WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Survey on IOT based Secure Bank Locker System

Amit V Mhaskar[1], Mr.Pravin Bhangale[2]

[1]M.Tech Scholar EEDept,KCE's COET Jalgaon
[2]Asst.Prof.KCE's COET Jalgaon
amitmhaskar89@gmail.com

ABSTRACT

The objective of this paper is to have a survey on a bank locker security system using different technologies like Iris Scanner, Face Recognition, Fingerprint and passwords for securing valuable belongings in the locker. The bank customers are now more concern of their valuables like documents, jewellery, and many more material. The safest place to keep all such valuable is bank. With the development in security related technologies, the bank locker security system also need to be more secure and theft proof. This survey further lead to design of IoT based multilayer security system for bank lockers.

Key Words: Fingerprint, IoT, Locker

1. INTRODUCTION

In present world, the safety and security is utmost priority for any bank vaults and locker systems. At present, bank uses passwords, keys, Personal Identification Numbers or identification cards for security of lockers. But, this systems have their own drawback. The cards can be stolen, and passwords and numbers can be guessed or slipped one's mind. The biometrics like fingerprint is more accurate method of recognizing a person based on a physiological or behavioral characteristic.

2. LITERATURE REVIEW

Arvasu Chikara, [1] described that a smart locker has been designed for banking sector. The main feature of this work is it keeps track of time, date and number of access of blocker by a user in the bank. The smart lock program will compare your image and fingerprint with the data already stored in the database. After checking the authenticity of the user, the microcontroller (Arduino) will give signal to the lock and it will open. It also gives a message when the number of permissible access turns increases in a given duration.

Ashutosh Gupta, Prerna Medhi, Sujata Pandey [2], describes a multilayer security system which can be used in Home, Bank Lockers etc. to prevent thefts. Multilayer security provided by the combination of three securities which is based on the sequence of (I) RFID, (II) password and (III) Biometric consecutively. All the three modules are controlled through a microcontroller. The Proposed system is more efficient and reliable due to multistage security and may not be breached with the combination of all three stages.

Raj Gusain [3], the objective of this paper is to design a bank locker security system which is using Face Recognition, Iris Scanner and Palm Vein Technology (PVR) for securing valuable belongings. A face recognition system is a system which identifies and authenticates the image of the authorized user by using MATLAB software. The images of a person entering a unrestricted zone are taken by the camera and software compares the image with an existing database of valid users. Iris Recognition system uses generous characteristics present in human body. This technology is employed for biometric authentication in ATM's, Immigration & border control, public safety, hospitality and tourism etc. This paper serves techniques so that capability of palm vein recognition system can be improved using modified vascular pattern thinning algorithm. Palm Vein Recognition (PVR) is a technology which recognizes palm vein pattern of an individual and matches it with the data stored in database for authentication. This is a very reliable technique and has a very good accuracy and is considered as the most secure and better technique for security purposes.

3. SYSTEM DESIGN AND DEVELOPMENT

3.1 Design methodology

With reference to literature review and problem statement, easy and secure locker system using microcontroller is the area of concern in the project work. So, this work is concentrated on following points

Design conceptualization and requirement analysis.

Selecting appropriate EDA tool for circuit design.

Component selection and circuit design
PCB designing & fabrication
Development of boot loader and application programs.
Testing and analysis of designed system.
The method followed and necessary steps required to design and develop hardware platform with AVR device are shown in Fig. 3.1. These steps are conceptualization, analysis, design, capture (logical design) and layout (physical design).

