International Journal of Electrical and Computer Engineering (IJECE)
Vol. 11, No. 4, August 2021, pp. 3267~3274
ISSN: 2088-8708, DOI: 10.11591/ijece.v11i4.pp3267-3274

Residential access control system using QR code and the IoT

Pak Satanasaowapak, Witawat Kawseewai, Suchada Promlee, Anuwat Vilamat
Department of Computer Engineering, Rajabhat Maha Sarakham University, Thailand

Article Info

Article history:

Received Aug 31, 2020
Revised Dec 23, 2020
Accepted Jan 13, 2021

Keywords:

Access control
Authentication
Cryptography
Internet of things
QR code

ABSTRACT

This paper presents a residential access control system (RACs) using QR codes and the internet of things (IoT) to improve security and help house owners. The contribution of this paper is that it proposes two mechanisms in the authentication phase and the verification phase, respectively, to enhance residential access control. The main idea is using cryptography between smartphones and access control devices. The cryptography compares secret codes on the key server via the internet. The RACs can notify a user of the residential access status through the LINE application and show the statuses of devices through the network platform for the internet of everything (NETPIE) in real-time. We compare this system's performance with that of the current access control methods in terms of security and access speed. The results show that this system has more security and has an access speed of 5.63 seconds. Moreover, this system is safer and more flexible than the comparative methods and suitable for contactless authentication.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Pak Satanasaowapak
Department of Computer Engineering
Rajabhat Maha Sarakham University
80 Nakornsawan Road, Talad, Muang District, Maha Sarakham, 44000, Thailand
Email: pak.satanasaowapak@gmail.com

1. INTRODUCTION

Currently, residential safety is considered to be a priority by people. Most people use keys or key cards to access their residences. These things are what they have to carry with them at all times. However, if the keys or key cards are cloned, the residence can be accessed by an intruder. The common problems found in using keys to access residences are having to carry many keys, forgetting keys, losing keys, or even carrying too many items to the point that a person cannot use a key with their hand. Currently, many places do not require a key to access them, including convenience stores, airport entrances, and shopping malls. These doors or gates are designed to facilitate their users, and they are usually installed in public buildings.

Moreover, some doors and gates are used by many users. These include office entrances, dormitory entrances, apartment and condominium entrances. These doors may require identification that does not use a key, such as a key card, a fingerprint scan, or a password. Even though these types of doors do not increase the number of keys for the users, the users still have to carry another object that causes the same problem as carrying a key. The fingerprint scan may be inconvenient if the user has to hold many things. Moreover, if a guest arrives at a residence before the house owners do, the guest has to wait until the owner arrives. This can be time-consuming, and the guest may not want to wait. Therefore, this research aims to solve the problem of using a key to access residences, buildings, or other places so that users will not need to carry additional objects or use biological information for authentication. Hence, users will be able to create keys for those who have been granted access.

Internet of things (IoT) technology has begun to play more roles in people's daily lives, as seen in the popularity of IoT equipment. Besides, smartphones have become indispensable for many people since

they are capable of processing instructions similar to a computer and communicating via wireless networks such as Wi-Fi or Bluetooth. A safe access control system can be created using encryption technology and IoT applied to a smartphone.

We aimed to develop a residential access control system (RACs) using QR codes and the IoT for authentication and develop an Android smartphone application to create an authentication key. The device that controls the door will scan the QR code generated from the Android application. The application has a system that can allow home users to manage the devices that are allowed to access the home. The encryption uses smartphone-specific information authentication. The encryption code can be used only once. Moreover, the RACs can notify the house owners via the LINE application when someone enters or leaves the residence, and the house owners can view the status of the devices through the dashboard. This system is convenient for accessing residences and can reduce the trouble of carrying keys or forgetting keys. It can also increase residential security.

In this paper, we proposed a mechanism to enhance the residential access control system that can improve security and help house owners since they will not have to carry keys or use biometrics for identification. As a result, home users can access their residences conveniently with higher security. Moreover, the system can notify a user of the access status of the residences' members, which will result in a higher quality of life.

