ABUAD Journal of Engineering Research and Development (AJERD)
ISSN (online): 2645-2685; ISSN (print): 2756-6811

Volume 7, Issue 2, 484-492

Development of a Smart Lock System using QR Code Technology

Mary ADEDOYIN, Farouq OLUKOYA

Department of Electronic and Computer Engineering, Lagos State University, Nigeria
mary.adedoyin@lasu.edu.ng/farouqolukoya2002@gmail.com

Corresponding Author: mary.adedoyin@lasu.edu.ng, +2348020586312
Date Submitted: 21/03/2024
Date Accepted: 08/10/2024
Date Published: 11/11/2024

Abstract: *A smart lock system refers to a modern security solution that enables users to remotely control access to their homes or businesses using a smart device such as smartphone, tablet, or computer. This paper presents the development of a smart lock system using Quick Response (QR) code technology to address the problem of insecurity, inconvenience, and inflexibility in access control. The proposed system eliminates the need for physical keys or complex authentication and verification methods. The system integrates an ESP8266 microcontroller, barcode scanner, 16x2 liquid-crystal display (LCD), solenoid lock, relay, and a 12V power supply. The system allows authorised users to generate unique QR codes representing their access credentials through a user-friendly interface. These QR codes are scanned by the system, which processes the codes, verifies access permissions via a central server and provides real-time feedback through the LCD. Upon successful verification, the system triggers a relay to control the solenoid lock, to grant or deny access. The implementation and testing of the smart lock system demonstrated successful operation. The performance indices include authentication speed, system reliability, accuracy and response time, which were evaluated and found to be satisfactory. The obtained results showed that the proposed system outperformed traditional methods such as keys, and fingerprint authentication, with an access speed of 2.00 seconds, which is significantly faster than the alternatives. Comparative analysis with existing access control techniques demonstrated the developed system's enhanced security features and user-friendly operation, making it applicable for residential, commercial, and industrial use. Additionally, the system's scalability and adaptability allow it to be customised for various environments, offering a versatile solution to diverse security challenges. This work contributes to the field of security technology by providing an efficient and scalable smart lock system with novel algorithms, which enhances the convenience, robustness of access control and seamless user experience.*

Keywords: *Smart Lock System, Access Control, QR Code, ESP8266, Security Systems*

1. INTRODUCTION

The rapid advancement in smart technologies has spurred the development of innovative security solutions, among which smart lock systems have gained significant attention. These systems enable users to control access to their homes or businesses remotely, typically via smartphones, tablets, or computers. However, despite the benefits of existing smart locks, traditional access control methods such as physical keys, passwords, key cards, and biometric authentication face several limitations. Issues of security vulnerabilities, lack of flexibility, and inconvenient authentication methods continue to present challenges for users in residential, commercial, and industrial settings [1-3]. The primary problem to be addressed in this work is the inadequacy of current access control systems in providing both robust security and seamless user experience. Existing methods like fingerprint recognition and RFID technology offer a degree of automation, but they come with drawbacks such as complex setup processes, high costs, and potential privacy concerns. Furthermore, physical keys and passwords, which are still widely used, are prone to loss, duplication, and theft, thus compromising security [4].

In recent years, the integration of Quick Response (QR) code technology in security systems has emerged as a promising solution. QR codes offer a highly flexible and scalable method for secure information transfer, making them an ideal candidate for modern access control systems. The widely used QR code, a barcode standard created by Japanese company Denso Wave in the 1990s, forms the foundation of the scan access door security system. A QR code is a two-dimensional (2D) barcode that can be read by smart devices. The common applications of QR codes are adding people on LINE, adding a contact, and sending a link that can be opened on a smart device. QR codes make it easy to share information with other people. Since QR codes are 2D, more information may be stored in them than with conventional 1-dimensional (1D) barcodes. It holds information in both the vertical and horizontal directions. The primary source of the security hazard is mechanical door lock keys. Hence, security technologies that use QR scanners have been introduced to address the issue. Furthermore, the current system that uses radio frequency identification (RFID) technology is expensive and complicated. Consequently, the cost-effective approach is the QR technology, which is simple to use and significantly less expensive than RFID [6, 7]. Existing research has demonstrated that QR code-based security systems can enhance both the security and convenience of access management, but there remains room for improvement in terms of speed, reliability, and adaptability to different environments.

Access door security systems are essential for protecting physical areas. However, the existing authentication techniques, like keys, cards or PINs are frequently used in conventional access control systems, which present difficulties like the possibility of unlawful entry due to misplaced keys, cards or forgotten codes, susceptibility to unwanted access attempts and processing delays. Hence, access door security systems with QR code integration offer a chance to address these problems and offer more efficient, cost-effective and safer alternatives. Securing the keyless door system is essential to stop burglars from entering critical areas unnoticed [8]. Users only need to display their QR codes to the assigned scanner to gain access. To confirm the user's identity and authorisation, the system instantaneously examines the data and cross-references it with the database. Easy access is provided by the door unlocking if the QR code is legitimate. This quick and easy procedure reduces wait times and raises users' satisfaction levels overall.

