International Journal of Scientific Research & Engineering Trends
Volume 5, Issue 2, Mar-Apr-2019, ISSN (Online): 2395-566X

# Cloud Based Secured Locker

**Shilpashree P.S** shilpashree@sit.ac.in
**Abhishek Kumar Tiwari** abhitiwari8797@gmail.com
**Ashutosh Prakash** ashutosh.1si15ec018@gmail.com
**Saurabh Kumar Singh** saurabhnit@gmail.com
**Electronics and Communication Engineering**
Siddaganga Institute of Technology
Tumakuru, India

***Abstract*- In the modern era, security plays a significant role. Every individual has valuable accessories like gold, jewellery or cash. It is not enough to have these accessories, but security of this is very important, for this purpose some people prefers to keep them in bank lockers. Still it is common to hear or read in news that some fake person accessed the locker of another person and have stolen their accessories. In order to deal with this type of frauds, verification of the person who wants to use the locker is very important. In this project, advance secured system is designed which will make sure the authentic access of the locker overcoming all the misuses. For this purpose, it is better to have unique password technique through the OTP verification and use of biometric verification which is more effective, secured and fast. If an unauthorized user tries to breach the locker, the alarm signal would be raised to notify the security guards. The owner is also notified by sending the snapshot of unauthorized user to authenticated email id. In this system locker will have a wireless module which connects to the Internet and communicates with the user and admin through internet from anywhere in the world. The main objective of this project is to embed a locking system in the door consisting of two step with locking positions, controlled by the user and admin using android app and burglar alert system when someone tries to open the locker manually.**

***Keywords*- OTP, biometric, e-mail id, embed, alert system.**

## I. INTRODUCTION

The aim of this project is to overcome one of the security issues existing in the present society. It has been very complex for people to have better security system even though in the enhanced technological situations. A variety of solutions have already been proposed in the field of locker system using ZigBee, Bluetooth and Radio Frequency modules. The entire previous systems lacked wide range of accessibility as well as security. In this system, it is not the lock but a brand-new door is made with high-quality mechanical arrangement and strong locking system without losing the original essence of the locker.

As the device is linked to internet it can be controlled by the user from any place with internet connectivity. This system is also embedded with security alert system using a sensor acquisition, biometric sensor and Android App which alerts user about the successful locking (using One Time Password) and unlocking which admin can monitor at any point of time using mobile phone. The OTP generated changes each time the user requests and sent to the android app accessed by admin. User has to open locker by entering the unique password (OTP) on keypad provided by admin to user followed by biometric test. The admin can send the OTP through android app to user which is more secured as the admin's and user's page are separately designed. In case if the person is unauthorized or anyone tries to cheat him by opening his locker in his absence, the admin will be alerted via email including the snapshot of the culprit. In this locker system, Solenoid Locker will be embedded for secured locking of the door. While the raspberry pi will be used to trigger the locking system. Along with an android application that interfaces with the security system. To make it effortless to lock and unlock our door a time interval is given after which the door is locked automatically.

.

## II. LITERATURE REVIEW

There are numerous types of security locker techniques that are being adopted. An embodiment of the present invention provides a compact electronic security locker system which is electronically locked and digitally accessed. One aspect of an embodiment of the present invention is that it allows authorized personnel access to the identification of the person storing an accessories in a particular locker. In another aspect of an embodiment of the present invention, the locker security system based on RFID and GSM technology which can activate, authenticate and validate the user. Nowadays, locker security systems of banks are continuously improving by integrating increased amount of electronic components. Therefore designing a system for the security of locker using Android application, camera, IR sensors, biometric, keypad and buzzer seems to be more efficient. Some of

the techniques are discussed and their disadvantages are listed.

**1. Finger print based door locker:**
The aim of the project was to control the locker using biometric authentication [1]. Use of finger print is found more secured as it relies on the use of unique physical traits rendering biometric technology a very accurate technique of authenticating end users. Most of the major door lock security systems have a number of loopholes which could be broken down to gain access to the required places, and it creates a concern for a secure and proper working surroundings. Furthermore, terrorism and unauthorized access to places have become a major concern now-a-days, and there is a need for a secure system to avoid unauthorized access particularly in shared access environment. With this consideration, a design of a biometric fingerprint based door lock system has been presented in this paper. Biometric systems such as fingerprint offer tools to implement dependable logs of system transactions and look after an individual's right to privacy.