The performance test will provide an overview of the system's performance. The access speed of this method will be compared with those of other methods. The rest of the paper is organized as follows. Section 2 provides the related studies on residential access control. In section 3, we propose the methodology of this system. The research results will be provided in section 4. Finally, section 5 concludes this paper.

2. RELATED STUDIES ON RESIDENTIAL ACCESS CONTROL

Internet of Things technology has increased the quality of life for people. The application of this technology mainly emphasizes the monitoring system, which measures the environment using various sensors, displays information through the dashboard, and collects data for further analysis. Applying this technology to residential access systems is, therefore, a huge challenge. The system will increase the convenience for users and reduce the burden of carrying keys or the problem of forgetting keys. Besides, the security and authentication of the access control system are seen as essential in this research, and the results will give more confidence to house owners in using this system.

The security of access to buildings or residences using technology can be guaranteed in various methods. Using a password is the easiest method, but it has the lowest security. Using radio frequency identification (RFID) is convenient for access, but it needs to be carried like a key. Biometrics is another method that has high security, but its limitation is the inability to access the security system remotely. Moreover, sending a password directly to a user by using a wireless network, such as Wi-Fi or Bluetooth, may run the risk of the data being stolen by hackers. Currently, many studies have proposed solutions to these issues, which are as follows:

- Using hardware for authentication: This method involves using a keypad together with sensors and smartphones to form a digital door lock system [1], creating a password from a computer or a smartphone and having a user enter digits using the keypad [2], using a wearable device, such as a smartwatch deploying an android application, for identity verification [3], and using RFID for authentication and access control [4].
- Using biometrics for authentication: This method includes developing equipment to unlock a door by using a fingerprint scanner for authentication [5-6], the development of a facial recognition system for authentication when accessing a building, where the system can send a notification to a smartphone when an intruder tries to enter a building [7-8] or use an image classification technique for a smart door closer system [9], and using an iris biometric to control access [10].
- Using distance for authentication: This system detects the distance between the user and the device to confirm access. For example, the IoT and global positioning system (GPS) technology are used to check the distance of users approaching a smart lock system (SLS) device, which uses special features of Bluetooth to find the distance between the user and the device to lock/unlock the door [11]. Moreover, there are studies on the use of secure Wi-Fi based on the concept of the trusted area as a geofence [12] and the design of a prototype for an IoT and GPS enabled door lock system [13].
- Using a smartphone's feature for authentication: This technique uses the feature of a smartphone, such as visible light communication using the LED flashlight [14], using an Infrared (IR) optical wireless signal (OWS) [15], or a voice call from the global system for mobile communications (GSM) module to verify a valid phone number for the access control of a door and notify the door's status via a short message service (SMS) notification [16].

Furthermore, there are other techniques used, such as developing a device to lock or unlock a door by communicating over a Wi-Fi network using the encryption code for more security [17], using real-time control based on the WCDMA/LTE module for communication with objects that control a lock system in real-time [18], using gait recognition and dress validation for a smart video access control system [19], using efficient image recognition based on a deep neural network applied to home access control systems [20], applying cryptography and steganography for image encoding to access a residence [21], and using a one-time password (OTP) to enhance the security of digital door locks [22].

A QR code is a two-dimensional barcode that can be read by smartphones. The common applications of QR codes are adding people on LINE, adding a contact, and sending a link that can be opened on a smartphone. QR codes make it easy to share information with other people via smartphones. Studies have used the benefits of QR codes to create an access control system, including using a contactless door-locking solution based on QR code technology [23], using an access control system with a single key-lock based on an aesthetic QR [24], and developing a novel combination of QR codes, distributed secret sharing, and attribute-based encryption [25].

