SAFE AND SECURE ENTRY SYSTEM WITH DYNAMIC QR CODE

[1]**C Sudhakara,** PG scholar, Department of E.C.E, VIKAS COLLEGE OF ENGINEERING AND TECHNOLOGY Email id: Sudhakar.dcp@gmail.com
[2]**B Venkateswara Reddy,** Associate Professor, Department of E.C.E, VIKAS COLLEGE OF ENGINEERING AND TECHNOLOGY Email id: hodece.vikas@gmail.com

Abstract:
When the coronavirus pandemic hit in March 2020, QR codes began popping up everywhere. The early adopters were restaurants and wallet payment applications, cleverly creating QR code menus that were fully accessible by phone, as the virus provoked a shift to health and safety measures that demanded touchless interactions. In recent years, owing to the proliferation of Internet of things, homes and offices square measure being translated into good homes and offices. The proposed system presents an epitome of sensible entry system which may be accustomed enhance the safety and security. Entry systems measure a standard prevalence in our everyday lives. Yet, we tend to still trust ancient doorknobs, that use physical keys that brings with it several issues like key duplication from photos and lock-picking. The focus being security, the system involves the IoT and dynamic QR code technology. QR is one of the most secure way to ensure security as it can generate a new code dynamically for every entry. It will be extremely helpful in tracking the number of individuals trying to access the system securely. The proposed system equipped with camera module to capture the scene of the unauthorized entry attempt and send the picture along with notification message to authorized person. The proposed system includes Raspberry Pi equipped with camera and an android mobile phone. This project aims to make safe and secure entry system as an improved alternative that accepts dynamic QR codes for the entry access system.

Keywords: Raspberry-pi, IoT, Web cam, LCD, Buzzer

1 Introduction

Several popular touchless authentication methods are in use, including palm scans, where users hold their palm about six inches above the reader, and voice recognition and iris scans. According to KBV Research, contactless biometric revenues will grow by about 19 percent annually and reach $18.6 billion by 2026. The firm expects the sales growth will be fueled by faster and easier authentication and interest generated by COVID-19. In March, the New York Police Department stopped using fingerprint biometrics to authenticate access to its headquarters, and governments, including India, also heavily restricted the use of touch biometrics. This summer, Pasadena, California-based PopID, a provider of facial recognition payments, was deployed at about 25 retailers and quick-serve restaurants, including CaliBurger. The system works at kiosks and display screens at checkout and enables scans by wait staff using Android mobile devices. The company also offers a similar service for building access. Of course, there are barriers to the adoption of touchless biometrics. Many of those barriers are similar to the obstacles to adopting touch biometrics: cost, accuracy, standards, and privacy concerns. The National Institute of Standards and Technology has studied contactless fingerprint biometric technologies for several years now. This spring, NIST released an interoperability assessment that evaluated the accuracy of contactless and its interoperability with traditional touch fingerprint scans. The study found contactless fingerprint biometrics are less accurate than traditional fingerprint biometrics, which can be attributed to the way prints are captured. When a finger is pressed on a conventional reader, it creates a two-dimensional print of the finger's unique features. However, with contactless, the finger is lit and the 3D surface is captured, resulting in more deviation than with the user physically touching the biometric scanner. While traditional fingerprint biometrics scanners are not 100 percent accurate, they can be more than 99.5 percent accurate. However, in NIST's evaluation, while contactless biometric devices were only 60 to 70 percent accurate, accuracy rose to between 90 and 95 percent when devices used multiple fingers. Another barrier is a lack of industry standards making 3D biometrics compatible with existing 2D databases Still, the industry is moving ahead with contactless biometrics, especially in payments. And major companies are moving fast. Amazon announced in late September that it's enabling customers who pay in-store to use its Amazon One contactless palm scanner system. The company is deploying the system at two Amazon Go stores in Seattle to start. As a choice for shoppers, Amazon will place Amazon One at entrances, and it could become a form of payment or check-in for loyalty cards. Amazon also sees eventually deploying Amazon One at stadiums and office buildings. "Amazon One could be part of an existing entry point to make accessing the location quicker and easier," the company said in a blog post. Amazon One follows a similar move from Walmart, which earlier this year announced contactless Walmart Pay. With Walmart Pay, shoppers don't have to use a credit card or touch a screen. Instead, they can scan a QR code at the kiosk with their phone and pay within Walmart's phone app. "The way we're all living and shopping is changing. We know customers want and need to be served differently. And we're moving quickly to adapt to those changing needs. It's one way we can help to add some stability to our customers' lives," said Janey Whiteside, executive vice president and Walmart chief customer officer, in a statement. Another example of touchless is biometric credit cards. These cards, currently being piloted, look just like chip cards except they come equipped with fingerprint readers. Card carriers can place their finger on the card and then put it in the chip reader or place it on the reader for contactless payment. The primary benefit is the elimination of PIN codes.