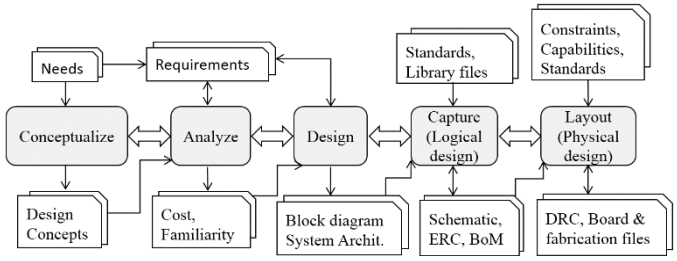

Fig. 3.1 System design and implementation flow

One most important part of designed system is boot loader code which is in-system programming technique. The code is been developed with reference the AVR microcontroller. The communication between microcontroller and ESP 01 module is implemented.
The application of this designed method is to demonstrate easy and secure locker system using biometric and password based security levels. The system implementation flow is shown in Fig. 3.1.
The design flow has a well-defined start and finish point, and the developer and customer can decisively identify the progress process with the essential requirements. This demonstrates the priority placed on the requirements and design phases, resulting in less waste of time and effort, as well as a lower risk of customer expectations not being realised. Due to client involvement throughout the whole project life cycle, this methodology decreases risk. As a result, any change in requirements before the project's conclusion is feasible. With the help of prototyping and tools, the methodology chosen is robust enough for the development of a locker system and would increase system quality by meeting client needs at each stage, resulting in a considerable reduction in errors. In the event that this process fails, the project can be restarted at the user design phase. Because each step includes specialised deliverables and a requirement analysis procedure, this model will be simple to maintain. With this model, the proposed project's deliverables will be more valuable because each phase will be clearly demonstrated to the client. The following are some examples of how this model can be useful:

- Problems will be easier to solve;
- large volumes of code will be easier to manage; and
- human labour will always be verified.

Table 3.1 Comparative study of existing system

Parameters if or Comparison	Locker system based on GSM & RFID technology	Locker system based on fingerprint technology	Locker system based on and GSM technology , RFID& fingerprint, password	Proposed Locker System based on two-factor Authentication
Authentication approach "Something you know" Examples: user account	Two password are used in this system whereas a user require to enter the given	An 8 character password is used to authenticate a user. Referred	A user needs to enter the 8 character password which is send to	A user need to enter the 6 character PIN which is send to authenticated user mobile number.
Names, password, PIN and pass code.	Password through the keypad and the same password must be send to microcontroller using GSM modem. The entropy of 8character password is low and it can bestolen/guessed/forgotten.	Password for the system is permanent which can be easily breakable.	Authenticated user mobile number.	Each access has a restricted time span, thus the specified PIN is generated at random. This type of PIN eliminate the necessity in remembering the PIN/password.

Authentication approach "Something you have" Examples: smart cards, token cards, phone and RFID cards.	RFID card is used as one of the authentication in this system. The RFID card can be stolen/duplicated.	No authentication used in the type of Something you have.	RFID card is used as one of the authentication as earlier system. A user might be forgotten to bring the RIFD card.	A phone is used for the authentication purpose. When a person receives a PIN over GSM, he or she must bring the phone in order to see it. Although a user may forget to pack their phone, it is uncommon to find someone without one in today's environment.
Authentication approach "Something you are" Examples: fingerprint, face, hand geometry, iris, retina, voice and signature.	No biometrics authentication type is used in this system.	The fingerprint technology is used as one of the authentication in this system. It's harder to fake , guess, misplace and forget when compared to user selected password.	The fingerprint authentication issued in this system.	The fingerprint verification is used in this system to authenticate a user. Fingerprint identification is a powerful approach since even identical twins with the same DNA have unique fingerprints, resulting in great uniqueness.
Type of authentication used overall	Something you know (Password) + Something you have (RFID)	Something you know (Password) + Something you are (Fingerprint)	Something you know (Password) + Something you have (RFID) + Something you are (Fingerprint)	Something you know(One time Password) + Something you have(Phone) + Something you are(Fingerprint)
Microcontroller	ATi89C51i	P8iV51RD2i	LPC2148i	Arduino Mega 2560i-Ri3
Platform	Assembly Language and Embedded C	Assembly Language and Embedded C	C programming language	Open Source platform, code can be written in Java.
Fingerprint Scanner	Not implemented	R303A scanner	Data not available	GT-511C3 scanner
GSM Module	SIM300 V7.03 module	Not implemented	SIM300 module	SIM800L Fona GSM module

4. CONCLUSIONS

In this paper, we have studied various locker management techniques and technologies. We can conclude that, the system need to be robust, efficient, easy to maintain and durable. The log of the customers accessing the locker with date and time is also required. All this will help banks to utilize enormous manpower wasted for maintaining locker system in banking sector. For making this system safer as it is related to banking sector we added fingerprint authentication hardware setup which work in sync IoT part. Hence this will help banks to automate their locker system

.