The main contribution of this paper is that it proposes a residential access control system using QR codes and the IoT to increase security and facilitate authentication. The residence access control system consists of RACs applications, RACs devices, and key servers. This paper has tested the efficiency of the developed system by measuring the efficiency using the accuracy of the whole system's operations, testing the authentication, comparing the access speed to those of other methods, and testing the security performance.

3. PROPOSED METHOD

In this section, we will propose the residential access control system using QR codes and the IoT for authentication. The process consists of; i) an authentication phase: authentication using the QR codes developed from an Android application and ii) a verification phase: the device verification process. Each process can be described in detail below.

- Authentication phase: This process is activated when the user opens the RACs application and selects a door to access. After the QR code is generated, the RACs application will display the QR code generated from the encryption of the international mobile equipment identity (IMEI), door name, and a random code, which are encrypted with the secure hash algorithm (SHA-2). The QR code is used for authentication on an RACs device, and the encrypted data will be combined with a salt message that is set for each door by using SHA-2 on the key server. The encrypted messages will be collected in a database. The pseudocode of this process is shown in Figure 1.
- Verification phase: This process is started when the user scans the generated QR code on the RACs device. The message will be sent to the key server to be combined with the salt message and encoded with SHA-2. Then, the key server will compare the secret codes for both sides. If the secret codes match, the key server will set the status as "OK". The RACs device will read the status and unlock the door. After 30 seconds, the door will be locked automatically. Furthermore, the RACs device will send a notification to LINE and send the door access information to the network platform for internet of everything (NETPIE) to notify one of the door's status in real-time. Further details of the verification phase and the interaction of RACs are described in Figures 2 and 3, respectively.

Algorithm 1: Algorithm for authentication phase

```
1: begin
2:    users select door_name via RACs application;
3:    users generate QR_Code via RACs application;
4:    m_qr = SHA2(imei, door_name, random_code);
5:    QR_Code = m_qr;
6:    RACs application send m_qr to key server;
7:    m_ref-1 = SHA2(m_qr, salt_ref);
8:    key server encrypts m_ref-1;
9:    key server collects m_ref-1;
10: end
```

Figure 1. Pseudocode of the algorithm for the authentication phase

Algorithm 2: Algorithm for verification phase

```
1: begin
2:    RACs device read QR_Code;
3:    m_device = m_qr;
4:    RACs device send m_device to key server;
5:    m_ref-2 = SHA2(m_device, salt_ref);
6:    key server encrypts m_ref-2;
7:    key server compares m_ref-1 and m_ref-2
8:    if m_ref-1 equal m_ref-2 then
9:        key server set OK status;
10:       RACs device get server status;
11:       if server status equal OK then
12:           RACs device unlock;
13:           wait until 30 seconds then RACs device lock;
14:       end
15:   end
16: end
```

Figure 2. Pseudocode of the algorithm for the verification phase

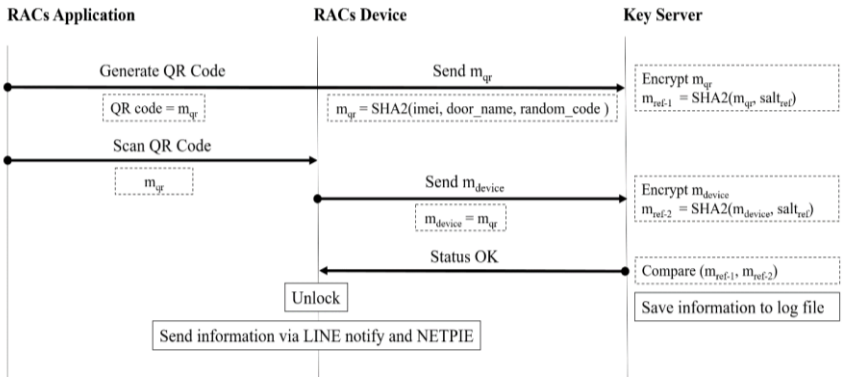


Figure 3. The interaction in the RACs

To test the system's performance, we developed a system with three main components: i) A key server, used for collecting the data of the user and the generated key; ii) An RACs application, used for generating a key for authentication; and iii) An RACs device, used for key verification. Each component is operated as follows:

– The key server: This section consists of a user interface on the website. The user must log in to the RACs, as shown in Figure 4. After logging in, the user must add their personal information and set the name of the doors they wish to access. More details are shown in Figure 5.

