An IoT based Bank Locker Security System

J. Thirumalai[1], Gokul. R[2], Ganasekaran. P[3], Manellore Murali. M[4], Jackson Jublience Joseph. L[5]
[1]Assistant Professor, Department of Electronic and Communication Engineering
[2, 3, 4, 5] Students, Department of Electronics and Communication Engineering,
TJS Engineering College, Peruvoyal, Chennai - 601 206, Tamil Nadu, India

*Abstract***:- This paper will focused on effective recognizing and controlling system for Bank locker room which is fully self-determining. In cases of robberies, it's commonly happen that the banned entrance in the locker room area which can be detected by our security system. If the robbery take place the banks are not be capable to recognize the robber due to absence of the proof by using the current human operated security system. Development of various sensors has enabled systems to have preventive and corrective measures in this regard significantly. In order to deliver a concrete security solution for critically important and confidential documents and goods, we proposed an Automated Safety Vault with Double Layered Defense Mechanism. The solution comprised of an Electronic Lock driven by password verification and a Biometric authentication for users using a Fingerprint scanning and sensing tool. Both of these two layers ensured the authenticity of the user by preventing any unauthorized access to the Vault. The system was then implemented in a prototype scope for testing and validation of the proposals. The implemented system and testing data showed that the Automated Safety Vault with all its security features had successful operation. The specification of the whole system as well as the results is observed and verified.**

Keywords: Internet of Things (IoT), sensors, Security, GSM, Fingerprint.

1. INTRODUCTION

The Bank which is used to place that indicates the very high level security. In day to day life every person are involved in banking transaction. Because of high level security, we use bank lockers to secure our important documents, expensive jeweler, or cash ect., Hence it has become a very important part for every common human being [1]. To suffer in this world and for a continuous development; the banking sector needs to accommodate a very hinge rise security. As we know new branches are opening by considering the public interest. Hence more security for every sector is required. Because of development current system and services becomes autonomous and banking service is not so far from that. Various researches show that there are accountability in devices and technologies in security system [2]. In automatic security systems generally passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost. The most secured system is fingerprint recognition because a fingerprint of one person never matches the other. Biometrics studies commonly include fingerprint, face, iris, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment.

Among these available biometric traits fingerprint proves to be one of the best traits providing good mismatch ratio, high accurate in terms of security and also reliable. That's why we are motivated to do this paper. Therefore, the study shows all the approaches intent to solve the dire problem of security to critical systems of an institution with proper authorization [3]. Such systems are only accessible by the designated users and not by the mass. Moreover, the solution must ensure the obstruction of all possible ways of violation of security within the periphery of the secured area. It is also expected to regulate the access to certain users divided in different using capacity groups.

2. PROPOSED SYSTEM

Our proposed provides a highly secure, valid and easy to operate for both the customer's who has a locker in a Bank and the head of the branch who responsible for all the operations connected to the safety lockers. Our work does verification process by user fingerprint, legitimate login credentials for authorized user. The key objective of the proposed solution is to obtain the result of collective decision making based on the data provided by multiple sensors. To attain this performance, a controller is employed to analyze the sensor data and to generate desired controlled variables in order to ensure the security of the vault. Arduino UNO platform is a modern day phenomenon for achieving prototypes of such controlling tool with various peripherals. As shown in Fig.1, the controllers played the key role of decision making populated with the biometric and the physical motion detecting sensors and generated the controlled response or regulated to drive the servo motor of the vault door or buzzing the alarm due to unauthorized entry. However, the proposed solution does not only ensure vault security, but also provides certain degree of assistance in designing other similar prototypes involving biometric as well as physical sensing. The main goal of this paper is to overcome the major drawbacks of different locker security systems such as GSM and RFID, Pattern analyzer. Automated vault locking mechanism driven by actuated servo motor controlled and directed by ensuring double layers of safety. Pattern recognition of biometric data i.e., users fingerprint which would be pre-enrolled by scanning the fingerprints of the thumb and index fingers. The patterns were stored in the system database. It ensures the secondary layer safety to the secured vault after successful adherence to the primary layer of password protection. Motion detection in case of extreme violation of both layers of protective measures using sensor to assist physical intervention of security in charge from the law-enforcement agencies the controller served as the brain of the proposed system which

Special Issue - 2020

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ECLECTIC - 2020 Conference Proceedings

being specified with the sensors' data, set the system trajectory to follow security compliances [10].
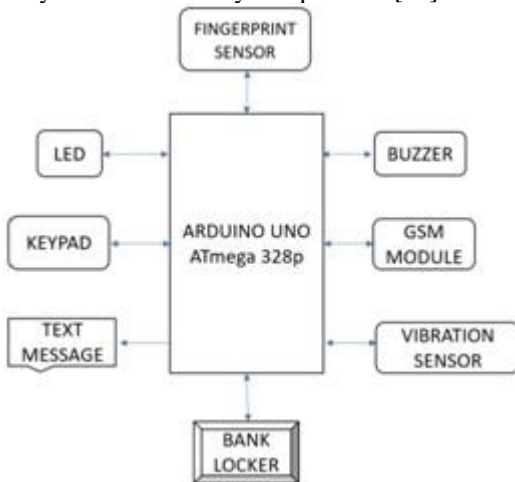

Fig.1 Block diagram of proposed system

The authentication followed a procedure of password verification with a trial limit of three inputs from the user. Failure to provide the correct password within that limit of attempting to access the system would result in system lock down and buzzing the alarm [4]. After successful initializing of Layer 1, the next layer of authentication using fingerprint scanner would be presented to the user for scanning his\her fingerprint. Upon the complete match with the pre-stored fingerprint would activate the servo motor attached to lock of the door of the secured vault to be opened. The proposed model was implemented as a prototype for validation of the working criteria to ensure the safety of a vault using double layers of security.

