

Reviewed document: **BANK LOCKER SYSTEM (Muhammad tawqeer) 20-6-2020.docx**
Processing date: **23.6.2020 10:28 CEST**

A total of 86 sentences were analysed. As a result **66** sentences (76.7%) were found in other documents.

These sentences are highlighted in the text by using different color shades according to the amount of similarity. The darker the highlighting color, the more words were found in another document. You may click the highlighted sentences in order to get further details about found reference documents. Learn [more about this report](#) and [how to evaluate it](#).

The following graphic shows the distribution of found sentences within the checked document. The colored parts of the overview bar indicate those parts of the document in which sentences were found in other documents. The left boundary of the bar corresponds to the beginning of the document and the right boundary to the end of the document accordingly. By clicking into the overview bar you are directed to the corresponding position in the document.



Reference documents

The following list contains titles and addresses of documents in which similar sentences were found. With a click on the number of found sentences („x Sentences“) the corresponding sentences are highlighted in the document as well as in the navigation bar by a colored border and you are directed to the first position of the corresponding sentences in the document. Another click on „x Sentences“ resets the highlighting.

61 Sentences were found in a text with the title: „**IRJET-V5I10320.pdf**“, located at:
<https://www.irjet.net/archives/V5/i10/IRJET-V5I10320.pdf>

5 Sentences were found in a text with the title: „**233-W057.pdf**“, located at:
<http://www.inse.org/vol4/233-W057.pdf>

4 Sentences were found in a text with the title: „**Paper Title (use style: paper title)**“, located at:
<http://elektro.untirta.ac.id/dosen-hartono1.php>
<http://www.ijert.org/soldier-protection-vesture>
<http://www.jetir.org/papers/JETIRCS06054.pdf>
http://www.ijarcce.com/upload/2016/may-16/IJARCCE_211.pdf

3 Sentences were found in a text with the title: „**Finger Print Based Bank Locker Security System – IJERT**“, located at:
<https://www.ijert.org/finger-print-based-bank-locker-security-system>

3 Sentences were found in a text with the title: „**Development of Microcontroller-Based Biometric Locker ...**“, located at:
https://www.researchgate.net/publication/282481702_Development_of_Microcontroller-Based_Biometric_Locker_System_with_Short_Message_Service
https://www.researchgate.net/profile/Crystalynne-Cortez/publication/282481702_Development_of_Microcontroller-Based_Biometric_Locker_System_with_Short_Message_Service/links/57f5be3808ae886b897f825c/Development-of-Microcontroller-Based-Biometric-Locker-System-with-Short-Message-Service.pdf
<https://mafiadoc.com/development-of-microcontroller-based-biometric-locker-system-with-598c46051723ddcb690d7fbb.html>

3 Sentences were found in a text with the title: „**Paper Title [Font: Times New Roman, Size:20]**“, located at:
http://ijirt.org/master/publishedpaper/IJIRT148861_PAPER.pdf

2 Sentences were found in a text with the title: „**233-W057 | Biometrics | Arduino**“, located at:
<https://www.scribd.com/document/329602061/233-W057>

2 Sentences were found in a text with the title: „**digital locker new account 5_ | Documentine.com**“, located at:
https://www.documentine.com/digital-locker-new-account_5.html

► In 76 further documents exactly one sentence was found. (click to toggle view)

Subsequent the examined text extract:

BANK LOCKER SYSTEM USING BIOMETRIC IDENTIFICATION

Engr. Tauqeer Sahibzada .

Faculty of Engineering & Technology . Gomal University, Dera Ismail Khan, Pakistan
muhammadtawqeer800@yahoo.com

.....
.....
.....
.....

Abstract— The paper describes development of a microcontroller Arduino based biometric bank locker system with Aadhaar card database management in cloud storage, mobile app and webpage, which ensures the security of personal and confidential belongings of a person. In this system, we have used R305 fingerprint module for biometric security which is IOT enabled using HC05 Bluetooth module. The safe lock unlocks itself using servomotor when correct fingerprint or pin is entered. The android mobile application is used to operate the system, which also has a QR code sensor which scans the Aadhaar Card of the user and stores the information in a Google sheet, which can be accessed from anywhere with proper username and password. The webpage describes all the major features and advantages of the system and also includes an in-depth video of the working of the system. This webpage is also accessible from the app. Hence, this is user friendly and easy-to-use biometric locker system, wherein an app and a website give all the information regarding the system and its features.

Keywords—Aadhaar Card, Biometric, Servomotor.

1) Introduction.

Bank lockers are popularly used by Indian population; they prefer keeping their valuables in the bank lockers rather than in their homes. Most of the banks have lockers such that one key is with the user and the bank has a master key. Moreover, they also have password which the user has to tell the bank subordinate before going in the locker room, now if the user loses the key then, it is a big security risk. Common bank lockers do not guarantee full safety of the users' belongings and can easily be opened by any person without the user's consent.