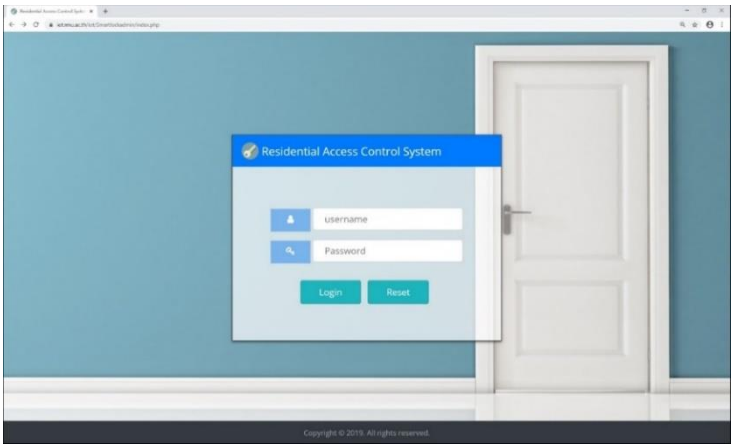


Figure 4. The RACs login page

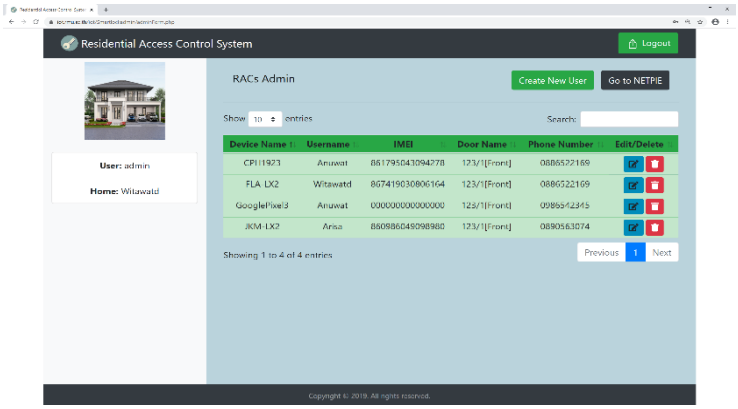


Figure 5. The RACs administrator page

- The RACs application is responsible for generating a key and sending it to the key server. The RACs application will generate the QR code according to the specific information on a smartphone for authentication. The QR code will expire within 5 minutes of being generated. Figure 6 demonstrates the RACs application.
- The RACs device is used to verify the QR code before it allows access to a residence. The RACs device consists of an ESPIno32CAM, an electric solenoid bolt, relays, a push button, an LED, and a power source. The circuit connection in the RACs device section is shown in Figure 7.