The RFID or permanent identification number (PIN) based door lock mechanisms can easily be compromised when the RFID card or passwords are shared or hacked, thus for facilities with shared access needs biometric-based secure locker system. In the proposed system, authorized users are enrolled with finger print and verified to give access to a facility that is used by multiple users. A user can also be isolated and a new user can be authenticated in the system. A centralized control system is implemented from where who can access the locker and who cannot can be controlled. This is an Arduino UNO based flexible working device that provides physical security using the biometric sensor technology. But the project only focused on single step verification to access the locker which may not be more secured in case of multiple users.

**2. Bank locker security system based on RFID and GSM technology:**
The aim of the project was to control the locker using RFID authentication and GSM technology which can activate, authenticate and validate the user [2]. In this paper, safety of the money in the bank locker, house, and office (treasury) by using RFID and GSM technology is implemented which will be more secure than other systems. Radio-frequency identification (RFID) based access-control system allows only authorized users to access the locker with GSM technology.

There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Some of the most commonly used RFID kits are lower-frequency (30-500 kHz), mid-frequency (900 kHz-1500MHz) and higher-frequency (2.4 - 2.5GHz). Global system for mobile communication (GSM) is a worldwide acknowledged benchmark for digital cellular communication.
But using biometric is found more efficient and secured as it assures physical presence of user to access the locker instead of RFID as it needs to be carried and may be stolen. Also it is realized that use of android app instead of GSM technology is more secured as the person needs to enter login id and password to access the application.

## III. METHODOLOGY

**1. MQTT-dashboard (Android app)**
It is a publish and subscribe based extremely lightweight messaging protocol. Since it is lightweight, it can be used with connections which have a very low bandwidth (Slow Speeds) or connections which are unreliable. Instead of using the common client-server pattern, MQTT uses publish and subscribe method to transfer information. In this method there are two main entities,

**2. MQTT Broker**
Eclipse Mosquitto is an open source message broker that implements the MQTT protocol. Mosquitto is lightweight and is suitable for use on all devices from low power single board computers to full servers. The MQTT protocol provides a lightweight method of carrying out messaging using a publish/subscribe model. This makes it suitable for Internet of Things messaging such as with low power sensors or mobile devices such as phones, embedded computers or microcontrollers. The Mosquitto project also provides a C library for implementing MQTT clients, and the very popular mosquito_pub and mosquitto_sub command line MQTT clients.

**3. MQTT Client**
When we talk about a client, we almost always mean an MQTT client. Both publishers and subscribers are MQTT clients. The publisher and subscriber labels refer to whether the client is currently publishing messages or subscribing to messages (publish and subscribe functionality can also be implemented in the same MQTT client). An MQTT client is any device (from a micro controller up to a full-fledged server) that runs an MQTT library and connects to an MQTT broker over a network. For example, the MQTT client can be a very small, resource-constrained device that connects over a wireless network and has a bare-minimum library.

The MQTT client can also be a typical computer running a graphical MQTT client for testing purposes. Basically, any device that speaks MQTT over a TCP/IP stack can be called an MQTT client. The client implementation of the MQTT protocol is very straight forward and streamlined. The ease of implementation is one of the reasons why MQTT is ideally suited for small devices. MQTT client libraries are available for a huge variety of programming languages. For example, Android, Arduino, C, C++, C#,

Go, iOS, Java, JavaScript, and .NET. Figure 3.2 shows connection of MQTT broker and clients are connected.

