IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

OTP Supported Ultra-Security System for Bank Lockers

Mr. Gaikwad S. V., Shinde Rutik Avinash, Wakchaure Samiksha Mangesh, Karpe Abhijit Balasaheb
Department of Electronics and Telecommunication
Amrutvahini Sheti and Shikshan Vikas Sanstha Polytechnic, Sangamner, India

Abstract: *Now-a- day's people are more concern about security of their valuable things. As security towards our valuable things is at most risk because we are using bank as safer place. As with tremendous development due to new technology era people started earning more and buying more precious things. With this huge development of the same need of security is more. Security is very important, for this purpose as people keep these valuable things in a bank locker as for safety. Still, we often hear in newspapers every now and then that some unauthorized person has access the locker and stolen valuable things. In order to overcome this, authentication of the person who wants to uses locker is very important. To overcome this security issue, a strong security system has been proposed using three levels as password identification, RFID detection and GSM technology for OTP. Our goal is to provide solution to security for bank locker from unauthorized person. As there is demand for more efficient security techniques to avoid access bank locker by unauthorized person. The main goal of our paper is to provide 3- ways authentication to provide high security. In this system there will be three steps to authenticate an authorized user*

Keywords: flexible, Easy use, fully automatic, Reliable

I. INTRODUCTION

The Now-a-days safety has become an essential issue for most of the people. Increase in threats in bank has cause of concern as the banks are always targets by criminal. Increasing crimes in banks has become a serious issue. In order to overcome this type of threats, authentication of the person who uses bank locker is very important. Because of this risk, there is a need to define security techniques for identifying a person. [2] So, only authentication of the user is an area of concern.

However, as per research in this domain smarts cards might be stolen, passwords can be easily cracked. Manual way bank people need to be involved with every person. To provide high security and to make easier process, we are taking the help of different technologies like OTP, RFID TAG reader, password. To provide high security, OTP authentication is strong technique as each person has unique biological information. In this paper, we provide three level securities by PASSWORD, OTP authentication and smart phone. Smart phone will help to provide request and get one time password which changes for every access and gives high security. By this three level security system we can provide high security and save the time of both bank employees and the customers. [1-3]

Bank locker room security is important for many reasons. One of those reason is it secures precious things like jewels, hard cash, property papers many things which is very difficult to earn. The present security systems are suffering with the issue of security levels. The less number of security levels can be easily faked by the robbers. In this paper "A Multi Layer Bank Security System" has been designed. This particular security system does not need presence of any human being. The security system itself consists of two distinct security systems which are independent of each other. The first system will be placed at the front door of the locker room area and another will be placed at the gate of the locker room. Most doors are generally manually controlled by the security person employed by the bank with the use of handle locks operated by a key. In this system each user will be provided with a unique RFID card. The front door will open only when a authorize person wants to enter with an authorize card. In the locker room area a passive infrared sensor will be mounted with a camera. In case if a person gets enter at the locker room area without any authorize card then a passive infrared sensor is actively waiting for it, which will send a signal to a microcontroller and the microcontroller will take two actions, first it will switch on the alarms which will inform the local security and second it will take a snapshot of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

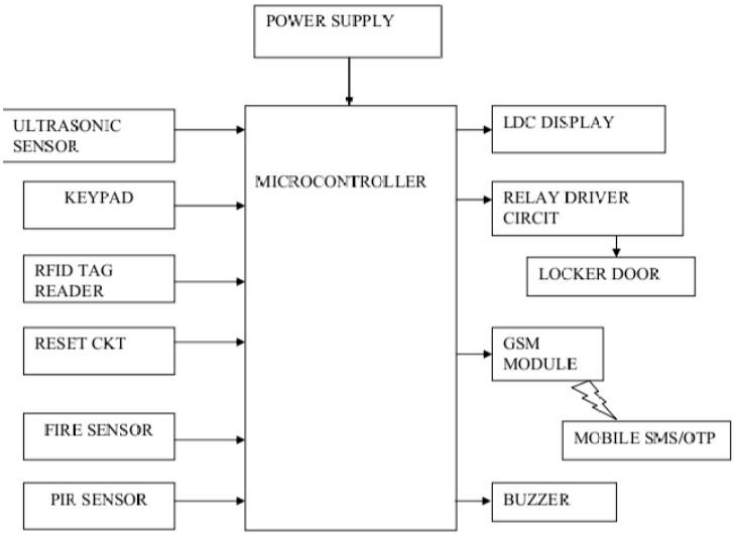
the locker room area and mail it to the authorize person using a personal computer. The second system which is placed at the locker room entrance consist a biometric system. To open the gate of the locker room the person needs to get his/her iris scanned and fingerprints to be verified. When these two processes will complete, only then the locker room will be opened.[4]

The paper proposes the most efficient security system because of different layers of security for detecting any unauthorized activity which should not occur in the confidential areas of a bank. [5]

II. LITERATURE REVIEW

1. The Locker Security System using Facial Recognition and One Time Password (OTP) offers a robust and convenient way to safeguard your belongings. By combining the power of facial recognition Technology with the added security of OTP, this system ensures that only authorized individuals can access lockers.[1]
2. This paper presents hand gesture analysis for human-security system interaction. It evaluated an improved hand gesture recognition using web camera and successfully implemented a prototype for security in bank from robbery which is having a detection accuracy rate of 95.7%. [2]
3. In this paper the system will communicate the image data continuously to the remote location control rooms using web-based monitoring through local area network (LAN) and can also send the warning text short message service (SMS) to the operator using GSM technique.[3]
4. The primary aim of this paper is to provide a solution towards a complete biometric based authentication mechanism for operating the safety lockers. [4]

III. ACTUAL METHODOLOGY FOLLOWED



Level 1: A person will visit bank and request for permission to open a bank locker through a RFID tag reader. if identification is successful then asking for password.