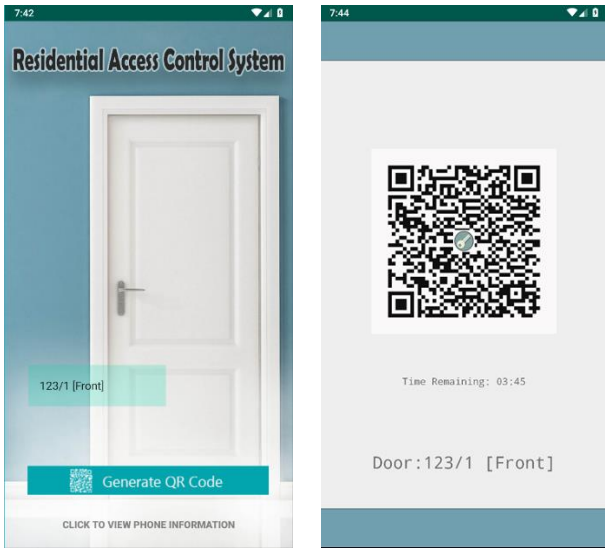


Figure 6. The RACs application on smartphone

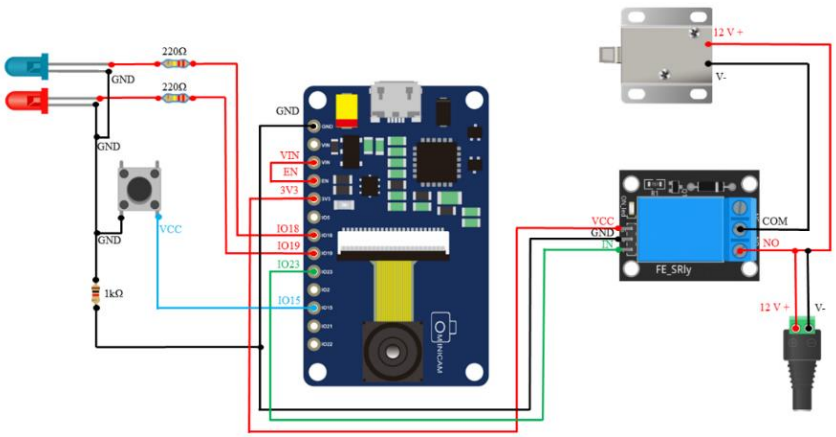


Figure 7. The circuit diagram for the RACs device

4. RESULTS AND ANALYSIS

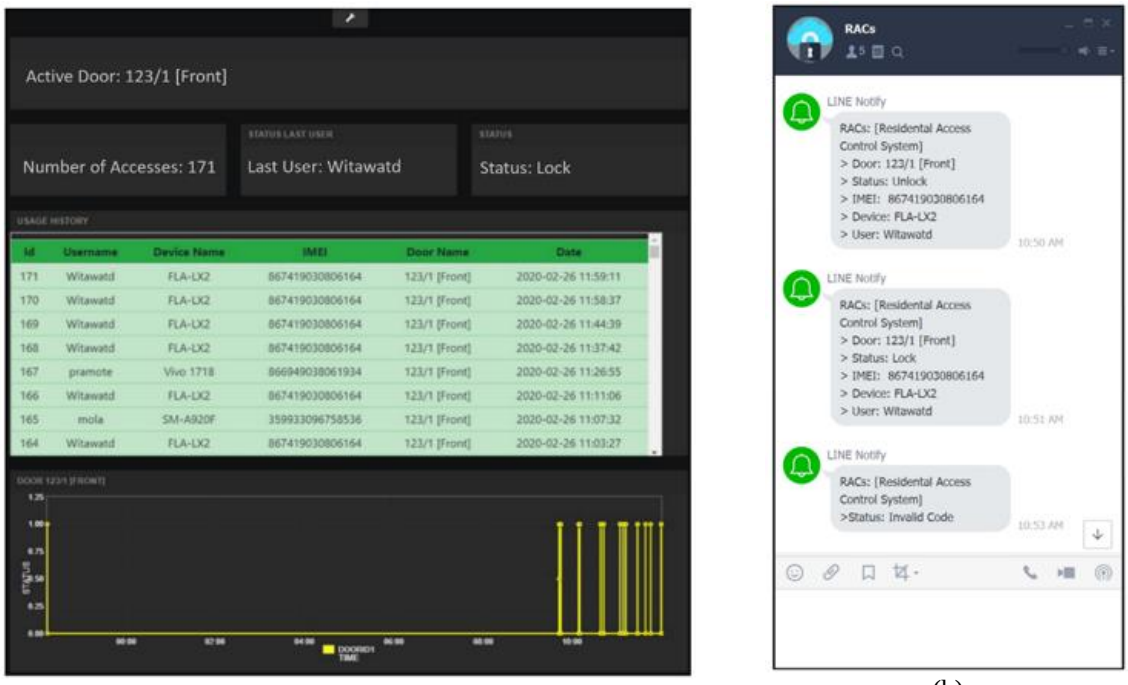
The proposed RACs testing is described in this section. To prove that the RACs is feasible for residential use, we tested the RACs in the computer engineering laboratory at our university. We test the performance in terms of the software and hardware, authentication speed, and security performance. The experimental results are discussed as follows.