Biometric allows a person to be identified and authenticated based on a set of recognizable and verifiable data, which are unique and specific to them. Biometric authentication is the process in which a person's characteristics are compared with the person's biometric "template", wherein this reference model is first stored in database, and then biometric identification is used to determine the identity of the person using the image of their fingerprint, iris or face. Biometric data are considered as unique for every individual and cannot be copied or stolen. [1]

Fingerprints are the most common biometric technology used in different applications. The fingerprint recognition and matching is one of the simplest ways of verifying a person's identity. It requires the imaging and comparison of the print pattern which includes the ridges and minutiae points. These patterns are unique to every individual. Several studies using fingerprint biometric recognition were conducted to enhance locker systems. One of them was the study of Lay, Yang and Tsai (2011) entitled "Biometric Locker System" wherein fingerprint recognition technique was used to open and shut the lock of a cabinet system. The system first detects the fingerprint of the locker renter and matched the fingerprint to reopen the locker. This was done to reduce troubles of keys and to ensure the security of the renter [2]. Although there were existing studies about biometric lockers, the present system is developed to enhance security. Here the user has to scan the QR code of their Aadhaar Card so that the database is maintained to ensure who opens and accesses the locker. The Aadhaar card database implementation makes the management of users' database hassle-free. Moreover, an app is developed to make all the functions of the model easily accessible. A website is designed so that the bank personnel can understand the working of the locker and also the app.

OBJECTIVE OF THE STUDY.

The system is aimed to develop a prototype of a microcontroller- based locker system that can:

1. Enroll or delete fingerprints of the user and save these patterns within the database.
2. Control the locker using mobile app and send commands thereto using the app connected through Bluetooth.
3. Scan the QR code of the Aadhaar card to take care of a database
4. If the locker renter whose fingerprint is employed to open the locker features a problem with fingerprint scanning thanks to injury or any treatment then a then pin is additionally provided for every locker, alongside Aadhaar details verification.
5. Webpage to supply the working and outline of the prototype and application.

PROPOSED SYSTEM.

We are implementing a Biometric Bank Locker System using Fingerprint Reader and identification, Bluetooth and QR Code. The Aadhaar Card has all the important information about the person which includes his name, date of birth, address. The QR code when scanned through the phone camera saves all this information. This system is implemented using microcontroller Arduino Uno, the fingerprint module uses software serial communication to send and receive

signal from the Arduino. Bluetooth module HC-05 which uses hardware serial of Arduino is used as a communication media between mobile app and Arduino. The system is operated using the app designed for the bank authorities.

Figure. 1 (Block Diagram)

SYSTEM DESCRIPTION.

Components of the system.

Arduino Uno:

The Arduino UNO is an open-source microcontroller board supported the Microchip ATmega328P microcontroller and developed by Arduino.cc. The board is provided with sets of digital and analog input/output (I/O) pins which will be interfaced to varied expansion boards (shields) and other circuits. The board has 14 Digital pins, 6 Analog pins, and programmable with the Arduino IDE (Integrated Development Environment) via a kind B USB cable. It's powered by external 9V power supply. [4]

Fingerprint Module

The fingerprint module used is R305 by Sunrom which uses TTL UART interface. The user can store 127 fingerprints, where each fingerprint image is stored within the sort of a code. It's directly interfaced with 5V Microcontroller Arduino.

Servo Motor.

Servo Motor is employed for opening and shutting of locker. It's work to lock the locker by moving the latch in and out because the fingerprint is correctly identified and confirmed by the software application. It gives precise control of linear position, which may be controlled by giving input from Arduino. The shaft of the motor is connected to a lever rocker, which provides us the linear movement required for the Locker latch. If a circular lock is employed, it's going to be directly attached employing a gearing. Here a solenoid based option could also be also used, but it's going to require a current driver circuit between the microprocessor and therefore the drive, thanks to larger initial current requirement.

All the components are given uniform 5V power supply using 7805 power regulator.

Mobile App Development

The project implementation has been done using an app developed on MIT App inventor. The app developed is presently for the bank operator side, it also can be extended to the user side to urge the notifications about the activity log of the user. The app has mainly two screens. the primary screen features a display box which displays information like if the locker is locked or unlocked, or if the user's fingerprint is valid/ invalid, or the pin, allotted to the user, entered is valid or not and instruction for operating the system. Also, the primary screen has direct buttons for adding a replacement user, deleting a replacement user, for directly verifying the pin and opening the online page designed for the project. Then, there's a button saying "QR code of Adhaar", this button, when pressed, opens the second screen. The second screen features a button 'Scan', which when pressed opens camera for scanning the QR code of the Adhaar card and after scanning the result's

shown within the app also because the Google Sheet is updated with information of user with the time and date of visit for opening the locker system. The app works with the Bluetooth module, making the project IOT enabled.

Webpage.

A webpage within the sort of the assistance manual for showing the operation of the system is formed using web development tools like CSS, JavaScript, and HTML. The webpage contains the overall information and therefore the advantages of a biometric based locker over a standard bank locker. It also gives a summary of all the features of the system alongside a video of the working system.