Level 2: user has to enter 4 digit passwords first. If password match successfully then asking for next verification level. If password is wrong then alert SMS will be sending to owner mobile number.

Level 3: Admin of bank will grant permission in terms of OTP to the person. After putting OTP user will be authenticated. If not then again request will be send. [2-4]

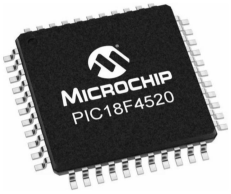
3.1 Impact of the project

In the development of the high protection bank locker security system using live image and voice authentication marks a significant stride in the realm of security technology. Through the integration of cutting-edge biometric features, such as live image and voice authentication, this system offers a robust defence mechanism against unauthorized access to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

bank lockers and other secure areas. By harnessing the power of biometric data, organizations can elevate their security posture and install confidence among customers and stakeholders regarding the safety of their assets.Moreover, the implementation of this security system underscores the importance of continuous innovation in addressing evolving security challenges. [1] As threats to security become increasingly sophisticated, it is imperative for organizations to stay ahead of the curve by adopting advanced security solutions that leverage emerging technologies. The high protection bank locker security system exemplifies this proactive approach by leveraging live image and voice authentication to provide a multi-layered defence against unauthorized access, thereby enhancing the overall security posture of banking institutions and other high-security environments. [2] Furthermore, the successful development and deployment of this security system highlight the potential for technology to transform traditional security paradigms and elevate security standards to new heights. By embracing innovation and investing in state-of-the-art security solutions, organizations can not only safeguard their assets and infrastructure but also enhance operational efficiency and customer satisfaction. As the threat landscape continues to evolve, the high protection bank locker security system stands as a testament to the power of technology to address complex security challenges and pave the way for a safer and more secure future. [5]

3.2 Explanation of components



A. PIC1814520 Microcontroller

- The Data Memory up to 4k bytesn Data register map with 12-bit address bus 000-FFF
- Divided into 256-byte banks
- There are total of F banks
- Half of bank 0 and half ofbank 15 form a virtual (oraccess) bank that is accessibleno matter which bank isselected-this selection isdone via 8-bits
- Program memory is 16-bits wide accessed through a separate program data bus and address bus inside the PIC18.
- Program memory stores the program and also static data in the system.
- On-chip program memory is either PROM or EEPROM
- The PROM version is called OTP (one-time programmable) (PIC18C) The EEPROM version is called Flash memory (PIC18F).
- Maximum size for program memory is 2M n Program memory addresses are 21-bit address starting at location 0x000000

B. Ultrasonic Sensor:

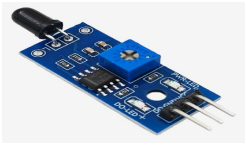
- Operating Voltage: 3V - 5V or 12V - 24V (depending on the model)
- Operating Frequency: Commonly 40 kHz
- Detection Range:
- Short-range: 2 cm to 400 cm (e.g., HC-SR04)
- Long-range: Up to 10 meters (industrial sensors)
- Accuracy: ±1 mm to ±3 mm

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

C. Heating sensor:-

Operating Voltage: 3.3V - 5V (for basic modules) or 12V - 24V (for industrial sensors)
Detection Range:
Basic sensors: 0.5m to 3m
Advanced sensors: Up to 100m (industrial applications)
Detection Angle: 60° to 120° (depending on the sensor type)

D. RFID Tag reader:-



Frequency Types:

- Low Frequency (LF) RFID: 125 kHz – 134 kHz
- High Frequency (HF) RFID: 13.56 MHz (e.g., NFC, MIFARE)
- Ultra High Frequency (UHF) RFID: 860 MHz – 960 MHz

Operating Voltage:

- 3.3V – 5V (for modules like RC522)
- 9V – 12V (for industrial RFID readers)

IV. RESULT

REFERENCES

[1] Guangyuan Zhao, Zhiwei Wang, Wei Li, Ke Wang, “An Embedded Laboratory Security Monitoring System”. 2011 Third International Conference on Measuring Technology and Mechatronics Automation.
[2] Basil Hamed, ‘‘Efficient Authorized Access Security System Control Using ATMEL 89C55 & Mobile Bluetooth”. International Journal of Computer Theory and Engineering, Vol. 4, No. 1, February 2012
[3] Sadeque Reza Khan, “Development of Low Cost Private Office Access Control System (OACS)”. International Journal of Embedded Systems and Applications (IJESA) Vol.2, No.2, June 2012.
[4] A.O. Oke, O.M. Olaniyi, O.T. Arulogun, and O.M. Olaniyan, “Development of a Microcontroller Controlled Security Door System”. The Pacific Journal of Science and Technology, Volume 10. Number 2. November 2009.
[5] Datasheet, ATMEGA16 - 8-Bit Microcontroller with 16K Bytes Flash -ATMEL Corporation [Online] .