



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 7.488**

 9940 572 462

 6381 907 438

 [ijirccce@gmail.com](mailto:ijirccce@gmail.com)

 [www.ijirccce.com](http://www.ijirccce.com)

# A Review on Secured Smart Locker System Using IOT

**Rabiya Muskan, Varuni Rao, Divya K Vaidya, Syed Reehan Ahmed, Dr.Kiran Y C**

UG Student, Dept. of ISE, Global Academy of Technology, Bengaluru, India

UG Student, Dept. of ISE, Global Academy of Technology, Bengaluru, India

UG Student, Dept. of ISE, Global Academy of Technology, Bengaluru, India

UG Student, Dept. of ISE, Global Academy of Technology, Bengaluru, India

Professor, Dept. of ISE, Global Academy of Technology, Bengaluru, India

**ABSTRACT:** Internet of Things (IoT) is a system of physical devices which is referred to as “things” connected with actuators, sensors, software with an aim of forming a connection and transferring data with other systems through internet. This paper does a survey as to how a QR code can be implemented using Arduino and ESP8266 which has a built in WiFi modem in order to secure door access. The project describes the creation of a wireless door lock that may be unlocked by scanning a QR code through smart phones. Using smart phones and smart devices becomes easier and affordable and it's a decent choice to make our project smarter by eliminating mechanical elements like keypad and sensors. An Arduino based system is implemented which makes use of a QR code. The QR code is stuck on the door of the locker, which is to be scanned by the user's smartphone. A login page appears on the user's smartphone as soon as the QR code is scanned. The login ID is then sent to Arduino Uno by the interface. Then the Arduino Uno processes the information and controls the voltage using a transistor and resistor to open the locker. a legitimate and unique login ID must be entered by the user which might be provided beforehand to him, only after which the solenoid lock will automatically open thereby opening the door of the locker. ESP8266 is employed to line up local Wi-Fi.

**KEYWORDS:** ESP8266 modem, Arduino Uno, npn transistor, resistor, IoT.

## LINTRODUCTION

People are concerned about the security of their highly esteemed belongings such as jewels and ornaments, cash, confidential files, etc. Hence they tend to use lockers as the safest place to store them. But, sadly they aren't secured as well, thanks to attacks by hackers, fraud. The rapid increase in technological advancement makes people possess highly secured systems to make the lockers withstand against hacker attacks. In recent times, many scams like card skimming, shoulder surfing, fake PIN pads, phishing, etc were carried out by some antisocial elements. Currently the main method of restricting room access to certain people involves the use of physical keys. They carry with them a great number of security issues like risk of losing physical keys, ambiguity in features like fingerprint and face scanning technologies. This leads to the violation of privacy policies of the account holders. Hence QR code scanners are used. In the recent times, ATM cards are replaced with QR code based ATM cards to avoid malfunction like mismatching of biometrics. The project describes the creation of unlocking a smart locker system through scanning a QR code by smartphones. This increases the functionality of smart phones at no additional cost. It makes programming easier by using major built-in library functions present in Arduino. The project designs a locker system that uses only QR code which is simpler and more secure than the existing system.

## II. LITERATURE SURVEY

### A. LockerSecurity System using Keypad and Radio Frequency Identification (RFID)

The proposed system uses password and RFID which allows an authorized user to unlock after a verified login. This includes an application of a secured system which uses RFID and a password supported by an ATmega16 microcontroller. The id from the RFID tag is read by the Radio Frequency Identification (RFID) reader. The user enters the password, if it is correct, then the locker will unlock. The RFID lockers are easy to install and portable and

therefore add an advantage to this system. The system uses Atmega16 which has very less availability of pins hence coding using Atmega16 is hard.

#### *B. Fingerprint Based Bank Locker System.*

The methodology used here is fingerprint matching using AVR microcontroller. The fingerprint sensor scans the fingerprint of the user and forwards it to the microcontroller to match with its records. If the print matches with one of the previous fingerprints of the microcontroller memory then the microcontroller will unlock the latch. But if the fingerprint is foreign, then the buzzer will be activated and the user will have to try again. Here the execution is fast since there is no boot loader that slows down the start up time of the microcontroller. The system has a complex structure, number of executions is limited and memory management is slowed down which affects the system.