2 Literature Survey

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 sign al (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 CDMA/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 openedon 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 objective of this project is that it proposes a safe and secure access control system using Dynamic QR codes and the IoT to increase security and facilitate authentication. The access control system consists of applications, devices, offices/industries and key servers.

3 Proposed System

In this section, we will propose the safe and secure access control system using dynamic QR codes and the IoT for authentication. The process consists of two phases;

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 Android application it generate QR code dynamically. After the QR code is generated, the application will display the QR code generated from the user name, and a random code. And the code sent to the IoT Server, which forward to the access control device.

The QR code is used for authentication on Access control device.

–Verification phase:

This process is started when the user scans the generated QR code on the access control device. The message will be compare the secret codes received from IoT Server. If the secret codes match, the device will read the status and unlock the door. After 10 seconds, the door will be locked automatically. Furthermore, the access control device will send a notification along with captured image to authorized email 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.

The block diagram of the proposed system is as shown in fig.3.

3.1 BLOCKDIAGRAM:

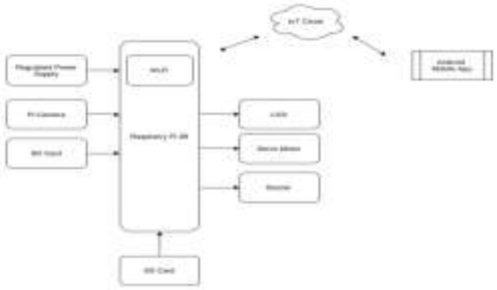


Fig 1 Block diagram

4 Proposed System Working:

The proposed system consists of Raspberry Pi as main processing unit along with Camera module, Liquid crystal display, buzzer, SD card along with Regulated 5v power supply unit. The working steps of this system as follows.

i. First User needs to open the access control app in their android phone with their fingerprint authentication.

ii. The android application generates a new QR code dynamically and send its information to open IoT platform Thing Speak.

iii. The access control device get the QR code information from Thing Speak cloud and stores in temporary variable which has the validity of 20 Seconds.

iv. The user needs to show the generated QR code to camera module, which read the QR image and fed to raspberry pi which decodes the QR information.

v. The decoded information is compared with temporary variable information received from IoT cloud.

vi. If both the information's are matches the raspberry pi allow the user by rotating servo motor.

vii. If mismatch found the system deny the user, activate the buzzer alert for one second, capture the image, and send to authorized email account.

Flowchart

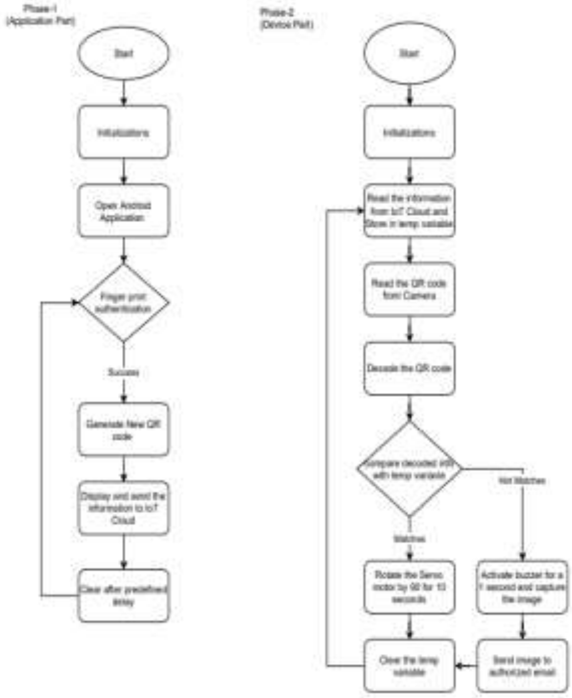

Phase-I
(Application Part)
Start
Initializations
Open Android Application
Finger print authentication
Success
Generate New QR code
Display and send the information to IoT Cloud
Clear after predefined delay
Phase-2
(Device Part)
Start
Initializations
Read the information from IoT Cloud and Store in temp variable
Read the QR code from Camera
Decode the QR code
Compare decoded info with temp variable
Not Matches
Matches
Rotate the Servo motor by 90 for 10 seconds
Activate buzzer for a 1 second and capture the image
Clear the temp variable
Send image to authorized email

Fig 2: Flow Chart

5 Hardware Requirements:

LCD

The features of this LCD mainly include the following.