4.1. The results from testing the RACs

We tested the developed system in many aspects, including testing a registration system login system; adding, deleting, and editing users' information; and the application's performance on an Android smartphone. Moreover, we also tested the QR code system, the data collection on the key server, the encryption of the QR codes on the RACs device, the notification of residential access via a LINE

notification, and the status of the devices using NETPIE. The results showed that the web RACs administered on the key server could register, login, and manage user information properly. The RACs application could generate QR codes and send the secret codes to the key server correctly. The RACs device could effectively read the QR codes and could compare the information with that on the key server to unlock the door. Moreover, the RACs device could effectively send data via LINE notifications and NETPIE.

NETPIE could display real-time usage information by dividing the display into three sections. The first section showed the general information of a door, such as whether the door was active, number of accesses, last user, and status. The second section shows the usage history information of residential access by displaying the last accessed time. The third section displayed the one-day access data in a chart to allow the house owners to conveniently access information daily. The data on NETPIE are illustrated in Figure 8(a). The data on LINE notifications can be described in Figure 8(b). A notification would display the door's name, the door's status (lock/unlock), the IMEI number, the device name, and the current user. In case the QR code was incorrect or was already used, the RACs device would display an "Invalid Code" message.



(a) (b)

Figure 8. These figures are; (a) NETPIE and (b) LINE notification

4.2. The authentication speed results

Five different residential access methods were tested a total of twenty times each. The residential access methods tested were residential access using a key, access to dormitory door by entering a six-digit password or using a key card, workplace access using a fingerprint, and access to a computer engineering laboratory using an RACs. The results found that the RACs system took an average time of 5.63 seconds (S.D.=0.4479) for authentication starting when the RACs application was opened. Residential access using a key, dormitory access using a six-digit password, dormitory access using a key card, and workplace access using a fingerprint took average times of 5.13 seconds (S.D.=0.9086), 4.78 seconds (S.D.=0.5149), 2.44 seconds (S.D.=0.3975), and 2.98 seconds (S.D.=0.4155), respectively. The RACs system took slightly more time than the other methods. This occurs because the RACs device uses a low-resolution camera device, and the ESP32 has a slow processing speed. Therefore, to reduce the access response time, the system switched to a high-resolution camera module and used a Raspberry Pi instead of the ESP32. The RACs did not require keys or other objects compared to using keys or key cards. Besides, when using the RACs system, users do not need to touch the device, and this system is easier to register in the system compared to systems that use passwords or fingerprints. Moreover, the RACs can also send keys from house owners to other users who are allowed to them to access the house. Therefore, the RACs are safer and more flexible than the comparative methods. The experimental results are shown in Figure 9.