The aim of this paper is to develop a smart lock system using QR code technology, to address the shortcomings of existing methods. This is necessary for enhanced security, efficient access control, convenience and user-friendly operation. The proposed system eliminates the need for physical keys or complex authentication processes by allowing users to generate unique QR codes as access credentials. These QR codes are scanned, processed, and verified using an integrated system comprising an ESP8266 microcontroller, barcode scanner, 16x2 liquid-crystal display (LCD), solenoid lock, relay, and a 12V power supply. The system provides real-time feedback and ensures that only authorised individuals can gain entry.

This paper is structured as follows: Section II reviews the current literature on smart lock systems and QR code-based security solutions. Section III details the design and implementation of the proposed system. Section IV presents the experimental results and performance evaluation, followed by a discussion in Section V. Finally, Section VI concludes the paper and outlines future research directions.

2. LITERATURE REVIEW

Several studies have explored different technologies for access control, such as RFID, biometric authentication, and Bluetooth-based systems. RFID technology has been widely adopted due to its ability to enable contactless access control. For instance, the authors in [9] demonstrated an RFID-based smart lock system with real-time monitoring capabilities. This approach enhances convenience; however, its major limitation lies in the vulnerability to cloning and unauthorised access due to weak encryption protocols. Similarly, biometric-based systems, including fingerprint and facial recognition technologies, have gained popularity due to their high level of security. In [10], a voice-based door access control security system was developed. The work outlined the various ways that identity cards, cryptography, PIN pads, traditional and electronic keys, and dual control processes can be used to prevent illegal access to secure facilities. In the proposed system, access could be granted just by having a registered user talk into a microphone that was connected to the system. After that, the system will determine whether to approve or deny the user, or it may indicate a lack of confidence and ask for more information before making a choice. Furthermore, verified person models based on voice were developed using the intelligent system technique. The system used fuzzy inference systems to distinguish between authorised and illegitimate users. The experimental results validated the efficacy of the proposed intelligent voice-based door access control system. However, this solution is expensive and the installation is cumbersome. The authors in [11] designed and implemented a facial recognition access control system by combining an RFID system with a face recognition system. A modem sends a reply to a distant station if the PIN on the RFID card matches the identified face to increase security's robustness and dependability. The authors in [12] developed a biometric access control system using fingerprint recognition, showing high accuracy in user authentication. However, biometric systems face challenges in terms of cost, complexity, and user privacy concerns, which limit their widespread adoption. Bluetooth-based smart locks have also been explored as a means of improving access control. A Bluetooth Low Energy (BLE) system has been proposed in [13] which allows users to unlock doors using their smartphones. This method provides convenience, but its limitations include susceptibility to signal interference, security risks posed by unsecured Bluetooth connections, and the need for continuous power to maintain connectivity. These limitations highlight the need for an alternative approach that can balance security, convenience, and cost-effectiveness. In response to the limitations of existing access control methods, QR code technology has emerged as a promising solution for secure and scalable access control. QR codes can store encrypted access credentials that can be easily scanned and verified. Recent studies have demonstrated the potential of QR codes in various security applications. For example, the authors in [14] implemented a QR code-based payment system, showing that QR codes provide a cost-effective and user-friendly alternative to traditional payment methods. The use of QR codes in access control systems offers similar advantages, including ease of implementation, flexibility, and the ability to integrate with cloud-based platforms for real-time monitoring and authentication. However, while the integration of QR codes into access control systems has shown promise, several limitations remain. One of the key challenges is ensuring the secure generation, transmission, and verification of QR codes to prevent unauthorized access. The authors in [15] addressed this issue by developing a secure QR code system that uses encryption algorithms to protect the data stored within the code. Despite these advancements, QR code-based systems are still prone to attacks such as QR code spoofing and unauthorised code duplication, highlighting the need for further research into more secure algorithms and verification methods. The proposed smart lock system in this work addresses the aforementioned gaps by incorporating a novel algorithm for secure and efficient QR code processing. The system integrates an ESP8266 microcontroller, a barcode scanner, an LCD, and a solenoid lock to enhance access control security while maintaining ease of use. The key contribution of this work is the development of novel algorithms that enhance the authentication speed, system reliability, accuracy and response time, significantly faster than traditional methods, the integration of low-cost hardware components, and the provision of a scalable and user-friendly solution for diverse access control needs. Moreover, the proposed system demonstrates superior performance in terms of security and user convenience when compared to other existing solutions like keycards and fingerprint scanners. This work advances the state of knowledge in smart lock technology and offers a scalable, efficient, and user-friendly solution to access control.

3. METHODOLOGY

This section outlines the systematic approach taken to design, develop, and implement the smart lock system using the QR code technology. It includes the description of system architecture and schematic diagram as presented in Figure 1 and 2 respectively, system flowchart as shown in Figure 3, and process of hardware integration, software development, and testing phases that ensure the smart lock functions as intended.

3.1 Mathematical Framework

The mathematical models to describe the core operations of the system include QR code generation, encryption, access verification, and response time calculations.

1. **QR Code Generation:** QR codes encode access credentials in a matrix of black and white squares. The QR code generation process is given as [16]:

$$Q(x, y) = f(d_1, d_2, \dots . d_n) \tag{1}$$

where:

$Q(x, y)$ represents the QR code matrix with dimensions $x \times y$,

$f(d_1, d_2, \dots . d_n)$ is the encoding function that generates the QR code based on user data d_1, d_2,..., d_n, where d_n represents the access credentials or encrypted information.

