Cloud Computing based Intelligent Bank Locker System

A. Devi¹, M. Julie Therese², G. Premalatha³

¹Assistant Professor (S.G), Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram.
²Assistant Professor, Department of Electronics and Communication Engineering, Sri Manakula Vinayagar Engineering College, Puducherry.
³Assistant Professor, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram

⁰deviarumugam02@gmail.com, ²julietherese88@gmail.com, ³pgsmartprem@gmail.com

Abstract. Now a day’s personal security is a major concern in all the aspects. Most of the people have their personal asserts such as cash, gold, silver etc, in a locker due to security of the accessories. But the security of those asserts is not assured because of robbery and theft problem happening in day today life. In order to overcome the drawback, we proposed a system based on Cloud computing for providing and ensuring high security in the bank, Jewellery shop, home and every place where security of the locker is more important. The proposed system consists of wireless switch, Raspberry pi 3, GSM and finger print scanner in order to allow only authenticated customer to open their lockers to take their accessories. If the authentication fails, the GSM automatically sends the message to the customer regarding failure of locker opening, and gives the alarm signal that makes the people in the bank to notice.

1. Introduction
In present scenario, many people are concerned about the threat of rising crime in their communities. In all the bank, the locker system requires manual locking. Whenever the user wishes to open their locker, the bank employee needed to assist the customer. The major drawback of such manual locking system are lack of safety and waiting time of the customer can be increased. It is to be noted that any employee who is free at that time can accompany with the customers. Some people who are working in the bank will try to steal the accessories. Fortunately, there are many ways to protect from theft. Some of the ways are to install an alarming system in their bank or use password protected locker. But these systems may not be efficient in all the time. So in order to overcome this, authentication of a person is very important.

Personal security system such as passwords, PIN number or identity cards, are used for personal identification. But the card number can be guessed and the card can be stolen by the people. So in order to provide high security, the proposed system is designed to solve these problems with the help of biometric authentication together with emerging technology known as Cloud. The biometric system is otherwise called as a pattern-recognition system. The biometric authentication is one of the most important part in every authentication system i.e. Finger print. This biometric authentication is used to identify the individuals because it is unique to every individual. Generally the process requires many comparisons of the finger print pattern which are classified into arch, loop and whorl [11].

With the rapid development, many sectors spend large amount of money for developing and installing software in to order improve their services and ensures the bank usage satisfaction of their clients. Past decades all the software was installed on local servers. But now, most of the sectors choose cloud computing based solution in order to achieve reliable operations in real time. The cloud computing is an emerging paradigm which enables the people to access software on the internet as a service. With the help of cloud, the management of locker is performed effectively. This cloud based locker management provides protected environment. There are many reasons to use cloud computing solutions. Some important reasons are
- Reduced Cost: No need of buying a right device and hiring technical people. For cloud based solutions, the bank sector can pay for only serves acquired.
- Flexibility: Mobility is one of the major advantage of cloud computing solution.
- Scalability:
  - No backup action
  - Security of the data

Based above stated reasons, the proposed system is integrated with cloud computing. The proposed system performs fingerprint authentication followed by password authentication. In this proposed system, a wireless switch plays a major role of giving the access to use a fingerprint scanner. The raspberry pi will take the necessary action according to the signal provided by the fingerprint scanner.

The rest of the paper is organized as literature review for understanding the related work carried out, function carried out by proposed system, details of the hardware used to implement the proposed system, flow diagram for describing the entire process, implemented experimental set up and simulation result, finally concluded with future enhancement.

2. Literature Review
In this section some of the related work described for motivation to do the work to be carried out. There are number of secured locker system were developed. Various methods such password, RFID, biometric authentication based methodologies were adopted by bank. Now a days, bank also try to integrate technologies such as GSM to provide secured locker system. Some of the proposed techniques are given reviewed below.

Shilpashree P.S, Abhishek Kumar Tiwari at el (2019), both biometric and OTP verification were performed to allow authenticated customer to open the locker [1]. In this proposed model, password can be accessed easily by unauthorized user.

Mr. Lokesh M. Giripunje at el (2017), OTP generated by android app verification was performed, and identification of the accessing of customer was made based on the customer OTP number followed by fingerprint verification [2]. In the proposed model, there is a possibility of unauthorized customer who gain the access of locker.

Hiloni S. Detroja at el (2016), GSM, fingerprint and RFID technology were used for locker opening and closing actions. First SMS verification was performed for entering the password via keypad. Then the RFID and fingerprint verification were performed in order to open the locker [3].In the proposed model, there is a possibility of hacking of password by an unauthorized user.

S.V.Tejesvi at el (2016), two level securities has been proposed such as fingerprint and GSM methodologies. One time password authentication was proposed. The proposed work can provide security and also save time for banker and customers [4]. The proposed work, information cannot be properly intimated to bank.

Mrutyunjaya Sahani at el (2015), the face recognition, GSM and zigbee methodologies were adopted for monitoring and controlling of equipment via web [5]. In the proposed model, the face detection takes more complex algorithm.

