International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology

Subhash H. Jadhav[1], S. S. Agrawal[2]

[1] Government College of Engineering, Department of Electronics and Telecommunication, Dr. B. A.M.University, Aurangabad, India

[2]Professor, Government College of Engineering, Department of Electronics and Telecommunication, Dr. B. A. M. University, Aurangabad, India

Abstract: ***The main goal of this project is to design and implement a highly secured and reliable smart bank locker security system based on RFID, Biometric fingerprint, password and GSM technology. This can be organized in bank, offices(treasury), schools and homes. In this system only the authentic person can open the lock and collect the important documents, jewellery or money from the lockers. In this security system RFID, biometric fingerprint, passwordand GSM technology systems are used. In our proposed system first the user will enroll his user name, password and his mobile number, then the person will put finger on finger print module and finger print will be scanned and stored with fingerprint id . In this way user enrolment process will be completed. Then user will perform login operation. During login operation user first swipe RFID tag on the RFID reader if it is ok then finger print of authentic person will be scanned. If the finger is correct of that particular person then it will allow and display finger is matched and if the finger is not matched of that particular person then it will gives the signal to the siren and will play some time and then message goes to the user that the unauthorized entry is there please check. And if the finger print is matched then it will gives the signal to do next step to enter the Password, then the authorized person will enter the password. If the password is incorrect then it will play siren and the system will send the message to the user i.e. the unauthorized person is trying to open the lock so please check it and so on, if all the conditions are matched then the microcontroller processes the data and correspondingly drives the motor to operate the load i.e. lock will be opened. The main advantages of using RFID, biometric fingerprint, password and GSM technology is highly secure and reliable locker system than any other locker systems. This system can also create a log containing check in and check out of each user along with basic information.***

Keywords: Fingerprint, RFID, Microcontroller, GSM technology

1. Introduction

In the real world, peoples are more concern about their safety for their valuable things like jewelry, money, important documents etc. So the bank lockers are the safest place to store them. The advent of fast growing technologies makes users to have high security systems with electronic identification options. These identification technologies include Bank Lockers and ATM as well as other intelligent cards, user IDs and password based systems, and so on. But, unfortunately these are unsecure due to hacker attacks, thefts, and forgotten passwords. In spite of all these shortcomings and malfunctions these systems are still prevailing; however, the biometric or fingerprint authentication based identification is the most efficient and reliable solution for stringent security.

We are implementingthis bank locker security system using RFID, biometric fingerprint , password and GSM Technology based security system which provide most efficient and reliable security system than the traditional system. An RFID system consists of an antenna or coil, a transceiver (with decoder) and a transponder (RF tag) electronically programmed with unique information. There are many different types of RFID systems in the market. These are categorized on the basis of their frequency ranges. Some of the most commonly used RFID kits are low frequency (30-300Khz) , mid frequency (900Khz-1500Mhz) and high frequency (2.4-2.5Ghz) . The passive tags are lighter and less expensive than the active tags. Biometrics measureindividual's unique physical or behavioral characteristics to recognize or authenticate their identity. The physical characteristics are fingerprint hand, face, iris etc. and behavioral characteristics are signature, voice keystroke patterns etc. Biometric system is operates in verification mode or identification mode. In the verification mode system validates person's identity by comparing the captured biometric template which is pre-stored in the system data base .In the identification mode the system recognize an individual by searching entire template data base for match. And the system is perform one to many comparisons to establish the individual identity or fails if the subject is not enrolled in the system data base. So in our project we are using fingerprint biometric security system. Global system for mobile communication (GSM) is mainly used for sending or receiving data such as voice and message .In our security system GSM plays important role. Through the use of GSM the user will get the message if an unauthorized person will try to open the lock. The fingerprint sensor used here is R305 sensor is having excellent performance, low power consumption, low cost, small in size. The ARMLPC2138microcontroller is used here because it performs multiple numbers of operations at a time. . we are using SIM900A GSM modem to send the message on authorized person mobile.

2. Literature Review

Name of the author: Sagar S. Palsodkar*, Prof S.B. Patil
Title: Biometric and GSM Security for Lockers
Publication: Int. Journal of Engineering Research and Applications
Concept about work: In this review paper we will develop biometric (finger or face) and GSM technology for bank

lockers. Because in this system bank will collect the biometric data of each person for accessing the lockers because in this system only authenticated person recover the money, documents from the lockers[1].

Advantages: As biometric and GSM security has been used hence more advantages then other system.