This function maps the binary data to a matrix of QR code cells, each either black or white, depending on the data pattern.

2. **Encryption Algorithm:** Access credentials encoded in the QR code are encrypted, to ensure secure communication. The encryption is represented by:

$$E_k(M) = C \tag{2}$$

where:

M is the plaintext (QR code data),

$E_k(M)$ is the encryption function with the key k,

C is the resulting ciphertext (encrypted QR code data).

Decryption on the server side is represented as:

$$D_k(C) = M \tag{3}$$

where $D_k(C)$ is the decryption function that, when applied to the ciphertext C using the same key k, retrieves the original QR code data M.

3. **Access Verification:** Once the QR code is scanned, the system checks the access credentials against the database. This is modelled as a binary classification problem:

$$V(A, B) = \begin{cases} 1 \; if \; A = B \\ 0 \; if \; A \neq B \end{cases} \tag{4}$$

where:

A is the decrypted QR code data from the scanned QR code,

B is the stored access data in the system,

$V(A, B)$ is the verification function, returning 1 for a match (grant access) and 0 for no match (deny access).

4. **Response Time Calculation:** The system's response time, $\mathrm{T_{total}}$, is the time taken from QR code scanning to access being granted or denied. This includes the time for QR code scanning T_{scan}, decryption T_{dec}, verification T_{ver}, and triggering the solenoid lock T_{lock}.

$$T_{total} = T_{scan} + T_{dec} + T_{ver} + T_{lock} \tag{5}$$

where each component can be estimated based on system performance, and the total response time, T_{total} should ideally meet user expectations for quick access, as shown by the average access time of 2.00 seconds in this system.

5. **System Reliability and Accuracy:** The reliability of the system can be calculated using the reliability function $R(t)$, which measures the probability that the system will function without failure over a time period t:

$$R(t) = e^{-\lambda t} \tag{6}$$

where:
λ is the failure rate,
t is the operating time.
Similarly, system accuracy in authentication is typically defined using the accuracy rate, Acc, given as:

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (7)$$

where:
TP is the number of true positives (correctly authenticated),
TN is the number of true negatives (correctly denied),
FP is the number of false positives (incorrectly granted access),
FN is the number of false negatives (incorrectly denied access).
A high accuracy rate ensures that the system minimises both unauthorised access and denial of valid access.

6. **Energy Consumption:** Given that the system is powered by a 12V power supply, the energy consumption, E for a time duration t can be calculated as:

$$E = P \times t \quad (8)$$

where:
P is the power consumption of the system, which can be derived from the current III and voltage V using $P = IV$,
t is the operational time.

3.2 Architecture of Smart Lock System

The architecture of a smart lock system using QR code technology is shown in Figure 1, which can be broken down into the several key components that work together to ensure secure access control.

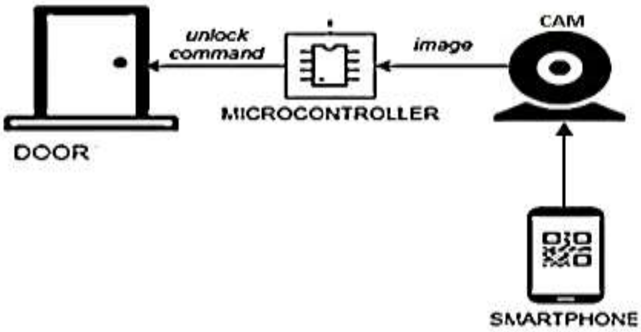


Figure 1: Architecture of smart lock system architecture.

The hardware components used in the system include a 16x2 LCD, ESP8266 microcontroller, solenoid lock, relay, barcode scanner, power supply, and plastic casing. The architecture of these hardware components consists of interconnected modules working together to achieve secure access control. The description of the roles and how each component functions within the system is summarised in Table I. Figure 2 shows the schematic diagram of the smart lock system.

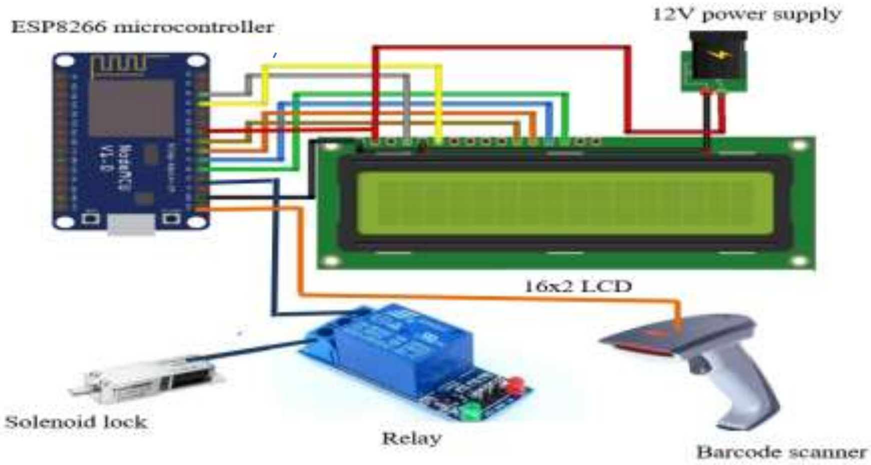


Figure 2: The schematic diagram of the smart lock system.

