SINERGI Vol. 26, No. 3, October 2022: 379-384
http://publikasi.mercubuana.ac.id/index.php/sinergi
http://doi.org/10.22441/sinergi.2022.3.013

Design and development of smart lock system based QR-Code for library's locker at Faculty of Engineering, Universitas Riau

Yusnita Rahayu[1*], Luthfi Afif[1], Ping Jack Soh[2]
[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Riau, Indonesia
[2]Centre for Wireless Communications – Radio Technologies, University of Oulu, Finland

Abstract
A security system is needed to prevent theft or other criminal acts. One of the implementations of a popular security system today is the Smart Lock System. This study discusses the design of an intelligent lock system using QR Code scanning as a locker key at the Library of the Faculty of Engineering, Universitas Riau. The design of the device system consists of one piece of ESP8266 Node MCU module, one piece of 12V Power Switch Adapter, one piece of AMS 1117 module with 3.3V and 5V output voltages, three pieces of 5V Relays, three pieces of 12V Solenoids. The security system has been improved compared with existing security systems, such as verification for personal data, email notification, and level login to get theft to treat notification. This paper also measured the delay of the device system. Based on measurement results, the average delay obtained is 1.66 seconds.

Keywords:
Library's locker;
QR-code;
Security;
Smart Lock Systems;

Article History:
Received: February 23, 2022
Revised: May 5, 2022
Accepted: May 13, 2022
Published: October 14, 2022

Corresponding Author:
Yusnita Rahayu,
Department of Electrical Engineering, Universitas Riau, Indonesia
Email:
yusnita.rahayu@lecturer.unri.ac.id

INTRODUCTION

The security system is essential to prevent theft or other criminal acts from preventing theft crime rate increases from year to year [1][2]. However, having many keys and maintaining entry to authorized-only persons is a problem. Besides the costs involved in the fabrication, duplication and distribution of keys, there are security concerns in case of lost keys. A keyless entry unit will address these problems and add additional features [3][4].

Smart Lock System usually consists of three parts. First is the key controller as a lock, central controller, or database as a key control center to open, close, or execute crucial commands in the system and mobile application as interface and place of command to unlock the device and register members or guests [3].

Several studies on the Smart Lock System have been carried out. For example, Ha [5] research discusses digital door locks with enhanced security functions designed to work with the Internet of Things. This research uses cameras, keypads, ultrasonic, and motion detection sensors. Each sensor installed serves to validate the user in 2 seconds. For example, the ultrasonic sensor can read and validate the user within 1.6 to 1.8 seconds. Therefore, this device has an average of 1.4 seconds to validate the user, capture the image, and send it to the mobile device. However, this tool has a weakness; when an invalid user enters the wrong password, the user can close the camera with their hands or move their face to take pictures on the camera inaccurately.

Meanwhile, a study by Rasid [6] discussed the design and construction of an automatic door security system using Radio Frequency Identification (RFID) technology. This study uses two RFID tags to distinguish each user, both of which have been programmed beforehand. Both of these tags can work and are recognized by the system so that the door can be opened automatically in less than 4 seconds, while the scanning process can only be done within 5 cm. However, RFID tags require special scanners that either need to be attached to the phone or used independently [7]. In addition, the existing

system that utilizes RFID technology is costly and complex [8].

The two methods and studies above are already quite good regarding security. However, it is ineffective in public spaces where many users use door access. Moreover, the security method using biometric sensors like fingerprints, eyes, voice, and facial recognition has weaknesses, such as requiring high costs to have a scanner with high sensitivity and accuracy. Meanwhile, security methods using RFID, digital pins, or conventional physical keys have drawbacks because there is a risk of losing keys and forgotten passwords. So apart from maintenance costs, there is also the risk of additional costs for fabrication, duplication, and distribution of lost keys.

This research will be used a Quick Response (QR) code as a key to access the lockers. QR-code technology is also a quick and easy way to share authorization data between users and information systems [9]. QR Code has several features such as large-capacity data encoding, dirt and damage resistance, high-speed reading, small print outsize, 360-degree reading, and structural flexibility of application [10]. QR codes can represent text used by a mobile device to act. Code can be generated to link directly to a Uniform Resource Locator (URL), create a Virtual Card (VCard), or initiate a phone call, text or email, and other functions [11]. The QR code structure is too complicated for humans to solve, but the machine can easily read and decode QR codes [12].