#### *C. Smart Security System Using Programmable Logic Controller (PLC).*

Here the locker unlocks at a particular location and at a particular time. At a proper geographical area, at a stipulated time, to open the locker, the user has to give the right password. As the password is verified, the user's fingerprint is taken as an additional factor of prime access to the locker. If someone has prime access, they will be ready to unlock the locker by their fingerprint, no matter placement and time. It has better accuracy, comprehensibility and simplicity. It is easier to troubleshoot and has faster response-time.

#### *D. An IoT Based Bank Locker Security System.*

The methodology used here is an electric lock which uses password verification, fingerprint scanning followed by IR sensor. Here the user will first enter his/her name, password and his/her registered phone number. Then the login process will be initiated by the user. Initially during login process the user will verify the RFID tag through RFID reader. If it matches, the user fingerprint is verified through fingerprint scanner. Once the fingerprint resembling the exact user, it accepts and shows a message "fingerprint is verified" also if the fingerprint does not resemble the exact user then an alert message is sent to the authorized user that "Warning!! There is an unaccredited login". This is followed by subsequent step to enter a password. Once all these steps are verified, the microcontroller will process the information and activates the motor to control the lock. Here IR sensors, which are capable of detecting motion within the presence or absence of light with same reliability, act as a bonus to the current system.

#### *E. Bank Locker Security with Fingerprint and Image Capture.*

The methodology used here is Fingerprint technology, facial recognition technology with Raspberry Pi and OTP generation. The system uses fingerprint sensing and image capture. This system scans the fingerprint and also captures the image of the user and compares it with the registered customer image. If a match is not found with an existing image of the particular user, then it sends the message to the concerned bank manager and the customer. Also, the buzzer is used to know about the unauthorized person to the bank manager immediately. If both the image and fingerprint are verified, then the locker is unlocked. The only problem is the servo motor needs more than 5 volts but raspberry pie provides less than 5 volts.

#### *F. High Protection Bank Locker Security System using Image Capture and Voice Authentication.*

The methodology used here is Voice identity technology, face detection technology and OTP generation. A digital camera is used for image seizing whose statistics is processed by means of matlab and Arduino. Mic is used for voice recognition. DC motor is used to open the locker door. The system consists of a buzzer and a GSM that alert the user in case of any wrong inputs. Since this system uses voice recognition there are chances of misinterpretation or misspelling of words which results in wrong input.

#### *G. Design and Implementation of Secured Banking System using Machine Learning Classification Algorithm.*

The system is employed to secure a locker by establishing three phases. The first phase involves recognition of the person's face. In the second phase a biometric scanner is used to get the person's fingerprint, if it matches, then it goes to the final stage where an OTP is sent to the authenticated person using GSM technology. Machine learning algorithm Voila Jones is used here for facial authentication. It is robust as the user authenticity is checked in every phase and only then the locker opens. However it requires proper lighting for face detection and is not reliable in case of identical twins.

*H. Secure Bank Lockers using RFID and Password based Technology.*

The project involves three user certificates. It contains three types of login having three different kinds of systems. In the first phase, the face of the user is identified and detected. When you recognize the right person, then it goes to the second phase. In the second phase it examines the person concerned / finger / RFID and checks if it is a match or not. In the third phase sends an OTP to the person's phone number via GSM technology, when the user logs into the OTP only then the lock will be opened. This paper introduces an intelligent bank locker system which is developed using matlab for face recognition, microcontroller with biometric scanner. It also consists of an IR sensor. The IR sensor is activated when a person enters and if the access is not given within 60 seconds the buzzer gets activated hence alerting the user.

*I. Fingerprint Based Bank Locker with Image Capture.*

The aim of the proposed system of a door locker with fingerprint and image capture is to provide security with zero human security activity. This method requires fingerprint verification while using the door locker, it also takes the snap of the user who is using the locker and stores it in a memory card. The system scans the fingerprint and if it is verified with the stored fingerprint, the locker unlocks and it also captures the image of the user handling the locker. This is done by ATmega328 microcontroller. The microcontroller operates the data sent by the system. If the fingerprint does not match the registered fingerprint of the user, it will send the alter message to the authorized user and immediately stored the image in the memory. So, the system is extremely essential for eliminating the theft. But the information is stored in a memory card hence there are high chances of losing it.