Table 1: Roles and functionalities of hardware components used in the development of the smart lock system

Hardware Components	Roles	Functionalities
ESP8266 Microcontroller [17]	The ESP8266 is a Wi-Fi-enabled microcontroller that acts as the brain of the smart lock system. It is responsible for controlling other components, connecting to Wi-Fi networks, and handling communications between the system and an external server.	The ESP8266 enables the smart lock system to establish TCP/IP connections, allowing real-time interactions with the server for QR code authentication and access control. It also sends and receives data from the database for component control and communication with the relay and solenoid lock.
16x2 LCD [18]	The 16x2 LCD serves as a user interface for the system, providing real-time feedback and status updates, such as “Access Granted” or “Access Denied.”	16x2 LCD is connected to the ESP8266, receiving data from the microcontroller to display information during the QR code scanning and authentication process.
Barcode/QR Code Scanner [19]	The barcode/QR code scanner acts as the input device for the system, capturing the QR code displayed on the user’s mobile device.	Once a QR code is scanned, the scanner transmits the encoded user information to the ESP8266. The microcontroller forwards this data to the server for verification against stored credentials.
Relay [20]	The relay serves as an electronic switch, controlling the solenoid lock based on commands received from the ESP8266.	The relay prevents current flow until it receives a signal from the ESP8266. When access is granted, the relay closes the circuit, allowing current to flow to the solenoid lock. The 5V power required to operate the relay is provided by the power supply through the AMS1117 module.
Solenoid Lock [20]	The solenoid lock is the physical locking mechanism of the system, responsible for securing or unlocking the door.	The solenoid receives a voltage pulse, causing its coil to generate a magnetic field when the relay is triggered. This magnetic field pulls the iron core inside the solenoid, unlocking the door. The solenoid remains in the locked position when no current is applied.
Power Supply [8]	The power supply is responsible for converting the high-voltage input (220V AC) into the required lower voltages to operate the system.	A 12V power switching adapter is used to step down the voltage from 220V AC to 12V DC. The DC-to-DC step-down converter (AMS1117 module) further reduces the 12V DC to 3.3V and 5V. The 3.3V powers the ESP8266, while the 5V is used to power the relay.
Plastic Casing	The plastic casing provides protection and structural housing for all the components.	The plastic casing ensures that the internal electronics are safe from dust, moisture, and physical damage, while also offering an aesthetic and compact design for easy installation and use.

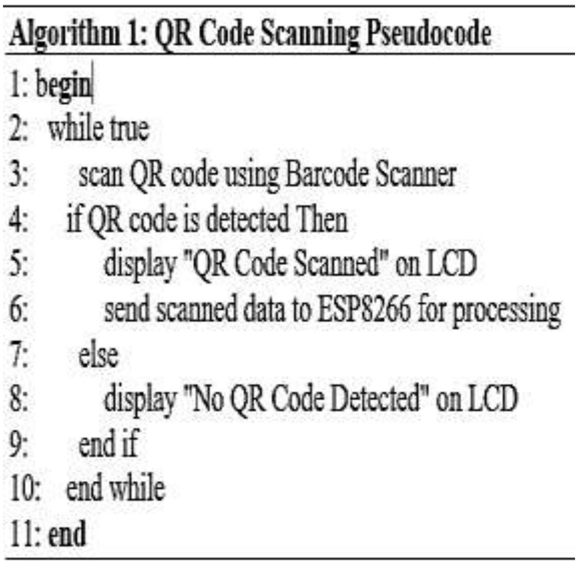
3.3 System Working Principle

The system operates in the following stages:

1. **QR Code Generation stage:** The user generates a unique QR code from a mobile application. This QR code contains encrypted information, such as the user's unique identifier (UID), which is linked to their credentials in the system's database.
2. **QR Code Scanning stage:** The user presents the generated QR code to the barcode scanner at the smart lock. The scanner reads the QR code and extracts the encrypted UID data. The pseudocode for this stage is shown in Table 2.
3. **Data Transmission to ESP8266 stage:** After scanning, the extracted UID data is sent to the ESP8266 microcontroller. The ESP8266, which is connected to the internet via Wi-Fi, forwards the UID data to a remote server for verification.
4. **UID Verification stage:** The server receives the UID from the ESP8266 and compares it with stored credentials, if the UID matches the information in the database, the server sends an "Access Granted" response back to the ESP8266. If the UID does not match, the server sends an "Access Denied" response. The pseudocode for this stage is shown in Table 3.
5. **Access Decision:** Upon receiving the server's response, the ESP8266 processes the result: If Access Granted, the ESP8266 triggers the relay to close the circuit, allowing current to flow to the solenoid lock and the door is unlocked. If Access Denied, no action is taken, and the door remains locked.
6. **System Feedback:** Throughout the stages, the 16x2 LCD display provides real-time feedback to the user:
   - "Scanning QR Code" during the scanning phase.
   - "Access Granted" if the UID matches the database and the door is unlocked.
   - "Access Denied" if the UID does not match.