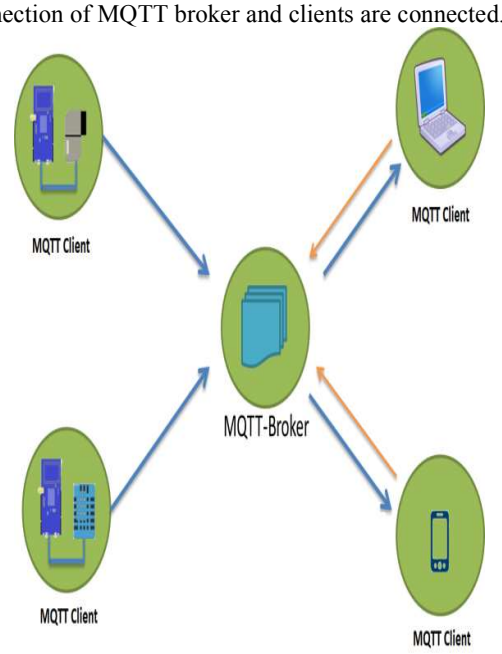


Fig. 1 MQTT communication.

Here iot.eclipse.org is used as cloud, as shown in Figure 1, act as interface between the android app and Raspberry pi, OTP is generated and thus sent over internet which is MQTT-broker and the admin gets the OTP which is shared by the MQTT broker to the MQTT client, which will be user who is accessing the locker, if owner authenticate the user then he can publish the OTP to the user.

**1. Block Diagram**

The block diagram of the cloud based secured locker is shown in Figure 2. This part talks about the square outline and the different segments utilized in Cloud based secured locker, which incorporate Raspberry Pi 3, picam, biometric, buzzer, LCD, storage, keypad, power supply, Android application, and cloud server. The portable application and the raspberry Pi is associated by means of cloud.

Here raspberry pi 3 is a tiny credit Card size computer which is controlling all the essential task of the venture. The key element of Pi 3 is that it is having interior Wi-Fi module. Picam is likewise associated with raspberry Pi so it can catch the image of the individual who is getting to the locker. Biometric is likewise added for giving extra security to the locker. Buzzer will give a humming sound at whatever point where there is any breach in the locker.

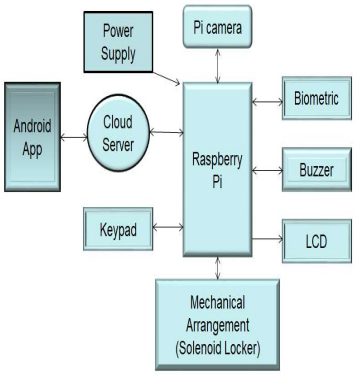


Fig. 2 Block Diagram

**2. Flow Chart**

The Figure of flowchart is shown in Figure 3. The first step for accessing the locker is enrollment, we need to enroll finger print of the authenticated user. After enrollment we need to request OTP by using android app, after getting OTP from the owner of the locker, enter the OTP by using keypad module, if entered OTP is correct then it asks for biometric test and if it matches then locker is open. Otherwise if there is any un-authentication access in the locker then there will be a beep sound from the buzzer and the snapshot of that person will be sent to the owner of the locker.

The components of the Cloud Based Secured Locker is initialized and connected to the internet. The first step for accessing the locker is enrolment, we need to enroll the finger print of the authenticated user. After enrolment, OTP is requested using keypad module by the user. A four digit OTP is generated randomly by raspberry pi which is sent to the admin through android app. After getting OTP the admin shares the same to the user through android app. This process takes place through Message Queuing Telemetry Transport (MQTT) protocol and use of cloud computing applications. The android app acts as an interface between the user and the admin. After getting OTP from the owner of the locker, the user enters the OTP by using keypad module.

If the entered OTP is correct then it asks for biometric test and if it matches then locker opens. This completes the two step verification which makes the locker more secured. Now if the user enters incorrect OTP or the biometric does not match then there is any un-authenticated access in the locker. There will be beep sound from the buzzer which notifies security guards about the breach taking place and the snapshot of that person trying to breach the locker will be sent to the owner of the locker on registered email id.