Working of the system.

Figure. 2 (working System)

Welcome Screen.

As shown in fig 2, the authority of the bank has got to login to the app with username and password only then the system will start. The welcome message on the app screen indicates that the sensor is correctly interfaced and now user is asked to place their fingerprint if they're already enrolled else the user can select options from the app: enroll, delete or modify and check their pin.

Fingerprint Already Created.

Referring to fig 2, user is asked to offer their fingerprint, if it's correct then a green led glows and therefore the servo opens the latch of the locker opens, the locker remains open until the user doesn't press a push, this push is provided in

order that the user can keep the locker open till their work isn't over, once the push is pressed the locker is locked, the app continuously reminds the user to press the push and if the locker is open for quite a specified time then the bank personnel is alerted to lock the locker.

Fingerprint Enrolment.

Figure. 3 (Finger print flow chart)

With regard to fig 3 the user is asked to first enter variety between 1-127, if the amount is already allotted an equivalent are going to be displayed and user has got to enter another number, once the amount is made the user is given instructions to stay their finger on the fingerprint module for a few time till 'Image Taken' isn't displayed, this is often done 2 times in order that clear image of the finger is captured.

Pin Generation.

If the owner of the locker can't be physically present then an option for opening the locker using pin is additionally provided, but this is often only possible after this feature is enabled within the app by the bank authority. The pin is given during the enrolment. The servo opens the latch of the locker if the pin is correct then the user has got to push the push and therefore the locker are going to be locked.

Delete/ Modify Fingerprint.

Referring to fig. 4, the user is first asked to enter their enrolment number. If the enrolment number exists, then the user is given option for modification or deletion of their account. If the user selects 'Modify' option, then they're asked to enter the enrolment number then the fingerprint is modified, and if user selects 'Delete' option then, they're asked to enter their enrolment number again so as to confirm if they're sure then the account is deleted.

Figure. 4 (Deletion flow chart)

Adhaar Card Database.

The app is formed for the bank authority now after an accurate fingerprint or pin is identified the servo won't open the latch till the Adhaar card of the person opening the locker isn't scanned. The app scans the QR code of the Adhaar card and updates the knowledge (Name, Address, and Father's Name) alongside date and time on a Google Sheet on real time basis. After this the bank authority has got to press the 'Scanned' button on the app, until this the servo won't operate. This permits to stay a record and database of all the people opening the lockers and further increases the safety of the system.

CONCLUSIONS

All the components of the system were compatible with the microcontroller, the programs were developed, tested and uploaded within the Arduino and Mobile app successfully felicitated their operations. the subsequent functions were successfully implemented and tested:

- 1). Enrolment, saving of the fingerprint and generation of the pin.

2). Proper identification of correct and incorrect fingerprint or pin.

3). Synchronized working of the mobile application with microcontroller code and hardware including the lock opening and shutting mechanism.

4). Proper establishment of the connection between Bluetooth based app and Arduino alongside proper scanning of the Adhaar Card and online uploading of the knowledge on Google Sheets.

This system are often further developed with GSM module, in order that the user can receive SMS regarding their locker opening and shutting times alongside the Adhaar card information of the person operating the locker. This module also can be wont to provide an OTP whenever the enrolment number is deleted or modified. Moreover elaborate security layers are often added to database system.

REFERENCES

<https://www.gemalto.com/govt/inspired/biometrics>

“Development of microcontroller-based biometric locker system with short message service” Lecture Notes on Software Engineering, Vol. 4, No. 2, May 2016, Crystalynne D. Cortez, Jaswinder S. Badwal, Jocelyn R. Hipolito, Ditche Jane C. Astillero, Melvie S. Dela Cruz, and Jaira C. Inalao .

<http://www.rhydolabz.com/documents/finger-print- module.pdf>

https://en.wikipedia.org/wiki/Arduino_Uno

Joyce Soares and A.N.Gaikwad, “ A Self Banking Biometric Machine with fake detection applied to fingerprint and iris along with GSM technology for OTP”, International Conference on communication and signal processing ,April 6-2016 , India.

N.Raghu Kisore , Institute for Development and research in Banking Technology , Hyderabad India ,” Secure SMS protocol for Implementing Digital Cash System”,2015 International Conference on Advances in ComputingCommunication and Informatics(ICACCI)

Jongpil Jeong , Min Young Chung and Hyunseung choo, “ Integrated OTP-Based User Authentication Scheme Using Smart Cards in Home Networks ”, processing of the 41st Hawaii International Conference on System Sciences 2008.

Abhilasha A Sayar¹ , Dr. Sunil N Pawar² , “Review of Bank Locker System Using Embedded System” , International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 5, Issue 2, February 2016.

SanalMalhotra, “Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology” ; International Journal of Advances inElectronics Engineering – IJAEE Volume 4 : Issue 3 .