7. **System Reset:** After the operation, the system resets itself to standby mode, waiting for the next QR code scan.

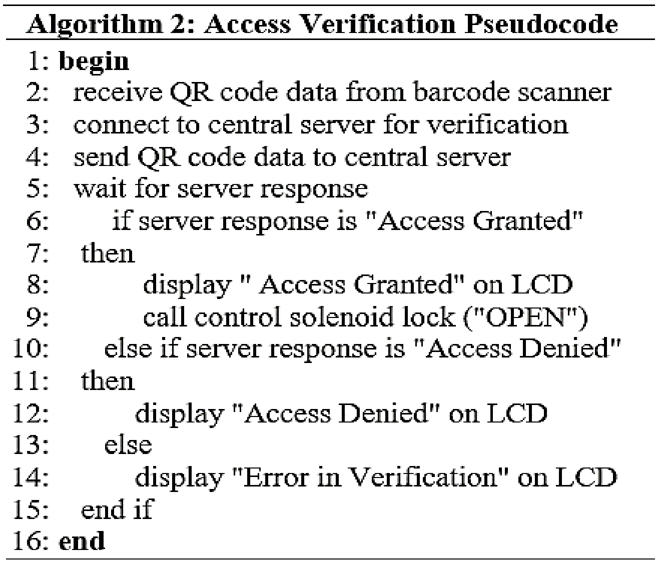
Table 2: Pseudocode for QR Code Scanning



Algorithm 1: QR Code Scanning Pseudocode

```
begin
  while true
    scan QR code using Barcode Scanner
    if QR code is detected Then
      display "QR Code Scanned" on LCD
      send scanned data to ESP8266 for processing
    else
      display "No QR Code Detected" on LCD
    end if
  end while
end
```

Table 3: Pseudocode for UID Verification and Access Decision



Algorithm 2: Access Verification Pseudocode

```
begin
  receive QR code data from barcode scanner
  connect to central server for verification
  send QR code data to central server
  wait for server response
    if server response is "Access Granted"
  then
      display " Access Granted" on LCD
      call control solenoid lock ("OPEN")
    else if server response is "Access Denied"
  then
      display "Access Denied" on LCD
    else
      display "Error in Verification" on LCD
  end if
end
```