Some studies regarding the implementation of QR codes have been discussed by Rao et al. [13], which explains the use of QR codes as car door security. This research was conducted by adding Atmega328P to the Arduino Uno as a microcontroller and the HC-05 Bluetooth module as a wireless communication tool. The system can rotate the servo motor (Micro servo DXW90) about 180 degrees (90 degrees per rotation) which is used to open and lock the car door. The last door lock has been programmed with encrypted data and will later be matched with the lock application; thus, it is challenging to hack while the application design is done using the MIT App inventor [13]. Also, a study by Al-Ghaili et al. [14] researched the use of QR codes for the Smart Verification Algorithm (SVA) on the Internet of Things (IoT). The proposed application carries out verification procedures to activate the user request authorization feature to access the smart system with the help of Encrypted QR tags [15, 16, 17, 18].

The access and services of the library are continuously evolving and changing based on the current technology available in the market. Traditional lockers exist on university campuses but are neither convenient nor secure [19][20].

The current security system in the locker's library of engineering faculty, Universitas Riau, uses a conventional or physical key. A physical key is a standard security system because it is cheap and easy to use. Still, if it is implemented in a public space like a library, physical keys have several weaknesses, such as when visitors bring the key, there is a risk of losing it or being carried home. Furthermore, there is no verification for visitors' data to access lockers. The keys can be duplicated easily, making this current security system vulnerable to theft if applied in public spaces. For this reason, this research is necessary to add some new improvements to the security system to prevent something terrible from happening.

So this research will use the android application provided for users to scan QR codes and create and validate an account to prevent door access by irresponsible parties. This process can only be accessed on the user's mobile device. Then, an additional security login level and an email notification are also added. This research is located in the Faculty of Engineering, Universitas Riau library.

METHODS

Device System Design

The design of the device system is presented in Figure 1. The device requires several main components such as NodeMCU ESP8266 module, solenoid, power switching adapter (PSA) 12V, DC-DC step down (module AMS1117) with outputs of 3.3V and 5V as well as relays of 5V and Solenoid 12V.

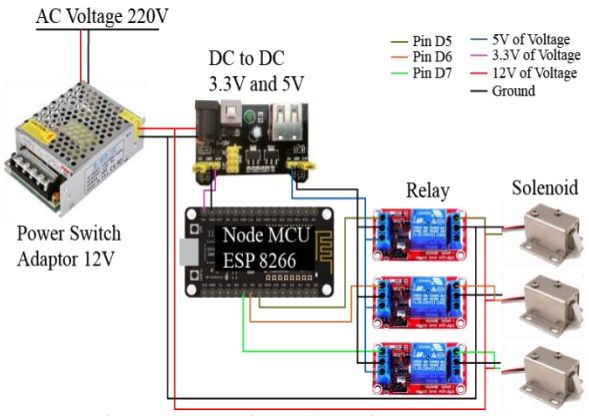

Figure 1. Design of Device System

Power Switching Adapter (PSA) 12V is used as an adapter that converts the AC voltage from the 220V into 12V DC voltage, then DC to DC step down serves to reduce the 12V Voltage to 3.3V & 5V using the AMS1117 module. This 3.3V will be used as a voltage source on the NodeMCU ESP8266 board and 5V as a relay voltage source.

NodeMCU ESP8266 is a microcontroller that will receive command data from the database to control components such as relay and solenoid and connect to a Wi-Fi access point for internet access. A relay will function as a switch and normally has a condition where the current circuit on the relay will be open or disconnected. If it is in a standby state, the electric current cannot flow and will act otherwise if an electric current is applied. Last is the solenoid as a tool to lock the door when the solenoid is given a voltage trigger through the relay. The coil on the solenoid will form a magnetic field around the iron core inside the solenoid so that the iron core will be pulled in and the locker will be open.

Additional Security System

The additional security elements in this research are as follows:

1. Using QR codes
   QR codes are complicated to read by humans and only can be read by computers or smartphones. Meanwhile, to access the locker, scanning QR codes only can be done by the application that has been provided. This can eliminate losing keys because visitors no longer need to carry keys wherever they go.
2. Verification Personal Data
   Visitors cannot access the locker before finishing the personal data verification process. This stage is to ensure that personal user data that was previously filled in on the registration page in the application is correct. This verification can only be done by showing the Student's Identity Card to the library officer.
3. Email Notification
   Email notifications will notify users of several features, such as personal data verification, password change, notification of accessed lockers, and blocking account notifications. In addition, this email will also function as a media report from the library if something unexpected happens in the future.
4. Level Login
   The login level aims to block accounts automatically if any visitor fails to log in by entering the correct data more than three times. It will be indicated as a suspicious action because irresponsible parties are sometimes trying to access lockers with data from other users. Every blocking action will be sent an email notification automatically, so the user must change his password as a security procedure to prevent irresponsible parties from getting access to his account.