- The operating voltage of this LCD is 4.7V-5.3V
- It includes two rows where each row can produce 16-characters.
- The utilization of current is 1mA with no backlight
- Every character can be built with a 5×8 pixel box
- The alphanumeric LCDs alphabets & numbers
- Is display can work on two modes like 4-bit & 8-bit
- These are obtainable in Blue & Green Backlight

It displays a few custom generated characters

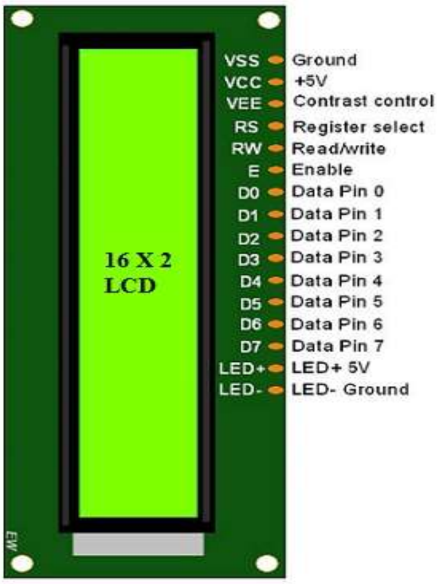


Fig 2 LCD Display

Raspberry-pi

The Raspberry Pi is a progression of little single-board PCs created in the United Kingdom by the Raspberry Pi Foundation to advance the instructing of essential software engineering in schools and in creating nations. The first model wound up much more prominent than foreseen, offering outside its objective market for utilizations, for example, mechanical technology. It does exclude peripherals, (for example, consoles, mice and cases). Be that as it may, a few frills have been incorporated into a few official and informal packs. As indicated by the Raspberry Pi Foundation, more than 5 million Raspberry-Pi were sold by February 2015, making it the top of the line British PC. By November 2016 they had sold 11 million units, and 12.5m by March 2017, making it the third top rated "broadly useful PC". In July 2017, deals came to almost 15 million. In March 2018, deals achieved 19 million. Raspberry Pi 3 Model B was discharged in February 2016 with a 64 bit quad center processor, and has on-load up Wi-Fi, Bluetooth and USB boot capabilities[18]. On Pi Day 2018 model 3B+ showed up with a quicker 1.4 GHz processor and a 3 times speedier system in view of gigabit Ethernet (300 Mbit/s) or 2.4/5 GHz double band Wi-Fi (100 Mbit/s)[1]. Other choices are: Power over Ethernet (POE), USB boot and system boot (a SD card is never again required). This permits the utilization of the Pi in difficult to-achieve places (perhaps without power).

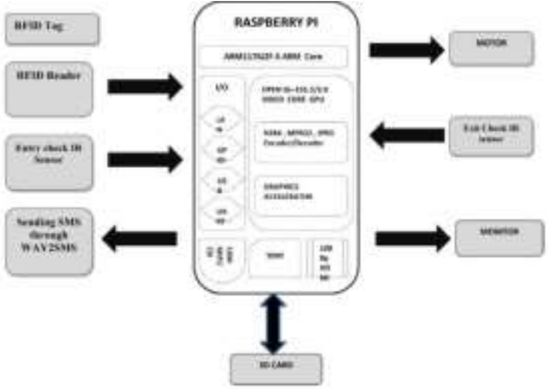


Fig 3: Raspberry Pi 3 Based Diagram

Pi Camera Module

The **Pi camera module** is a portable light weight camera that supports Raspberry Pi. It communicates with Pi using the MIPI camera serial interface protocol. It is normally used in image processing, machine learning or in surveillance projects. It is commonly used in surveillance drones since the payload of camera is very less. Apart from these modules Pi can also use normal USB webcams that are used along with computer.