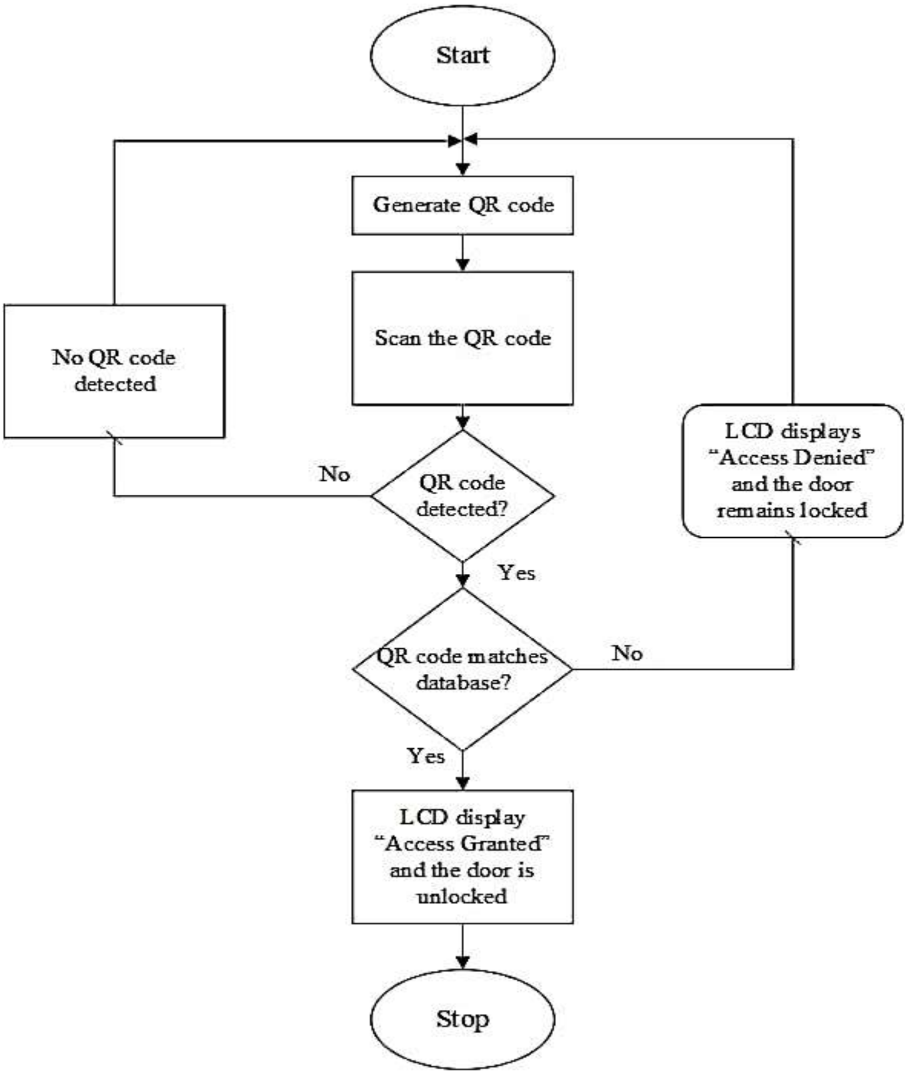
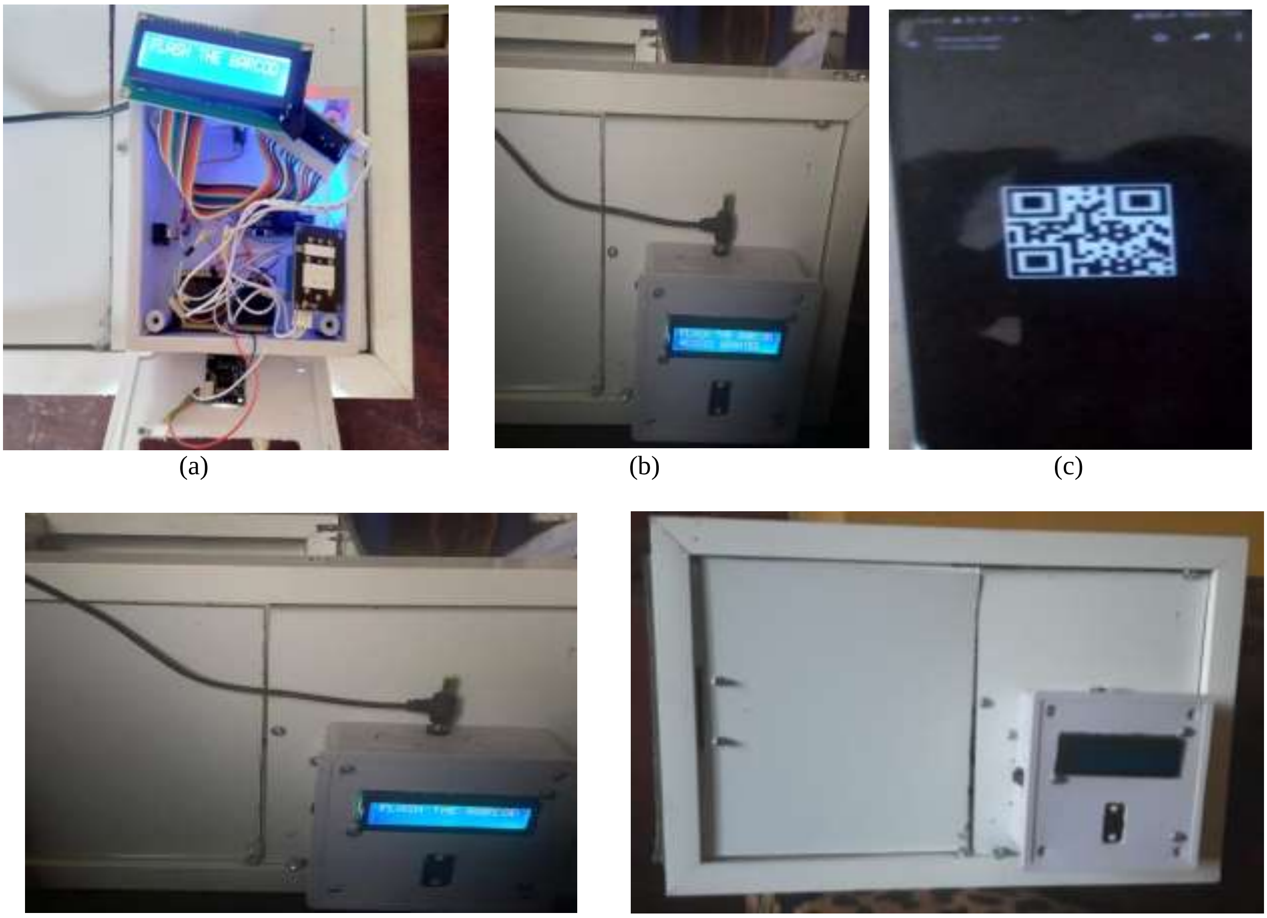

Start
Generate QR code
Scan the QR code
No QR code detected
No
QR code detected?
Yes
LCD displays "Access Denied" and the door remains locked
QR code matches database?
No
Yes
LCD display "Access Granted" and the door is unlocked
Stop

Figure 3: The flowchart of the smart lock system

3.4 Testing Phases

The testing phases involve

i. Component Testing: The internal components (e.g., QR scanner, locking mechanism, power supply) were individually tested as shown in Figure 4(a).
ii. Electrical Testing: During the electrical testing, power consumption and performance under three voltage conditions (5V, 9V and 12V).
iii. System Functionality Testing: The system was verified to ensure that it is inactive and in a secure state before scanning as shown in Figure 4(b).
iv. QR Code Scanning Testing: The QR code scanning process was tested and it was confirmed that the unique QR codes for each user is generated correctly as shown in Figure 4(c).
v. Scanning Accuracy Test: The QR scanner's ability to read codes at various angles and lighting conditions was also tested as shown in Figure 4(d).
vi. System Usability Test: Feedbacks were gathered from users on the scanning process, to ensure it is intuitive and quick for users. Responses were satisfactory.
vii. Data Encryption Test: The QR code data was verified and it was securely encrypted to prevent unauthorised access.
viii. System Integration Test: The smart lock integrates smoothly with mobile applications and the complete system is shown in Figure 4(e).