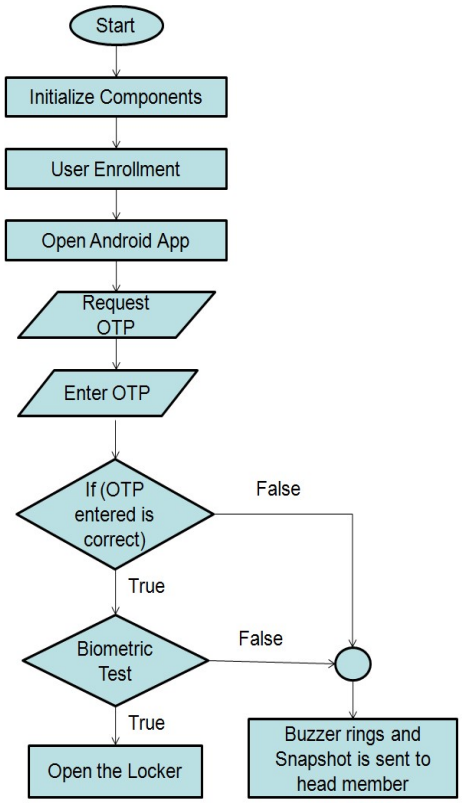


Figure 3 Flow Chart

## V. RESULTS

The two-way authentication of locker using android app and finger print sensor made it more secured. In addition, the OTP generated is only sent to admin's android app and other users can operate the locker only when admin allows them. We can see that the locker is multiple user but cannot be controlled without admin's permission. It is also seen that when an unauthorized user tries to access the locker buzzer rings and the image is captured and sent to owner's email id. This approach has enabled us to achieve the target of controlling the device remotely using a OTP-based system satisfying user needs and requirements. The system is cost effective as compared to the previously existing systems in market and is implemented with high reliability and security. The system is extendible and further additions can be done. Hence, the required goals and objectives have been achieved.

**1. Sanp shots**

**1.1 Receiving OTP in android app**

When 'A' button in keypad is pressed then 4 digit random OTP is generated and it is sent over cloud, admin can access this OTP by logging into MQTT dashboard android app, as shown in Figure 4.

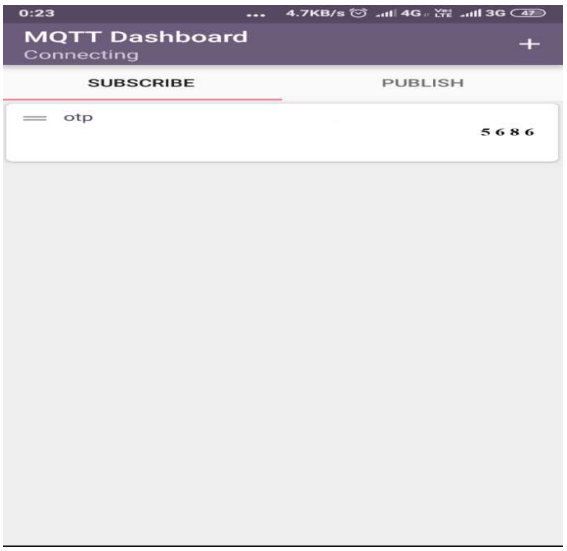


Fig. 4 Receiving OTP in android app.

**2. Publishing OTP to user**

After getting OTP from the cloud owner is publishes the OTP to the user of the locker and the user will receive the OTP in the android app, as shown in Figure 5.

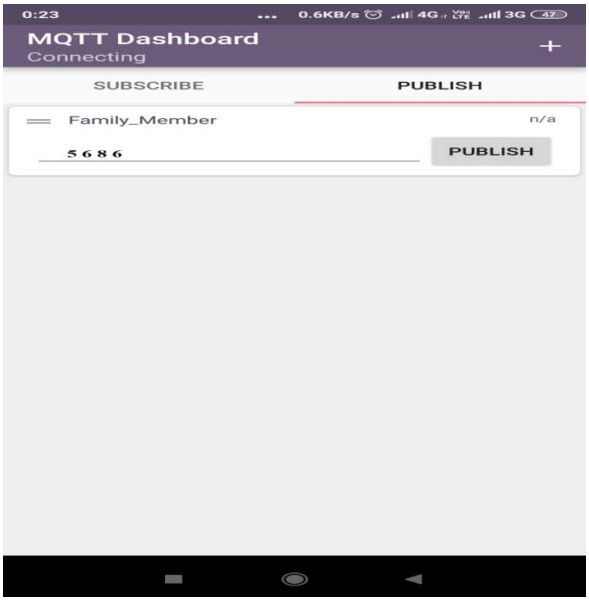


Figure 5 Publishing OTP to user

**3. Receiving the OTP from the admin**

The user who is accessing the locker will have MQTT dashboard android app soon after sharing the OTP by the admin the user can receive the OTP in the android app, as shown in Figure 6.