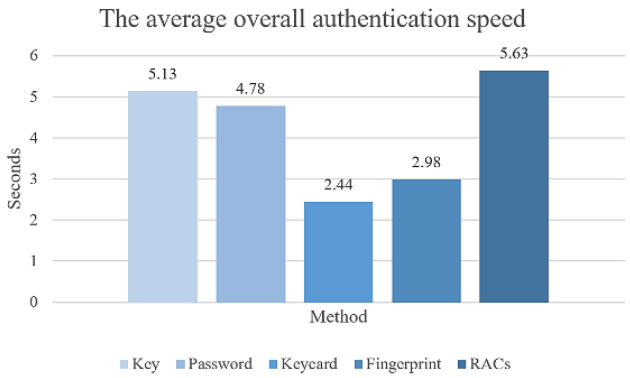


Figure 9. The comparison of the authentication speeds of different methods

4.3. The security performance results

We tested the security of the RACs by creating a fake QR code using the algorithm of this paper. The results showed that the intruder could not use the fake QR code to gain access because when the fake QR code is combined with a salt message on the key server, it will generate an invalid hash and cannot match the RACs device's hash value. Besides, the same QR code could not be used to access the residence because the system would only allow the QR code to be used one time and would randomly generate a new secret code to prevent an intruder from having the correct QR code. Finally, in the worst case in which an intruder could access a residence, the house owners would know this immediately via a LINE notification message or viewing the log via NETPIE. Moreover, to prevent data from being stolen during the data transmission between RACs devices and the key server, the RACs uses transport layer security (TLS) communication.

5. CONCLUSION

This paper proposes a residential access control system that can facilitate users' access to their residence and is flexible and highly secure. The developed residential control system is another option that can be applied to actual applications. We applied the Internet of Things technology and developed the RACs application used for generating a QR code on an Android smartphone to access a residence instead of using a key. The key generation process encrypted specific information by using SHA-2, which required the users to conduct authentication using the RACs device.

The results show that users could conduct effective authentication. Moreover, the house owners could send a QR code to a person who was granted access. The RACs could also prevent the reuse of the QR code, which increase security. It took an average of 5.63 seconds to verify access starting from opening the application to finally unlocking the door. According to the test results, the system worked properly every time, and it could send a real-time message alert via a LINE notification and NETPIE. This notification allows house owners to see the access status and to check past accessibility daily. The RACs system will help reduce the problems of carrying many keys, forgetting keys, or losing keys. Moreover, this system is relatively inexpensive compared to the devices used for access control today. To solve the problem in cases where the power is off or the internet connection is also off, the RACs device requires the use of an electric solenoid bolt with a key fail secure solenoid bot, which allows the lock to be opened when the system fails. Although OTP authentication technology is interesting for residential access control, the OTP requires a little time to enter a password and can be unlocked remotely. However, the RACs does not require a password to authenticate the RACs device. In the future, we will develop more complex cryptography algorithms and implement a high-performance device that will result in faster processing times.

REFERENCES

[1] Ha, "Security and usability improvement on a digital door lock system based on internet of things," *International Journal of Security and Its Applications*, vol. 9, no. 8, pp. 45-54, 2015.

[2] Presso, M., Scafati, D., Marone, J., and Todorovich, E., "Design of a smart lock on the galileo board," *2017 Eight Argentine Symposium and Conference on Embedded Systems (CASE)*, Buenos Aires, 2017, pp. 1-6, doi: 10.23919/SASE-CASE.2017.8115378.

[3] Diez, F. P., Touceda, D. S., Cámara, J. M. S., and Zeadally, S., "Lightweight access control system for wearable devices," *IT Professional*, vol. 21, no. 1, pp. 50-58, 2019, doi: 10.1109/MITP.2018.2876985.