(a) (b) (c)

(d) (e)

Figure 4: The comparison of the authentication time of different methods

4. RESULTS AND DISCUSSION

The performance measurement was carried out on the developed system using the following variables:

1) Authentication Speed: The time taken from scanning of the QR code to unlocking the lock for three voltage levels (5V, 9V and 12V) was measured and recorded as presented in Table 4.
2) Response Time: The time taken for the system to display feedback on the LCD after a QR code scan was recorded as shown in Table 4.
3) Accuracy: The number of successful and unsuccessful scans to determine the accuracy of the QR code reading under different voltage conditions was counted as presented in Table 4.

4) Access Methods: The proposed access methods was compared with the four methods, key, password, fingerprint and card presented in [8] as shown in Figure 5. The proposed method had an authentication time of 2.00 seconds that outperformed all others, notably faster than the average times of 5.13 seconds for a key, 4.78 seconds for the password, 2.44 seconds for a key card, and 2.98 seconds for fingerprint authentication.

Table 4 displays the relationship between voltage, current, power, authentication speed, response time, and scan success rates. The system's speed improved with increasing voltage, with the fastest authentication time being 2.0 seconds at 12V. The response time also decreased with higher voltage, reaching 0.2 seconds at 12V, indicating quicker feedback after QR code scanning. The number of successful scans increased with higher voltage, with 99 successful scans at 12V and only 1 unsuccessful scan, showcasing a high degree of reliability.

Figure 5 shows the comparison with other methods. The smart lock system's authentication time (2.0 seconds) outperformed traditional methods such as keys, passwords, key cards, and fingerprint scanning, making it a more efficient access control solution. These results demonstrate that the system is reliable, accurate, and faster compared to conventional access control methods, making it suitable for various environments.

Table 4: The results of the performance indices for different voltage levels

Variables			Performance Indices			
Voltage (V)	**Current (A)**	**Power (W)**	**Authentication Speed (s)**	**Response Time (s)**	**Successful Scans**	**Unsuccessful Scans**
5	0.20	1.00	2.50	0.5	96	4
9	0.15	1.35	2.40	0.4	98	2
12	0.10	1.20	2.00	0.2	99	1

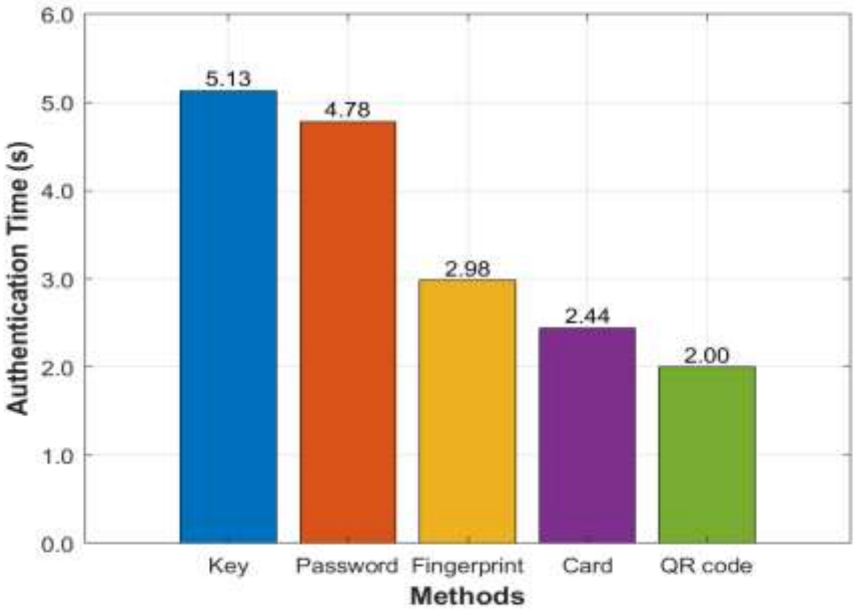


Figure 5: The comparison of the authentication time of different methods

5. CONCLUSION

In conclusion, the smart lock system utilizing QR code technology represents a significant advancement in the realm of access control and security. A streamlined and efficient solution that enhances both the convenience and robustness of access management has been developed using QR codes. A user-friendly interface that simplifies the authentication process while maintaining a high level of security was created. The system not only expedites the entry process for authorised personnel but also ensures that only individuals with the proper credentials can gain access to the designated areas. The integration of QR codes not only enhances the speed of access but also mitigates the risks associated with traditional key-based systems or manual check-ins. This technology provides an additional layer of security through its dynamic and unique code generation, making it significantly more resistant to unauthorised access attempts. Moreover, the scalability and adaptability of the smart lock system make it suitable for a wide range of environments, from corporate offices and educational institutions to residential complexes. The system can be easily customized to meet the specific needs and requirements of different organisations, showcasing its versatility in addressing diverse security challenges. In addition, the implementation of the smart lock system using QR codes marks a significant milestone in access control technology. This work not only enhances the security posture of the protected premises but also sets the stage for future innovations in the ever-evolving field of security systems. To further enhance the capabilities of this system, future work will focus on integrating artificial intelligence (AI) and Internet-of-Things (IoT) technologies. AI can be leveraged to improve decision-making by analysing user behaviour patterns and predicting potential security threats, thereby making the system more proactive in preventing unauthorised access. Additionally, IoT integration will enable the smart lock system to communicate with other connected devices, such as surveillance cameras or smart home systems, to provide a more comprehensive security solution. This integration will enhance real-time monitoring, enable remote access control, and improve the overall user experience, paving the way for more intelligent and interconnected access management systems.