REFERENCES

1. Arvasu Chikara, Pallavi Choudekar, Ruchira, DivyaAsija., "Smart Bank Locker Using Fingerprint Scanningand Image Processing", 6th International Conference on Advanced Computing & Communication Systems (ICACCS), 2020, IEEE
2. Ashutosh Gupta, PrernaMedhi, Sujata Pandey, "An Efficient Multistage Security System for UserAuthentication", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016, IEEE
3. Raj Gusain, "Enhancing bank security system using FaceRecognition, Iris Scanner and Palm Vein Technology", IEEE, 2020.
4. A. Z. M. Tahmidul Kabir, "Six Tier Multipurpose Security Locker SystemBased on Arduino", 1st International Conference on Advances in Science, Engineering and Robotics Technology 2019 (ICASERT 2019), IEEE.
5. Santosh Mahendra, "Smart Security System for Businesses usingInternet of Things (IoT)", IEEE, 2018.
6. R. S. Divya, Meera Mathew, "Survey on various door lock access control mechanisms", International Conference on Circuit ,Power and Computing Technologies (ICCPCT), IEEE, 2017
7. Prof. K. D. Mahajan, "Three Layered Security System For Bank Locker", SSRG International Journal of Electrical and Electronics Engineering (SSRG - IJEEE) – Volume 4 Issue 4 – April 2017.
8. SatvikGogineni, K Marimuthu, and Syed Amma Shei, "IOT Based Centralized Bank Security System for Monitoring and Auto Arresting", Advances in Wireless and Mobile Communications. ISSN 0973-6972 Volume 11, Number 1 (2018), pp. 1-9
9. Sandip Dutta; Nitin Pandey; Sunil Kumar Khatri, "Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner", International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, 2018
10. Ajay Kumar; PriyanSood; Utkarsh Gupta, "Internet of Things (IoT) for Bank Locker Security System", 6th International Conference on Signal Processing and Communication (ICSC), IEEE, 2020
11. Salma Mohammed; Abdul Hakim Alkeelani, "Locker Security System Using Keypad and RFID", International Conference of Computer Science and Renewable Energies (ICCSRE), IEEE, 2019
12. Jannatul Bake Billa; Anika Nawar; Md. Maruf Hasan Shakil; Amit Kumar Das, "PassMan: A New Approach of Password Generation and Management without Storing", 7th International Conference on Smart Computing & Communications (ICSCC), IEEE, 2019.
13. Hitesh Prasad; R. K. Sharma; Uddish Saini [13], Digital (Electronic) Locker, First IEEE International Conference on Measurement, Instrumentation, Control and Automation (ICMICA), IEEE, 2020
14. Prajwal D, NaagaSoujanya N, Shruthi N, "Secure Bank Lockers Using RFID and Password Based Technology (Embedded System)", International Journal of Scientific Development and Research, May 2018 IJSDR | Volume 3, Issue 5.
15. Pooja K M, Chandrakala K G, Nikhitha M A, Anushree P N, "Finger Print Based Bank Locker Security System", International Journal of nEngineering Research & Technology (IJERT), NCESC - 2018 Conference Proceedings, Volume 6, Issue 13.
16. Ambrish Kumar, Anish Kumar, Kushagra Gohil, LaxitPorwal, Manish Cheepa, Ankit vijayvargiya, "Fingerprint Based Bank Locker with Image Capture", International Journal of Advanced in Management, Technology and Engineering Sciences, Volume 8, Issue III, March/2018.
17. Guo Chun Wan; Chao Wang; Jian Zhou; Mei Song Tong, "A Novel Intelligent Door-Lock and Management System Based on STM32 Microcontroller", Progress in Electromagnetics Research Symposium (PIERS-Toyama), IEEE, 2018.
18. M Shanthini; G Vidya; R Arun, "IoT Enhanced Smart Door Locking System", Third International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, 2020.