Pin Description

Pin Number	Pin Name	Description
1	Ground	System Ground
2,3	CAM1_DN0, CAM1_DP0	MIPI Data Positive and MIPI Data Negative for data lane 0
4	Ground	System Ground
5,6	CAM1_DN1, CAM1_DP1	MIPI Data Positive and MIPI Data Negative for data lane 1
7	Ground	System Ground
8,9	CAM1_CN, CAM1_CP	These pins provide the clock pulses for MIPI data lanes
10	Ground	System Ground
11	CAM_GPIO	GPIO pin used optionally
12	CAM_CLK	Optional clock pin
13,14	SCL0, SDA0	Used for I2C communication
15	+3.3V	Power pin

PiCam Features

- 5MP colour camera module without microphone for Raspberry Pi
- Supports both Raspberry Pi Model A and Model B
- MIPI Camera serial interface
- Omnivision 5647 Camera Module
- Resolution: 2592 * 1944
- Supports: 1080p, 720p and 480p
- Light weight and portable (3g only)

The proposed system was fully developed and tested to demonstrate its feasibility and effectiveness. The screenshots of the proposed safe and secure access control using dynamic QR code system developed has been presented in Figures bellow.

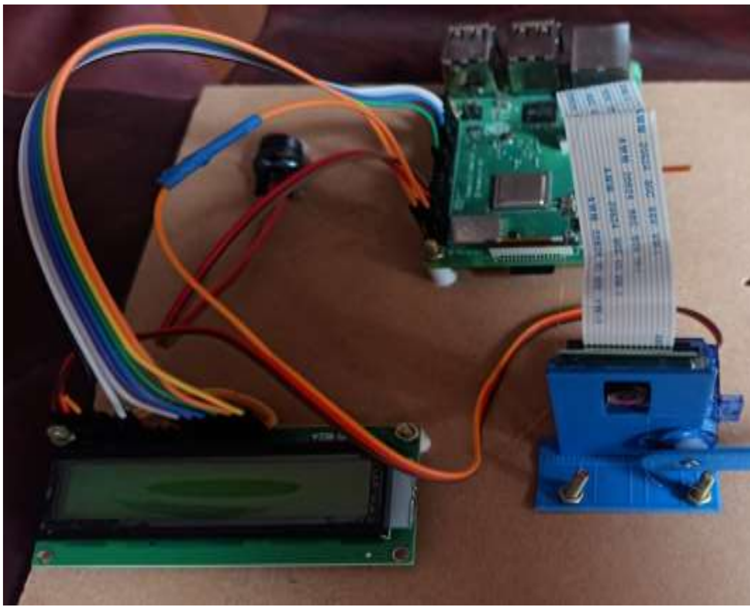


Fig4 Hardware setup of proposed system

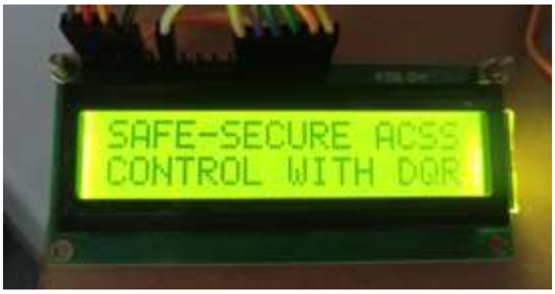


Fig 5 Initial message on LCD

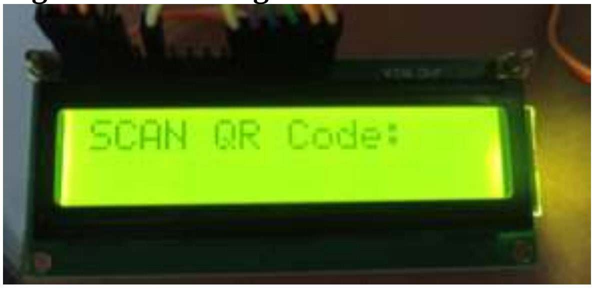
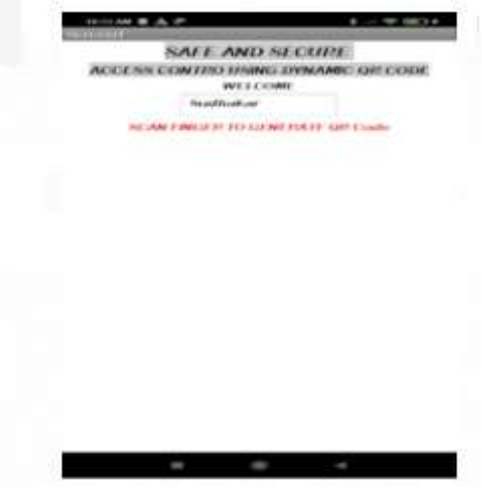
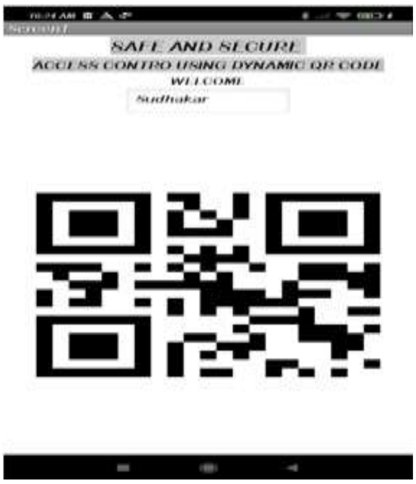


Fig 6 Request message on LCD



SAFE AND SECURE
ACCESS CONTRO USING DYNAMIC QR CODE
WELCOME
Sudhakar
SCAN FINGER TO GENERATE QR Code

Fig 6.2 (a)Initial mobile App screenshot



SAFE AND SECURE
ACCESS CONTRO USING DYNAMIC QR CODE
WELCOME
Sudhakar

Fig 7 QR code generated on mobile APP