*J. Biometric Finger Vein based Bank Security System using Arduino and GSM Technology.*

The main principle of the system is to reduce the amount of frauds and thefts that are occurring in our day to day lives in bank locker security systems. The system blocks the concept of proxy, as finger veins are one of biometric technologies and distinctive for every person. This model is built up with an Arduino and GSM technology. Initially, the biometric data of the authentic person is collected and stored to the specified database. This system only provides access to the authentic user and eliminates proxy. This system can be employed in finance, banking, ATM's, etc. The model consists of Arduino which is a ready to use structure with a built in package.

**III. PROPOSED SYSTEM**

To overcome the problems faced in the existing system a smart locker system is proposed that uses QR code as a security measure. The locker consists of a QR code which when scanned opens a login page using ESP8266 modem. The user on entering the login id (which is assumed to be a secret) opens the locker once the id is authorized. Figure 1 represents block diagram of the proposed system.

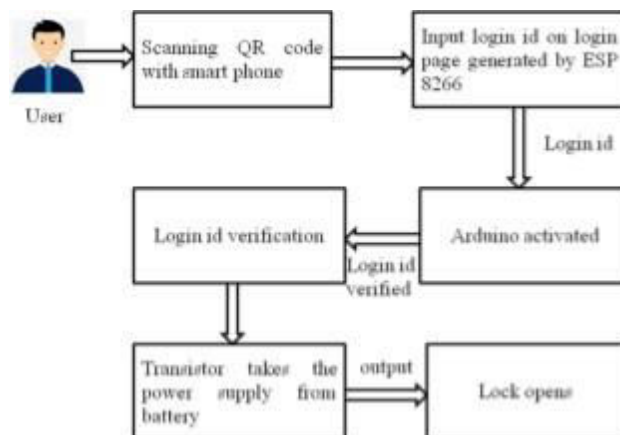


Figure 1: Block diagram of proposed system.



#### IV. SYSTEM ARCHITECTURE

The system has been developed using the Client-Server architecture. The figure shows the components in the Locker system. The QR code Scanner and User Login are both applications running on Android devices that act as clients to the server. The Arduino board is connected to the QR code Scanner via ESP-8266 modem and acts as a physical hardware interface to the solenoid lock.

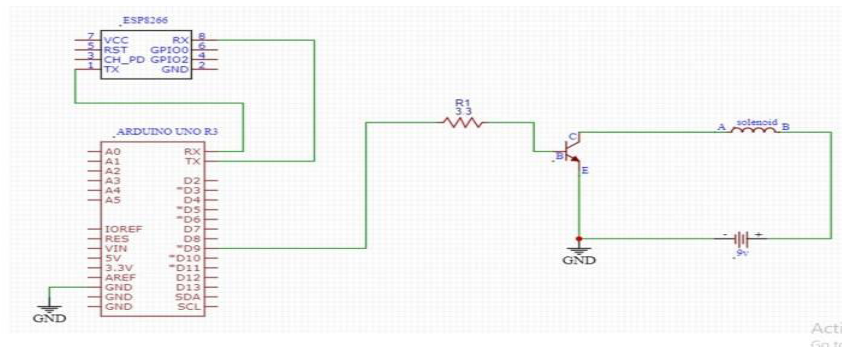


Figure 2 : Circuit Diagram

#### V. REQUIREMENTS

##### A. Arduino Uno R3.

Arduino Uno is an easily available microcontroller board which is based on the microchip ATmega328p. It consists of various Digital and Analog Input/Output pins that can be connected to various expansion boards (Bread - Board). It has six Analog Input/Output pins, fourteen Digital Input/Output pins and can be programmed with the Arduino IDE, through a USB cable. It can be connected to an external battery of 7 – 20 Volts or by an USB cable.



Figure 3: Arduino Uno R3

##### B. ESP8266 modem.

It helps a microcontroller to access a Wireless network to establish a simple TCP/IP network.