Limitations: As fingerprint or face biometric system is used then large data base is required

Name of the author: R.Ramani ,S. Selvaraju, S.Valarmathy, P Niranjan
Title: Bank Locker Security System based on RFID and GSM Technology
Publication: International Journal of Computer Applications
Concept about work: The main goal of this paper is to design and implement a bank locker security system based on RFID and GSM technology which can be organized in bank, secured offices and homes. In this system only authentic person can be recovered money from bank locker. The RFID reader reads the id number from passive tag and send to the microcontroller, if the id number is valid then microcontroller send the SMS request to the authenticated person mobile number, for the original password to open the bank locker, if the person send the password to the microcontroller, which will verify the passwords entered by the key board and received from authenticated mobile phone. if these two passwords are matched the locker will be opened otherwise it will be remain in locked position[2].
Advantages: This system is more secure than other systems because two passwords required for verification.
Limitations: As network signals are not available, then locker may not be opened

Name of the author: P. Sugapriya#1, K. Amsavalli#2
Title: Smart Banking Security System Using PatternAnalyzer
Publication: International Journal of Innovative Research in Computer and Communication Engineering
Concept about work: Initially pattern flow are collected as datasets and maintained in bank agent server. The machine has a camera to capture the pattern flow of user and sent for processing features of the logic were compared and user where recognized. In addition to the authentication of user there is another system to identify the user before that RFID tad checking is needed. Image processing is used and keypad password is needed for another level of security. In future bank can implement this type of authentication option for banking and from this projectshows that all the bank accounts can be accessed without using cards through this face recognition efficiently andsafely[3].
Advantages: Three level banking security is used.
Limitations: Time consuming method because huge datasets are require

Name of the author: Gayathri and Selvakumari
Title: Fingerprint and GSM based Security System.
Publication: International Journal of Engineering Sciences & ResearchTechnology.
Concept about work: Access control system forms a vital link in a security chain. The Fingerprint and password based security system presented here is an access control system that allows only authorizedpersons to access a restricted area. We have implemented a locker security system based on fingerprint, password andGSM technology containing door locking system which can activate, authenticate and validate the user and unlock thedoor in real time for locker secure[4].
Advantages: It will provide strong authentication key.
Limitations: It is time consuming.

Name of the author: Mary Lourde R and DushyantKhosla
Title: Fingerprint Identification in Biometric Security Systems.
Publication: International Journal of Computer and ElectricalEngineering
Concept about work: They says Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Among all the presently employed biometrictechniques, fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics. This paper deals with the issue of selection of an optimal algorithm for fingerprint matching in order to design a system that matches required specifications in performance and accuracy[5].
Advantages: Fingerprint identification systems have received the most attention due to the long history of fingerprints and their extensive use in forensics
Limitations: Only one biometric fingerprint authentication is used.

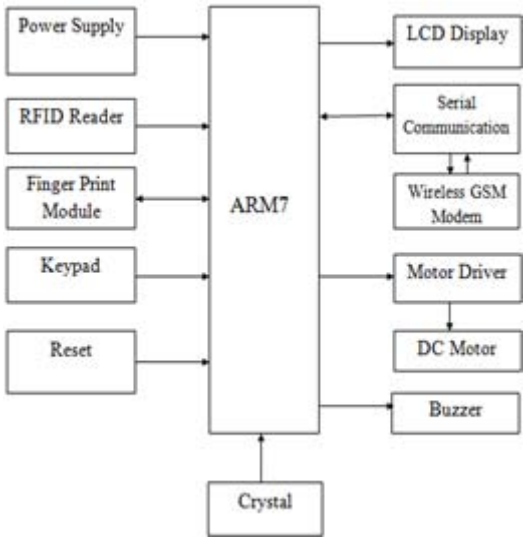
Name of the author: Pramila D Kamble and Dr. Bharti W. Gawali
Title: Fingerprint Verification of ATM Security System by Using Biometric and hybridization
Publication: International Journal of Scientific and Research Publications
Concept about work: The biometrics, fingerprint recognition is one of the most reliable and promising personal identification technologies. Fingerprints are the most widely used biometric feature for person identification and verification. But in this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability andhighaccuracy[6].
Advantages: Security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability andhigh accuracy.
Limitations: Suggestion only for ATM using only fingerprint with hybridization.