Delay Measurement

This Measurement aims to measure the device's effectiveness, and whether there is an increasing delay value on the device. At the same time, the number of lockers that are also accessed simultaneously increases. There are three measurement scenarios to get the delay value of this device such as:

- When one locker is accessed
- When two lockers are accessed
- When three lockers are accessed

The difference is only in the number of accessed lockers because this scenario might happen at peak hours or the level of visitors is high. Measuring delay's value on the device requires additional components, such as push-button connected to pins D1, D2, and D3 on the NodeMCU ESP8266 microcontroller.

These pins would act as input pins to calculate the delay's value on the device when the push button is pressed. Figure 2 illustrates the device circuit to measure the delay's value. Delay measurements start to calculate by pressing the push button when the QR code on the locker is successfully scanned. Then as soon as the solenoid on the locker is open, the push button needs to be pressed again, so the delay's value will be automatically displayed on Arduino serial monitor. It is obtained by subtracting the last-time value when the push button was pressed from the first-time value at the beginning.

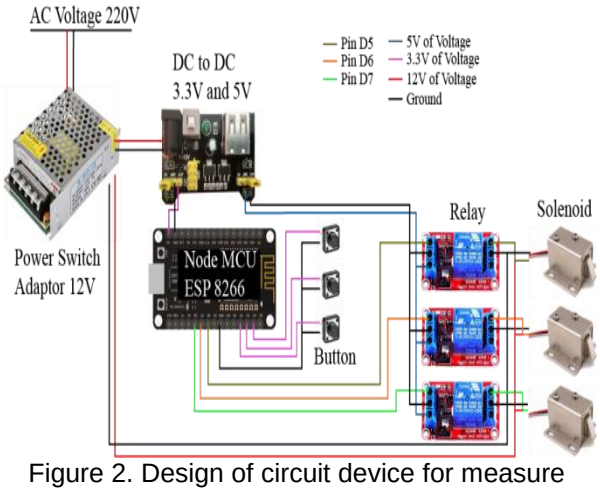

Figure 2. Design of circuit device for measure delay's value

Then all the obtained delay data will be calculated as the average per day and hour based on the library's operational schedule. To calculate the average delay, can use equation (1) below:

$$Average\ Delay = \frac{Total\ Delay}{Total\ Packet\ Recieved} \quad (1)$$

According to the TIPHON standard, several categories for the delay in measuring the qualities are delayed. Table 1 shows delay index quality based on TIPHON [18].

Table 1. Delay Index Quality

Delay Category	Delay (ms)	Index
Very Good	<150	4
Good	150-300	3
Medium	300-450	2
Bad	>450	1

RESULTS AND DISCUSSION

Functional System Testing

The proposed device system has already been tested as a prototype. This device has been working well to be implemented in the library. Each component works according to its function; therefore, a functionality test has been performed in Table 2. Figure 3 shows the prototype's implementation based on the component requirement.

Figure 3. Implementation of Device System

Table 2. Functionalities test on the proposed device system

No	Component	Function	Indicator	Status
1.	NodeMCU ESP 8266	NodeMCU ESP8266 can connect to the existing internet network on the Wi-Fi access point and destination database.	The serial monitor on Arduino software contains information about the IP Address of the Wi-Fi and response data from the user database.	Success
2.	PSA	Converting 220V AC Voltage to 12V DC Voltage	The solenoid automatically opens when this component is connected to a solenoid without a relay.	Success
3.	AMS1117	Lowering the 12V Voltage to 3.3V to be used as a voltage source on the NodeMCU ESP8266	When this component is connected to NodeMCU ESP8266, NodeMCU ESP8266 can work properly.	Success
4.	Relay	The relay usually is open and connected to the NodeMCU ESP8266. Relays can supply and break an electric current.	The solenoid will open on the other side when the relay gets a trigger from the NodeMCU.	Success
5.	Solenoid	A solenoid is connected to the relay and power switching adapter. A solenoid can open and close the locker door.	When the relay conducts an electric current, the solenoid will open; if not, the solenoid will be closed.	Success

Comparison of Security Systems

This proposed security system has already added some improvements using QR codes as a key to unlock the library's locker. However, it is hard for humans to understand and read it. Therefore, the solenoid is placed inside the locker as a component to lock and unlock the door. In addition, verification for personal data and theft threat notification is already added to the application provided by this proposed system. Both of these two systems are compared in Table 3.