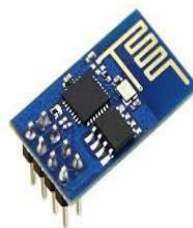


Figure 4: ESP8266 modem

C. NPN Transistor.

The NPN transistor is intended to pass electrons from the emitter to the collector. The emitter emits electrons into the bottom which controls the amount of electrons the emitter emits. The NPN transistor amplifies the weak signal entered into the bottom and produces strong amplified signals at the collector end.



Figure 5: NPN Transistor

D. Solenoid lock.

It is a little electromagnet that pushes or pulls a plug which is used to operate a function. The latch on the solenoid lock performs electrical locking and unlocking.



Figure 6: Solenoid Lock

E. Resistor.

Resistors are electric devices which have a specific, constant electric resistance. They are capable of restricting electrons in a circuit. They consume only power as they are passive components.

F. Battery.

Batteries are a tool consisting of electrochemical cells having a connection to provide power to electric appliances like torches, remote controls, radios, and automobiles externally. The solenoid lock requires battery voltage of around 6 V to 12V therefore we consider battery voltage of 9V.

### VI. CONCLUSION

This project describes a Smart Lock with secure and encrypted interactions with valid users. This project simulates the real Smart Locks performances and their functionalities. It successfully replaces the current traditional system that the banks are following. It fulfils the requirements of supporting autonomous locking device using QR Code compared to physical keys. The project gives way to a secure and smart locker which is less subjected to any kind of malicious activities.



#### REFERENCES

1. Salma Mohammed, Abdul Hakim Alkeelani, “Locker Security System Using Keypad and RFID”, Institute of Electrical and Electronics Engineers, June 2020.
2. Prashik Bagde, Ghanshyam Wadhvani, Harshdeep Bondade, Levia Bolli, Shivani Kumeriya, Dipali Pethe Professor, “Fingerprint Based Bank Locker System” International Journal of Engineering Science and Computing, Volume: 10, Issue No: 3, March 2020.
3. Kannan E, Gowtham S, Logesh G, Prabhakaran P, Prasanth M, Praveen Kumar P, “ Smart Security System Using PLC”, International Research Journal of Modernizations In Engineering Technology and Science, Volume: 2, Issue No: 3, March 2020.
4. Thirumalai, Gokul. R, Ganasekaran. P, Manellore Murali. M, Jackson Jublience Joseph. L, “An IoT based Bank Locker Security System”, International Journal of Engineering Research and Technology, Volume: 08, Issue No: 07, 2020.
5. V. Hindumathi, M. Sushmitha, M.Yoshitha, R. Venkata Harika, A. Sri Vaishnavi, “Bank Locker Security with Fingerprint and Image Capture”, Journal of Electronic Design Engineering, Volume: 5, Issue No: 2, July 2019.
6. Priya Kumari, Puskpanaik, Raghavendra, Parameshwara, Divya M N, “High protection bank locker securitysystem using live image and voice authentication”, International Journal of Scientific Research and Review, Volume: 7, Issue No: 3, March 2019.
7. Seema, Prafulla, Benaka R Shetty, Sanketh Shrikanth Hegde , Raveendra G, “Design And Implementation Of Secured Banking System Using Machine Learning Classification Algorithm”, International Journal of Scientific Research and Review, Volume: 7, Issue No: 3, March 2019.
8. Prajwal D, Naaga Soujanya N, Shruthi N, “Secure Bank Locker Using RFID and Password Based Technology”, International Journal Of Scientific Development and Research, Volume: 3, Issue No: 5, May 2018.
9. Ambrish Kumar, Anish Kumar, Kushagra Gohil, Laxit Porwal, Manish Cheepa, Ankit Vijayvargiya, “Fingerprint Based Bank Locker with Image Capture”, International Journal of Advanced Management, Technology and Engineering Sciences, Volume: 8, Issue No: 3, March 2018.
10. L.Jegan Antony Marcilin, V. Balamurugan, A.Vijayayyappan, “Biometric Finger Vein Based Bank Security System using Arduino and GSM Technology”, International Journal of Applied Engineering Research, Volume: 13, Issue No: 11, 2018.





**INNO SPACE**  
SJIF Scientific Journal Impact Factor

Impact Factor:  
7.488

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details