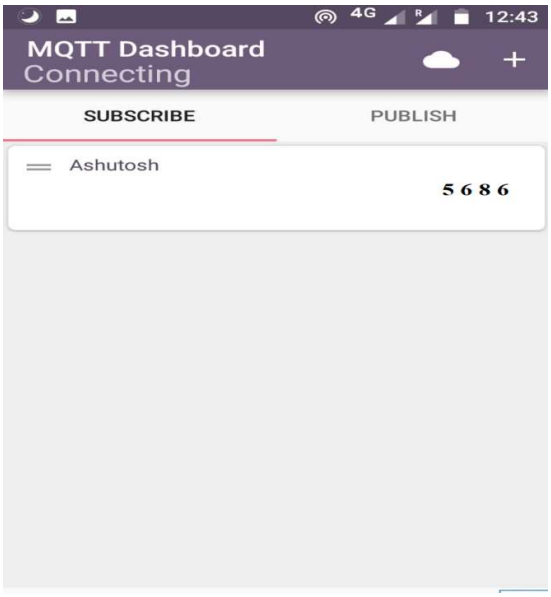


Figure 6 Receiving the OTP from admin

**4. Finger print enrolments**

Authenticated users can enroll their finger print, as shown In Figure 7, and can have access to the locker, by passing the second step of verification if it is correct then door is unlock or else snapshot of that person is sent to the admin.


Figure 7 Finger print enrolment.

**5. Entering OTP**

After getting OTP from admin user need to enter the received OTP by using keypad, as shown in Figure 8.

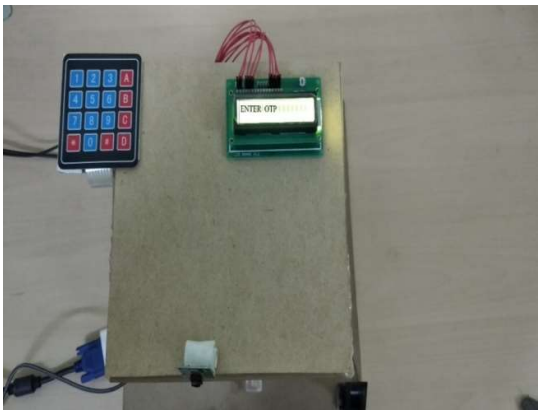

Figure 8 Entering OTP.

**6. Correct OTP**

After entering OTP, if it is correct then correct OTP is displayed on the LCD board, as shown in Figure 9.

Figure 9 Correct OTP

**7. Wrong finger print**

If the finger print does not match with the enrolled finger, then this message is displayed on LCD, as shown in Figure 10.

## V. CONCLUSION

The project Cloud Based Secured Locker is successfully implemented and tested under various conditions. It is done for providing better security, therefore we are using two-way authentication first is otp and second is biometric test. The owner of the locker is having full access to the locker, once getting otp, requested by the user he can give access to him by sharing otp to him and there is a pi camera installed with the locker so that if

there will be un-authentication then the camera takes the snapshot of that person send e-mail to the owner, thus proving better security.

## REFERENCES

1. S. N. Basha, D. S. A. Jilani and M. S. Arun, "An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT", International Journal of Engineering Trends and Technology (IJETT), 2016.
2. J. Baidya, T. Saha, R. Moyashir and R. Palit, "Design and implementation of ngerprint based lock system for shared access", 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017,pp 1-6.
3. Wassim Itani Ayman Kayssi Ali Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures", Eighth IEEE International Conference on Dependable, 2009.
4. S. Ramamani, S. Selvaraju, S. Valarmathy, and P. Niranjan, "Bank Locker Security System based on RFID and GSM Technology", International Journal of Computer Applications., vol. 57, no. 18, pp. 15-20, Jan. 2012.
5. R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of ngerprint veri cation systems", IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3 18, Jan. 2006.