REFERENCES

[1] Mohankumar, A., Ahamath, I., & Gowtham, R. (2024). Revolutionizing home security: A comprehensive overview of an advanced RFID door lock system for keyless access and smart home protection, *Asian Journal of Applied Science and Technology (AJAST),* 8(1), 1-13.

[2] Aluri, D. C. (2020). Smart lock systems: An overview. *International Journal of Computer Applications,* 177(37), 40-43.

[3] Sudhakara, C., & Venkateswara Reddy, B. (2021). Safe and secure entry system with dynamic QR code, *Dogo Rangsang Research Journal,* 8(3), 264-272.

[4] Zainuddin, A. A., Abd Rahman, A. D., Nor, R. M., Hussin, A. A. A., Mohd, N. N. M. S. N., Shamsudin, A. U., & Sapuan, M. S. (2024). Innovative IoT Smart Lock System: Enhancing Security with Fingerprint and RFID Technology, *Malaysian Journal of Science and Advanced Technology*, 360-365.

[5] Vaithilingam, S., & Shankar, S. A. M. (2024). Enhancing Security in QR Code Technology Using AI: Exploration and Mitigation Strategies, *International Journal of Intelligence Science*, 14(02), 49-57.

[6] Tejaswai, C.M., Avadhanam S. S., Amari S., Challagundla T. & Kandagaddla L. A. (2024). Development of an IoT-Based QR Code Access Control and Payment System usin Arduino and ESP8266, *Journal of Science and Technology*, 9(6), 20-32.

[7] Tu, J. F. (2016). A contactless door lock controlled by portable devices. Engineering Computations: *International Journal for Computer-Aided Engineering and Software*, 33(6), 1631-1641.

[8] Satanasaowapak, P., Kawseewai, W., Promlee, S., & Vilamat, A. (2021). Residential access control system using QR code and the IoT, *International Journal of Electrical and Computer Engineering (IJECE),* 11(4), 3267.

[9] Makanjuola, P. O., Shokenu, E. S., Araromi, H. O., Idowu, P. O., & Babatunde, J. D. (2022). An RFID-Based Access Control System Using Electromagnetic Door Lock and an Intruder Alert System, *Journal of Engineering Research and Reports*, 22(11), 7-17.

[10] Okafor, C. S., Nnebe, S. U., Alumona, T. L., Onuzuluike, V. C., & Jideofor, U. C. (2022). Door access control using RFID and voice recognition system, *International Journal for Research in Applied Science and Engineering Technology*, 10(3), 157-163.

[11] Rameswari, R., Kumar, S. N., Aananth, M. A., & Deepak, C. (2021). Automated access control system using face recognition, *Materials Today: Proceedings*, 45, 1251-1256.

[12] Mahadik, S., Narayanan, K., Bhoir, D. V., & Shah, D. (2009, January). Access Control System using fingerprint recognition. *In Proceedings of the international Conference on Advances in Computing, Communication and Control*, 306-311.

[13] Heyn, R., Kuhn, M., Schulten, H., Dumphart, G., Zwyssig, J., Trosch, F., & Wittneben, A. (2019, April). User tracking for access control with bluetooth low energy, *In Proceeding of 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring),* 1-7.

[14] Andati, E. M. (2018). Mobile application for filing of and payment for intellectual property rights using QR code: case of Kenya Industrial Property Institute.

[15] Al-Zahrani, M. S., & Wahsheh, H. A. (2022). Secure real-time artificial intelligence system against malicious QR code links an environmental approach, Fresenius Environmental Bulletin, 31(2), 1618-1623.

[16] The Thonky website. [Online]. (2024). http://www.thonky.com/qr-code-tutorial/

[17] Okomba, N., Adebimpe, E. S. A. N., Omodunbi, B., Sobowale, A., & Adanigbo, O. (2023). Development of an Android Based Home Automation System, *ABUAD Journal of Engineering Research and Development*, 6(1), 51-58.

[18] Soni, P., & Suchdeo, K. (2012). Exploring the serial capabilities for 16x2 lcd interface, *International Journal of Emerging Technology and Advanced Engineering*, 2(11), 109-112.

[19] Varallyai, L. (2012). From barcode to QR code applications. *Journal of Agricultural Informatics*, 3(2).

[20] Asman, F. F., Permata, E., & Fatkhurrokhman, M. (2019). A prototype of smart lock based on internet of things (IoT) with ESP8266, *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika (JITEKI),* 5(2), 101-111.