Swetha J (2014), all the customer was given with a separate RFID with different number in order to identify the customer and grant access to the customer’s locker [6]. In the proposed work, alert warning is not given to user.

Raghu Ram et al (2013), an RFID reader was used to read ID number. If the ID number is valid, then only access may be given to a fingerprint scanner. The fingerprints are matched, the password can be sent to the person mobile number. Finally, the authenticated person can enter both passwords via a keyboard. If these two passwords are matched, then the locker will be opened. A message was sent to the mobile number of the authenticated person, and it will remain in the locked position [7]. In the proposed model, if the mobile phone is hacked, the security of the system will get fail.

N. Khera at el (2014), the image of the people who tries to open the locker is captured. If unauthorized people tries to open the locker, image of the people is captured and the corresponding
warning message was generated [8]. In this proposed model, the corrective action cannot be taken simultaneously when the unauthorized people tries to open the locker.

S. Tanwar at el (2017), by using PIR sensor, the motion of the people can be captured. The captured image was send to the people via email in order to inform regarding theft [9].

S. Sridharan (2014), only dual key authentication and biometric authentication provided only for authenticated customers [10]. The proposed model can be easily used by unauthorized people.

3. Framework methodology
Initially personal details, fingerprint and mobile numbers of each customer are registered in the cloud data base. When the customer wants to open their locker, they need to approach the bank manager. If the bank manager switches on the wireless switch which is attached in the door, the signal will be received by the raspberry pi 3 which is attached with the locker. The raspberry pi 3 has inbuilt Bluetooth and Wi-Fi capabilities. The wireless switch plays a major role in the proposed method. Because when the wireless switch is switched on, then only the customer can able to do biometric and password based authentications. The wireless switch is placed at the bank along with the normal switches.

When the wireless switch is ON, the people who need to open their locker has to keep their finger on a fingerprint scanner. Once the finger print scanning is successful, then they have to enter the password. Once the password has been entered correctly, then it makes the motor to rotate in order to open the locker. If the finger print or password authentication fails, the GSM sends the messages to the user, and gives the alarm signal. The camera is used for capturing the image of the people. Suppose if the wireless switch is in OFF condition, the customer tries to open their locker by placing their finger print, the system will automatically send a message to the customer mobile for contacting the bank manager.

The proposed system can perform three level of authentication such as wireless ON condition, finger print authentication and password authentication. If any one of the authentication fails the customer couldn’t able to open their locker. So the security of the lock in the bank can be ensured. And also the altering message can be sent the customer regarding locker opening failure as a message. This system ensures personal asserts safety of the customers of the bank and reduce manpower for accessing the locker.
4. Hardware Details
The basic components used to implement the proposed locker system are explained in detail.

4.1 Wireless Switch
These switches can be easily installed like the standard switch [15]. One switch is enough to control multiple receivers. It does not require any wires for making the connection, and also it does not require any batteries. These types of switches can be used like a remote controller. In the proposed system, the wireless switch plays a major role. When the switch turned ON, then only the authenticated customer is allowed to enter their password.

![Wireless Switch](image)

Fig.2 Wireless Switch

4.2 Raspberry pi B+ Model
In the proposed work, raspberry pi B+ acts as a master [13]. It takes the control over all the components attached with it and takes the necessary actions [12]. Once the wireless switch is turned ON, the raspberry pi starts its works. The customer password and finger print authentication successful, it makes the motor to rotate for opening the locker.

4.3 Finger Print Scanner
In the proposed system, initially customer can put their finger image on the finger print scanner. This image will be stored in cloud database. If the customer wants to open their locker after switch ON wireless switch, they need to put their finger on the scanner. When the finger print image is matched with stored database, then password authentication can be proceeded.

4.4 Keypad
In the proposed system, the keypad is used to enter the password by the customer after successful completion of finger print authentication [14]. The password for each customer is enrolled initially. So once the password is entered, it tries to compare the password matching in the server in order to open the locker.

4.5 GSM modem
GSM (Global System for Mobile communications) is a cellular technology used for mobile voice and data services. It is developed using Time Division Multiple Access (TDMA) technique for communication purpose [16]. In the proposed work, the GSM is used to send the messages to the bank manager when authentication of the customer fails and the user.

4.6 Servo motor and Buzzer
In the proposed model, the servo motor is used to open the locker when the finger print and password authentications are successful. In the proposed model, the buzzer is used to give alarm signal when authentication fails.

4.7 Camera
Generally camera is used to capture the motion images. It has lens that focuses light from the scene, and camera body has an image capturing mechanism. In the proposed system, the camera is used to capture the image of a person who tries to open the locker.
5. Flow Diagram
The flow diagram of the proposed system is shown below. The step by step process has been described to the entire operation of the proposed system. The registration of the people by registering their fingerprint and mobile number in the Cloud server. If they need to open the locker, approach the bank manager for wireless switch activation. Once the wireless switch is activated, then fingerprint authentication followed by entering the password can be done. Once the authentication process pass, then the locker will get open. If authentication fails, alarm will get generated.