Table 3. Comparison of security system

No.	Security Feature	Conventional	Smart Lock System
1.	Risk of losing key	Yes	No
2.	User	Everybody	Only verified user
3.	Verification of personal data	No	Yes
4.	Theft threat notification	No	Yes

Delay Results

Delay testing measurement was done from Monday to Friday (working days). Three lockers are used in the scenario. From measurement

results, the overall average delay value is around 1.66 seconds. The lowest delay occurs on Thursday when two lockers are accessed simultaneously, with a delay of about 0.8 seconds. On Thursday, the highest delay occurs when three lockers are accessed simultaneously with 3.36 seconds delay value. Figure 4 presents the average delay per day.

Meanwhile, suppose the average delay is measured by hours. In that case, the average delay is around 1.66 seconds. The highest average delay value occurs when three lockers are accessed simultaneously, with a delay value of about 3.15 seconds at 02.00 PM. The lowest average delay occurs when two lockers are accessed simultaneously, with a delay value of about 0.86 seconds at 01.00 PM. Figure 5 is shown the average delay per hour.

The average delay is around 1.66 seconds from the two methods above, where the delay value is still categorized as bad by the TIPHON standard. The time value of the delay will also affect the time in reading the QR-code. The higher the delay value, the longer it will take to read the QR-code on the device. Besides, significant issues while measuring delay data are that the quality of Wi-Fi networks at the library is unstable, affecting the measurement results because it is a public network. Moreover, the delay's value is higher during lunch breaks than at other times caused by heavy traffic on Wi-Fi networks.

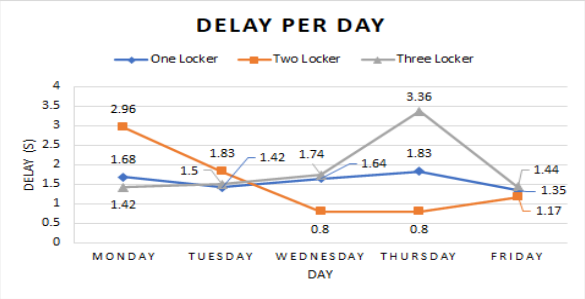

Figure 4. Average delay per day

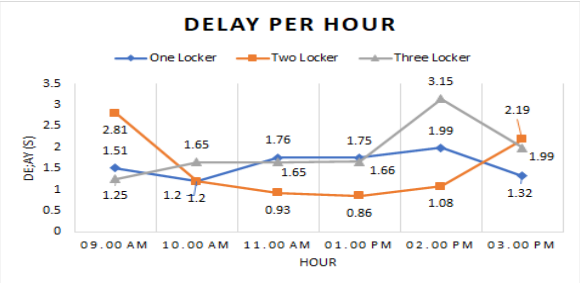

Figure 5. Average delay per hour

The solution to reducing the delay's value is using a private network or a priority network for the devices separated from the public network, so the load on the traffic network can be reduced and obtain the delay's value.

CONCLUSION

The proposed security system has been done and working correctly. On the security side, some improvements, such as using QR codes, verification for personal data, and theft threat notification, have been added successfully. For the delay results, if measured by day, the lowest delay occurs on Thursday at around 0.8 seconds with two lockers are accessed and the highest at around 3.36 seconds when three lockers are accessed. This delay happens on the same day. While delay measured by the hour, the lowest delay is measured at about 0.86 seconds at 01.00 PM with two lockers are accessed, and the highest is 3.15 seconds at 02.00 PM with three lockers are accessed. The delay on the device is still categorized as "Bad," with an average delay time of 1.66 seconds. The condition will affect the time it takes to scan the QR code. The higher the delay time, the longer it will take to read the QR code.

ACKNOWLEDGMENT

This research was supported by the Laboratory of Basic Electrical Engineering and the Library of Engineering Faculty. We hope this finding will be used as a reference to improve the library's locker facility. In addition, we also thank to research institute and community service (LPPM) Universitas Riau for the research motivation and award.

REFERENCES

[1] C. Sisavath and L. Yub, “Design and implementation of security system for smart home based on IOT technology,” *Procedia Computer Science*, vol. 183, pp 4-13, 2021, doi: 10.1016/j.procs.2021.02.023

[2] N. Srikanth and T. Prem Jacob, "An Real Time Cloud Security System and Issues comparison using Machine and Deep Learning," *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2021, pp. 523-529, doi: 10.1109/I-SMAC52330.2021.9640650.

[3] S. Kwon and H. -K. Choi, "Evolution of Wi-Fi Protected Access: Security Challenges," in *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 74-81, 1 Jan. 2021, doi: 10.1109/MCE.2020.3010778.

[4] A. Ramkumar, T. Vaigaiselvam, S.

