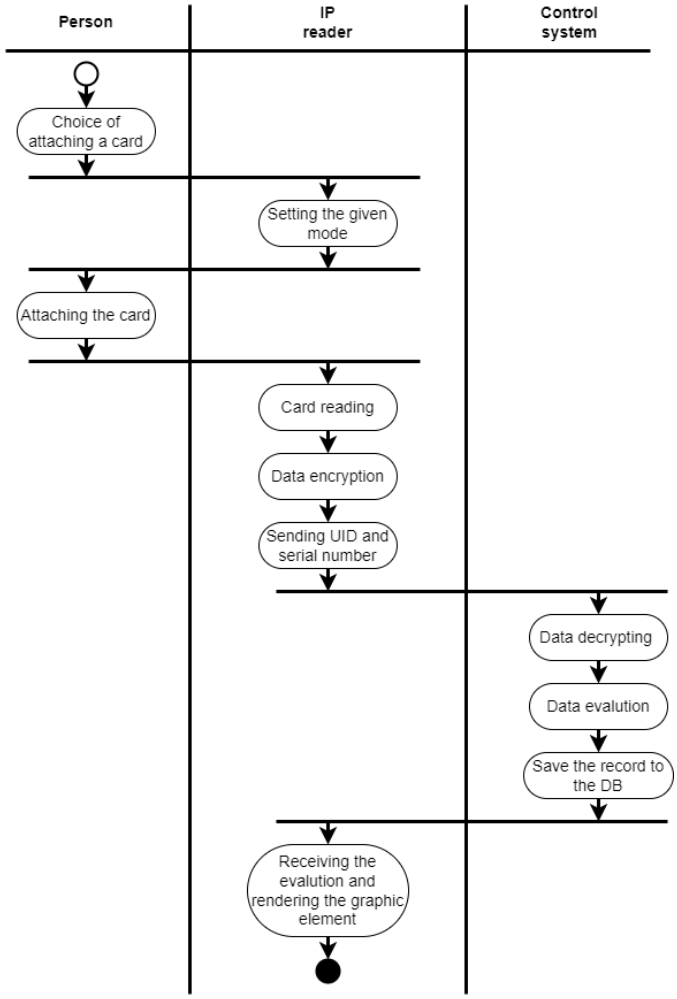

Fig. 8 UML diagram of activities after attaching the card

The process of verification and evaluation begins with the person selecting the verification mode on the reader. Once the mode is chosen, the person inserts their card into the reader. The reader then reads the card data, encrypts it, and sends it along with the reader's serial number to the control system. At the control system, the received data is decrypted, evaluated, and recorded in the database. The evaluation process involves checking the authenticity of the card, verifying the person's credentials, and determining the access rights to the assigned rooms. Once the evaluation is complete, the result is sent back to the reader. The reader receives the evaluation result and notifies the person accordingly. The person is informed of the outcome of the verification process, whether it was successful or unsuccessful, providing them with the necessary feedback. This entire process ensures the secure and efficient verification of individuals using the access system, allowing them to gain or be denied access to the designated rooms based on their authentication and authorization.

V. CONCLUSION

While the current system may have certain limitations and areas for improvement, it serves as a solid foundation for further development. Depending on the level of security required for a particular object, this version of the system can be suitable. However, for objects where a higher level of protection is necessary, additional enhancements and security measures may need to be implemented.

Continuous improvement and refinement of the system can be achieved by addressing the identified limitations, such as enhancing the encryption methods, implementing stricter access control policies, improving the user interface, and ensuring robustness against potential vulnerabilities. Regular updates and monitoring of security standards can also contribute to strengthening the overall security of the system.

By continuously investing in research and development, it is possible to enhance the system's functionality, reliability, and security, thus providing a more comprehensive solution for access control in various environments.

REFERENCES

[1] RANDOMNERDTURTORIALS. ESP32 Pinout Reference: Which GPIO pins should you use? [online]. Randomnerdtutorials.com. [cit. 2023-01-17]. Available on the Internet: https://randomnerdtutorials.com/esp32-pinout-reference-gpios/

[2] WIKIPEDIA. Access control. [online]. En.wikipedia.org. [cit. 2023-01-18]. Available on the Internet: https://en.wikipedia.org/wiki/Access_control

[3] Vince, Tibor, and Olena Slavko. "Enhanced centralized access control system." 2019 IEEE International Conference on Modern Electrical and Energy Systems (MEES). IEEE, 2019.

[4] Changhong, Zhu, and Xie Reneng. "Intelligent laboratory access control system based on ZigBee technology." 2020 International Conference on Virtual Reality and Intelligent Systems (ICVRIS). IEEE, 2020.

[5] Ahmad Aziz Arrizal, Ahmad Aziz Arrizal, et al. "Design and Build Entry Access Restriction System Laboratory Using Radio Frequency Identification (RFID) and Keypad Technology." Journal of Energy, Material, and Instrumentation Technology 3.2 (2022): 57-62.