3. LITERATURE SURVEY

3.1 Security using PIR and IR sensor

In this system two levels security protection is used. One security level uses PIR motion detection sensor and other level uses IR proximity detection. Here Programmable system on chip (PSoC) technology is used to interface these two detection algorithms. PIR is a passive infrared motion sensor used to detect infrared light waves emitting from objects around it. IR proximity sensor detects objects closer to the sensor. The main component in IR sensor is IR LED which radiates infrared radiations that are reflected when an object is in vicinity of sensor. However this system suffers a drawback as there are some colors.

3.2 Security using heat sensor, RFID, GSM

In this system along with RFID tag, heat sensor and GSM is used. Initially locker holder has to swipe his RFID tag which consists of information about bank locker holder like locker number and other details. Once the tag is recognized as valid tag, bank manager will provide respective locker through conveyer setup. Apart from this if somebody tries to open the locker through machine or any instrument, then that theft is detected by heat sensor. As burglar will use some sort of instrument then temperature will be increase, and this rise in temperature will be sensed and an alarm will trigger.

3.3 Security using Face recognition

This system uses face recognition technology to recognize a person, whether he is a bank holder or thief. Every bank has camera system implemented [7]. When a person enters strong room of bank locker, camera present in bank locker captures image of the person. The captured image of the person is given as input to one of the face recognition algorithm. Among various facial features skin color is used here to recognize person. However this system has drawbacks due to difference in facial expression, image orientation, also this system has to maintain huge database.

4. SECURITY USING FINGERPRINT IRIS SCAN

In this system a three level security system is designed. One level uses RFID, second level uses fingerprint scanner and third level uses IRIS identification [5]. At initial stage user has to swipe RFID tag, if the tag is valid then LCD display ask to place finger on fingerprint scanner. If the fingerprint scan is accepted then user has to go through third security level of IRIS scan.

IRIS scan technology is one of the biometric technologies that use pattern recognition technique to identify patterns of a person's retina. Here the person has to bring his eye in front of a camera. The capture eye pattern then will be compared to the eye pattern stored in database [9]. The match if found valid, person will be allowed to access hi locker otherwise bank manager will stop whole procedure. However this fingerprint scan and IRIS scan at initial stage will consume time, as customer will have to follow all this procedure.

5. CONCLUSION

In this paper, the design and implementation of a prototype of an automated vault door locking system is presented which warrants double layer of security. It ensures the proper user of the vault by securing the door with numeric password and biometric authentication. It monitors the conditions of operation of the vault from both the inside and the outside by employing several sensors which are continuously feeding information to the controller of the proposed system to confirm the robustness in terms of rightful access and security of the contents within the vault. The entire system can be easily managed with all the status updates being reeled by the controller to the administrators eliminating the unforced reasons of human errors. The future enhancement to this work could be done by adding some more aspects. Therefore it improved the reliability of bank locker and unauthorized access will be minimized. The enhancement could be further applied to identify the illegal entrance.

6. REFERENCES

[1] Sanal Malhotra, "Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology". International Journal of Advances in Electronics Engineering – IJAEE Volume 4 : Issue 3

[2] P. Sugapriya, K. Amsavalli, "Smart Banking Security System Using Pattern Analyzer". International Journal of Innovative Research in Computer and Communication Engineering. An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 8, October 2015

[3] M.P.Manjunath, P.M.Ram Kumar, Pradeep Kumar, Nalajala Gopinath, Ms. Haripriya M.E, "NFC Based Bank Locker System". International Journal of Engineering Trends and Technology (IJETT) – Volume23 Number 1- May 2015

Special Issue - 2020

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
ECLECTIC - 2020 Conference Proceedings

[4] Peng-Loon Teh, Huo-Chong Ling, Soon- Nyean Cheong, "NFC Smartphone Based Access Control System Using Information Hiding," IEEE Conference on Open Systems (ICOS), December 2013.

[5] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[6] Tarief M. F. Elshafiey, "Design and Implementation of a museum and bank security system using antenna as IR proximity sensor and PSoC Technology", IEEE symposium on wireless technology and applications, September 25-28 Malaysia 2011.

[7] Prof R.Srinivasan, T.Mettilda, D.Surendhran, K.Gopinath, P.Sathishkumar, "Advanced Locker Security System". International conference on Information Engineering, Management and Secuirty

[8] Roshiny Thomas, Sanjana Mathews, Sona Ojus, Sona Roselin Joseph, "Bank Locker Security System Using Face Recognition". International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) Vol 1, Issue 5, April 2015.

[9] Ms.Geetha Hanumanthu, Mr.Dilip Chandra E, "Wireless Identification Of RFID, Fingerprint & IRIS". International journal of innovative research and development.

[10] Seshapu Prasad, D.Suneel, "Proximity Sensor Based Security Lock and Theft Detection". International journal of Science Technology and Management, Vol. No.4, Issue No.01.