[4] Bakht, K., Din, A. U., Shehzadi, A., and Aftab, M., "Design of an efficient authentication and access control system using RFID," *2019 3rd International Conference on Energy Conservation and Efficiency (ICECE)*, Lahore, Pakistan, 2019, pp. 1-4, doi: 10.1109/ECE.2019.8920871.
[5] Anu, and Bhatia, D., "A smart door access system using finger print biometric system," *International Journal of Medical Engineering and Informatics*, vol. 6, no. 3, pp. 274-280, 2014, doi: 10.1504/IJMEI.2014.063175.
[6] Vargas, M. G., Hoyos, F. E., and Candelo, J. E., "Portable and efficient fingerprint authentication system based on a microcontroller," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 4, pp. 2346-2353, 2019, doi: 10.11591/ijece.v9i4.pp2346-235.
[7] S. Utkarsh *et al.*, "Smart locking system for homes," *International Journal of Control Theory and Applications*, vol. 9, no, 21, pp. 83-86, 2016.
[8] Patel, J., Anand, S., and Luthra, R., "Image-based smart surveillance and remote door lock switching system for homes," *Procedia Computer Science*, vol. 165, pp. 624-630, 2019, doi: 10.1016/j.procs.2020.01.056.
[9] Upadhyay, J., Deb, D., and Rawat, A., "Design of smart door closer system with image classification over WLAN," *Wireless Personal Communications*, vol. 111, pp. 1941-1953, 2020.
[10] Noma-Osaghae, E., Robert, O., Okereke, C., Okesola, O. J., and Okokpujie, K., "Design and implementation of an iris biometric door access control system," *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2017, pp. 590-593, doi: 10.1109/CSCI.2017.102.
[11] Hadis, M. S., Palantei, E., Ilham, A. A., and Hendra, A., "Design of smart lock system for doors with special features using bluetooth technology," *2018 International Conference on Information and Communications Technology (ICOIACT)*, Yogyakarta, Indonesia, 2018, pp. 396-400, doi: 10.1109/ICOIACT.2018.8350767.
[12] J. Haofeng and G. Xiaorui, "Wi-Fi secure access control system based on geo-fence," *2019 IEEE Symposium on Computers and Communications (ISCC)*, Barcelona, Spain, 2019, pp. 1-6.
[13] Adiono, T., Fuada, S., Anindya, S. F., Purwanda, I. G., and Fathany, M. Y., "IoT-enabled door lock system," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 445-449, 2019.
[14] Fan, L., Liu, Q., Jiang, C., Xu, H., Hu, J., Luo, D, *et al.*, "Visible light communication using the flash light LED of the smart phone as a light source and its application in the access control system," *2016 IEEE MTT-S International Wireless Symposium (IWS)*, Shanghai, China, 2016, pp. 1-4, doi: 10.1109/IEEE-IWS.2016.7585481.
[15] Dhondge, K., Ayinala, K., Choi, B. Y., and Song, S., "Infrared optical wireless communication for smart door locks using smartphones," *2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, Hefei, 2016, pp. 251-257, doi: 10.1109/MSN.2016.047.
[16] Raju, N. G., Vikas, J., Appaji, S. V., and Hanuman, A. S., "Smart lock controlled using voice call," *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2018, pp. 97-103, doi: 10.1109/ICSSIT.2018.8748770.
[17] Kassem, A., El Murr, S., Jamous, G., Saad, E., and Geagea, M., "A smart lock system using Wi-Fi security," *2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, Zouk Mosbeh, Lebanon, 2016, pp. 222-225.
[18] J. Jeong, "A study on smart door lock control system," *Cluster Computing*, vol. 19, pp. 1607-1617, 2016.
[19] W. Liu and Z. He, "Smart video access control system with hybrid features in complicated environment," *2016 3rd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)*, Zouk Mosbeh, Lebanon, 2016, pp. 222-225.
[20] S. Lee and C. Yang, "An intelligent home access control system using deep neural network," *2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, Taipei, 2017, pp. 281-282.
[21] Bapat, C., Baleri, G., Inamdar, S., and Nimkar, A. V., "Smart-lock security re-engineered using cryptography and steganography," *5th International Symposium (SSCC)*, Manipal, India, 2017, pp. 325-336.
[22] J. kook, "Design and implementation of a OTP-based IoT digital door-lock system and applications," *International Journal of Engineering Research and Technology*, vol. 12, no, 11, pp. 1841-1846, 2019.
[23] J. Tu, "A contactless door lock which controlled by portable devices," *Engineering Computations*, vol. 33, pp. 1631-1641, 2016.
[24] Huang, P. C., Chang, C. C., Li, Y. H., and Liu, Y., "Efficient access control system based on aesthetic QR code," *Personal and Ubiquitous Computing*, vol. 22, pp. 81-91, 2018.
[25] Belguith, S., Gochhayat, S. P., Conti, M., and Russello, G., "Emergency access control management via attribute based encrypted QR codes," *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China, 2018, pp. 1-8, doi: 10.1109/CNS.2018.8433186.