6. Experimental Setup
The hardware set up of the proposed system is shown in the Figure 4. The proposed module is attached at the locker. Wireless switch is placed at the bank manager place. When the manager switch on the wireless switch, then only the customer can put their finger on the fingerprint scanner. Once the biometric authentication successful, then the customer can enter their 4 digit password. If the password authentication succeed, then the locker will get open. If any of the authentication fails, then the message will be sent to the customer and the alarm signal will be generated by buzzer. The camera is used to capture the image of the people who tries to open the locker.
Fig. 4 Hardware setup of working model

7. Simulation Result
The simulation result of the proposed system is shown in the Figure 8. The simulation result is implemented using Proteus software [17]. The Proteus suits a PCB design and simulation tool [19] for electronic design automation. This tool is simple and easy to use by an electronics engineers to design PCB layout as well as microcontroller simulation.

Fig. 5 Simulation Result

8. Conclusion and future enhancement
The proposed system allows provides three levels of security to allow only authenticated customer to open their locker by switching ON the wireless switch. The system not only provides high security to
open the locker but also reduce the waiting time of the customer and mainly reduces banker’s workload in real time. It is easy to implement and use. The future of this paper can be extended by adding some other personal information of the customer such as face recognition and iris recognition. So that the unauthorized access of the locker can be avoided. Further, the proposed model can be applied to identify the illegal entrance.

References

[1] Shilpashree P.S, Abhishek Kumar Tiwari, Ashutosh Prakash Saurabh Kumar Singh, “Cloud Based Secured Locker” International Journal of scientific research & Engineering Trends (IJRSET),vol.5, no.2, 2019.
[2] M. S. Divya and M. N. Rao, “Centralized Authentication Smart Locking System using RFID, Fingerprint, Password and GSM,” International Journal of Engineering & Technology, vol.7, no.3, p. 516, 2018.
[3] Mr. Lokesh M. Giripunje, Suchita Sudke, Pradnya Wadkar, Krishna Ambure, “IoT Based Smart Bank Locker Security System” International Journal for Research in Science & Engineering Technology (IJRASET), vol.5, no.11, 2017.
[4] Hiloni S. Detroja et al, “GSM Based Bank Locker security System using RFID, Password and Finger print Technology”, International Journal for Innovative Research in Science & Technology, vol.2, no.11, 2016.
[5] Mrutunjaya Sahani , Chiranjiv Nanda , Abhijeet Kumar Sahu , Biswajeet Pattnaik “ Web-Based Online Embedded Door Access Control and Home Security System Based on Face Recognition” International Conference on Circuit, Power and Computing Technologies [ICCCPIT], 2015.
[6] Raghu Ram.Gangi, Subhramanya Sarma & Gollapudi, “Locker Opening And Closing System Using RFID, Fingerprint, Password” International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),vol.4, no.7,2013.
[7] Swetha J, “RFID based automated bank locker system” International Journal of Research in Engineering and Technology, vol.3, no. 5, 2014.
[8] N. Khera and A. Verma, "Development of an intelligent system for bank security" 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), pp. 319-322, 2014.
[9] S. Tanwar, P. Patel, K. Patel, S. Tyagi, N. Kumar and M. S. Obaidat, "An advanced Internet of Things based Security Alert System for Smart Home" International Conference on Computer, Information and Telecommunication Systems (CITS), 2017, pp. 25-29, doi: 10.1109/CITS.2017.8035326.
[10] S. Sridharan, "Authenticated secure bio-metric based access to the bank safety lockers," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, pp. 1-7, 2014.
[11] A.Devi and P. Dharani Devi and K. Gayathri, “Enhancement and Identification of Finger Print Image” (August1,2019). Proceedings of International Conference on Recent Trends in Computing, Communication & Networking Technologies (ICRTCCNT) 2019, Available at SSRN: https://ssrn.com/abstract=3430647 or http://dx.doi.org/10.2139/ssrn.3430647
[12] A. Devi and G. Kavya, "Intelligent System for Identifying Dyscalculia Based on Raspberry Pi," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 723-729, doi: 10.1109/ICCES45898.2019.9002398.
[13] “Raspberry Pi,” Wikipedia, 07-Sep-2020. [Online]. Available: https://en.wikipedia.org/wiki/Raspberry_Pi. [Accessed: 09-Sep-2020].
[14] “Keypad,” Wikipedia, 26-Aug-2020. [Online]. Available: https://en.wikipedia.org/wiki/Keypad. [Accessed: 09-Sep-2020].
[15] “October 12, 2012,” Fine Homebuilding. [Online]. Available: https://www.finehomebuilding.com/2012/10/12/. [Accessed: 09-Sep-2020].
[16]. “GSM Modem SIM 300,” Mepits. [Online]. Available: https://www.mepits.com/product/185/GSM/GSM-Modem-SIM-300. [Accessed: 09-Sep-2020].

[17]. “Proteus Design Suite,” Wikipedia, 25-Jun-2020. [Online]. Available: https://en.wikipedia.org/wiki/Proteus_Design_Suite. [Accessed: 09-Sep-2020].