Name of the author: Ashish M. Jaiswal and MahipBartere
Title: Enhancing ATM Security Using Fingerprint And GSM Technology
Publication: International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014.
Concept about work: First person inserting card and he place finger in finger print module then 4 digit code will generate through GSM on person mobile and person will entered the code by pressing key on the touch screen then transition will done [7].
Advantages: It will provide strong authentication
Limitations: It is time consuming at initial stage

3. Proposed System

Here we are implementing a Smart Bank Locker security system using RFID, Biometric Fingerprint and GSM technology. RFID is a wireless technology of identifying objects with the help of radio waves. Main components of RFID are RFID tag and RFID reader. Locker account holder will have RFID tag which will contain information about bank locker holder like his name, locker number and id like information. Whenever user has to access locker, he has to first swipe RFID tag. If the tag is valid then LCD will display go to fingerprint scanner to put finger and if not match then message on LCD will be "please try again". If the finger is matched then user has to go through third security level of password and if finger is not matched then Buzzer will ON and signal goes to user/security person and message on LCD will be " unauthorized entry please check." User has to enter password through keypad. If the entered password is correct then locker will be opened. If the entered password is wrong then buzzer will be "ON" indicating unauthorized user is accessing the locker and signal goes to security person. All these activities are informed to user with the help of message through GSM technology. GSM is a second generation digital cellular mobile system used to send text messages, calling. GSM is also integrated to microcontroller to send message of activities. Thus here a simple and convenient three level security are used to protect bank locker security, using RFID tag, fingerprint biometric and then password. As three technologies are used it is highly secured and reliable system and easily available to users at affordable price. Also because of simple circuitry there is less maintenance. Besides this there are some limitations like user has to remember password also there might be time delay in delivery of message due to poor network.

4. Block Diagram



5. Workflow

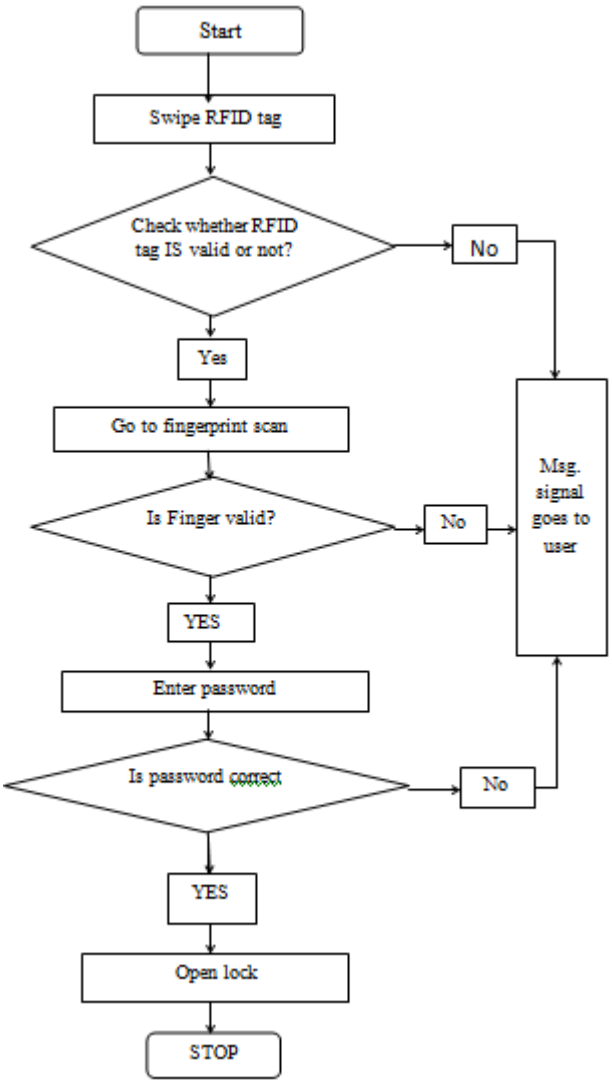


Figure: Flowchart

6. RFID (Radio Frequency Identification)

Radio-frequency identification (**RFID**) system uses radio frequency to identify, locate and track people, assets, and animals. Passive RFID systems are composed of three components– an interrogator (reader), a passive tag, and a host computer. The tag is composed of an antenna coil and a silicon chip that includes basic modulation circuitry and non-volatile memory. The tag is energized by a time-varying electromagnetic radio frequency (RF) wave that is transmitted by the reader. This RF signal is called a carrier signal. WhentheRF field passes throughan antenna coil, there is an A C voltage generated across the coil. This voltage is rectified to supply power to the tag. The information stored in the tag is transmitted back to the reader. This is often called back scattering. By detecting the back scattering signal, the information stored in the tag can be fully identified.[14]

Tags

A radio-frequency identification system uses *tags*, or labels attached to the objects to be identified. Two-way radio transmitter-receivers called interrogators or readers send a signal to the tag and read its response.RFID tags can be either passive , active or battery-assisted passive. An active tag has an on-board battery and periodically transmits

its ID signal. Active RFID tags have limited life spans A battery-assisted passive (BAP) has a small battery on board and is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery; instead, the tag uses the radio energy transmitted by the reader. However, to operate a passive tag, it must be illuminated with a power level roughly a thousand times stronger than for signal transmission. That makes a difference in interference and in exposure to radiation.Tags may either be read-only, having a factory-assigned serial number that is used as a key into a database, or may be read/write, where object-specific data can be written into the tag by the system user. Field programmable tags may be write-once, read-multiple; "blank" tags may be written with an electronic product code by the user.RFID tags contain at least two parts: an integrated circuit for storing and processing information, modulating and demodulating a radio-frequency (RF) signal, collecting DC power from the incident reader signal, and other specialized functions; and an antenna for receiving and transmitting the signal. The tag information is stored in a non-volatile memory. The RFID tag includes either fixed or programmable logic for processing the transmission and sensor data, respectively.