Fig 8 Scanning QR code in Device

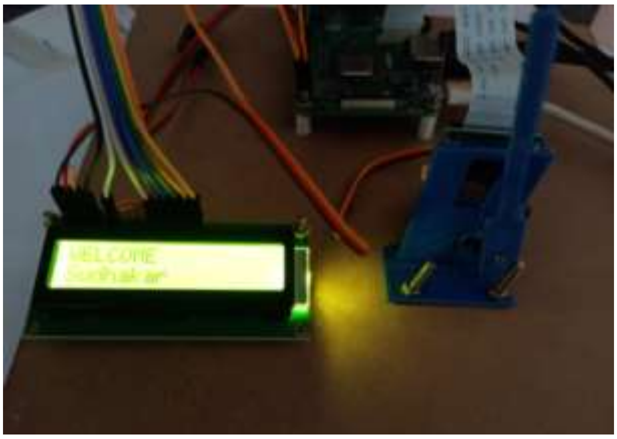


Fig 9 Welcome message to authorized person and opening the door gate

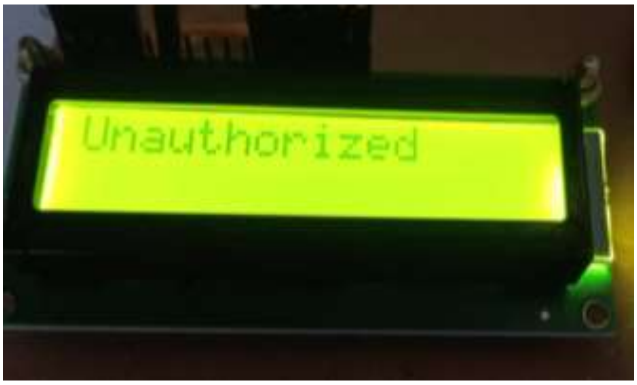


Fig 10 Message to unauthorized

Fig 11 E-mail Screenshot for unauthorized

Conclusion

This project proposes a safe and secure access control system that can facilitate users' access to their entry safely, flexible and highly secure. The developed access control system is another option that can be applied to actual applications. We applied the Internet of Things technology and developed the Access control application used for generating a QR code dynamically on an Android smartphone to access the device instead of using a physical key. which required the users to conduct authentication using the device. The results show that users could conduct effective authentication. The device could also prevent the reuse of the QR code, which increase security. It took an average of 6 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 IoT notification and image. This notification allows authorized admin to see the access status and to check past accessibility daily.The 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. However, the device does not require a password to authenticate. In the future, we will develop more complex cryptography algorithms and implement a high-performance device that will result in faster processing times.

REFFERENCES

[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: 0.1016/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 national 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.