Rajendran, S. Saravanavel, A. Kamalesh and K. Rajesh, "Android Controlled Smart Home Automation with Security System," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 1245-1249, doi: 10.1109/ICACITE53722.2022.9823575.

[5] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in *IEEE Access*, vol. 8, pp. 88892-88932, 2020, doi: 10.1109/ACCESS.2020.2993553.

[6] S. M. R. Rasid, F. Rashid, A. A. Sabri, and R. Islam, "Design and Construction of an Automatic Security System of a Door Using RFID Technology," *International Journal of Scientific & Engineering Research*, vol. 9, no. 9, pp. 1067–1073, 2018.

[7] A. Gadekar, A. Kandoi, G. Kaushik, and S. Dholay, "QR scan based intelligent system for school bus tracking," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 1074–1080, 2020, doi: 10.1109/ICSSIT48917.2020.9214161.

[8] A. F. M. Fauzi, N. N. Mohamed, H. Hashim, and M. A. Saleh, "Development of Web-Based Smart Security Door Using QR Code System," *2020 IEEE Int. Conf. Autom. Control Intell. Syst. I2CACIS 2020 - Proc.*, no. June, pp. 13–17, 2020, doi: 10.1109/I2CACIS49202.2020.9140200.

[9] V. Susukailo and Y. Lakh, "Access control system based on encryption in QR-Code technology," *Proc. 2018 IEEE 4th Int. Symp. Wirel. Syst. within Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. IDAACS-SWS 2018*, pp. 158–161, 2018, doi: 10.1109/IDAACS-SWS.2018.8525779.

[10] R. Focardi, F. L. Luccio, and H. A.M.Wahsheh, "Usable security for QR code," *Journal of Information Security and Applications*, vol. 48, 2019, doi: 10.1016/j.jisa.2019.102369

[11] A. G. Khan, A. H. Zahid, M. Hussain and U. Riaz, "Security Of Cryptocurrency Using Hardware Wallet And QR Code," 2019 *International Conference on Innovative Computing (ICIC)*, 2019, pp. 1-10, doi: 10.1109/ICIC48496.2019.8966739.

[12] H. A. M. Wahsheh and F. L. Luccio, "Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions," *Information*, vol. 11, no. 4, pp. 217, 2020, doi: 10.3390/info11040217

[13] P. P. Rao, P. Bai, Sneha K, and K. P. Lakshmi, "QR Code for Safety and Security Applications," *IJRET: International Journal of Research in Engineering and Technology.*, vol. 06, no. 06, pp. 15–18, 2017, doi: 10.15623/ijret.2017.0606003.

[14] A. M. Al-Ghaili, H. Kasim, F. A. Rahim, Z. A. Ibrahim, M. Othman, and Z. Hassan, "Smart verification algorithm for IoT applications using QR tag," *Lect. Notes Electr. Eng.*, vol. 481, no. 9, pp. 107–116, 2019, doi: 10.1007/978-981-13-2622-6_11.

[15] J. Suhartono, S. Karya, and S. Candra, "The utilize of NFC technology for campus library services management," *Proc. 2017 Int. Conf. Inf. Manag. Technol. ICIMTech 2017*, vol. 2018-January, no. November, pp. 60–64, 2018, doi: 10.1109/ICIMTech.2017.8273512.

[16] J. W. Tan, H. Hata, T. Muronosono, K. Fukae and T. Kobayashi, "Chameleon: Contactless Operation Application on Campus," *2021 IEEE 11th International Conference on Consumer Electronics (ICCE-Berlin)*, 2021, pp. 1-3, doi: 10.1109/ICCE-Berlin53567.2021.9720025.

[17] Rokhmadi, A. Sofwan and M. Somantri, "Smart School System with Single ID based on RFID Through NFC using FCM Notification," *2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*, 2021, pp. 485-490, doi: 10.1109/IC2IE53219.2021.9649272.

[18] J. Sa-Ngiampak *et al.*, "LockerSwarm: An IoT-based smart locker system with access sharing," *5th IEEE Int. Smart Cities Conf. ISC2 2019*, pp. 587–592, 2019.

[19] R. Muwardi et al., "Network Security Monitoring System Via Notification Alert," *Journal of Integrated and Advanced Engineering (JIAE)*, vol. 1, no. 2, pp. 113-122, 2021, doi: 10.51662/jiae.v1i2.22

[20] Y. A. Pranata, I. Fibriani, and S. B. Utomo, "Analisis optimasi kinerja Quality of Service pada layanan komunikasi data menggunakan NS-2 di PT. PLN (Persero) Jember," *SINERGI*, vol. 20, no. 2, p. 149, 2016, doi: 10.22441/sinergi.2016.2.009.