Readers

RFID systems can be classified by the type of tag and reader. A Passive Reader Active Tag (PRAT) system has a passive reader which only receives radio signals from active tags (battery operated, transmit only). The reception range of a PRAT system reader can be adjusted from 1–2,000 feet (0–600 m), allowing flexibility in applications such as asset protection and supervision.An Active Reader Passive Tag (ARPT) system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags.An Active Reader Active Tag (ARAT) system uses active tags awoken with an interrogator signal from the active reader. A variation of this system could also use a Battery-Assisted Passive (BAP) tag which acts like a passive tag but has a small battery to power the tag's return reporting signal.

7. Fingerprint

This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port.[4]

Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks, etc.The fingerprint sensor can be wired as below. Do not follow colour code of connector provided.

Figure 3.5: Connection of Fingerprint to Microcontroller

8. Working Principle of fingerprint

Fingerprint processing includes two parts, fingerprint enrolment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template. When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library.

For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

GSM Module

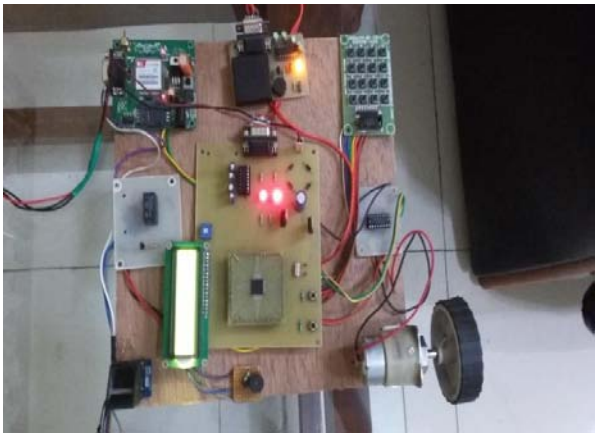
TTL –Modem is SIM900 Quad-band GSM device, works on frequencies 850 MHZ, 900 MHZ, 1800 MHZ and 1900 MHZ. It is very compact in size and easy to use. The Modem is designed with 3V3 and 5V DC TTL interfacing circuitry, which allows 3V3 Microcontrollers (ARM, ARM Cortex XX, etc.). The baud rate can be configurable from 9600-115200 bps through AT (Attention) commands. It is suitable for SMS as well as DATA transfer application in mobile phone to mobile phone interface. GSM MODEM is a class of wireless MODEM devices that are designed for communication of a computer with the GSM and GPRS network. It requires a SIM (Subscriber Identity Module) card just like mobile phones to activate communication with the network [1].

AT Commands

AT commands are used to control MODEMs. AT commands with a GSM MODEM or mobile phone can be used to access following information and services: Information and configuration pertaining to mobile device or MODEM and SIM card, SMS services, MMS services, Fax services, Data and Voice link over mobile network.

Hardware

Hardware implemented is as shown in the figure.



9. Observations

The following conditions are to be observed after implementing the project.

Steps	Event	Condition	Buzzer Condition	LCD/Mobile Display
01	Reset	System ON	Buzzer OFF	Condition OK
02	Swipe RFID tag	OK	Buzzer OFF	Welcome Mr. Sunil Card no. 00 go to Fingerprint
03	Swipe RFID tag	NOT OK	Buzzer ON	Unauthorized entry please try again .
04	Fingerprint	OK	Buzzer OFF	Finger found. Card no. 00. Please enter password.
05	Fingerprint	NOT OK	Buzzer ON	Wrong Finger please check .signal message goes to the security.
06	Enter password	OK	Buzzer OFF	Welcome Mr. Sunil. Lock is opening.
07	Enter password	NOT OK	Buzzer ON	Incorrect password please check., signal message goes to the security.

10. Conclusion

Thus, by implementing this Smart Bank locker security system project using RFID ,Fingerprint, password and GSM technology money, jewelry and any other important documents of a every citizen we can make at safe custody. Using this smart technology a authorized person can only open the lock and collect the money, jewelry and any other important documents. This is a low cost equipment, low in power consumption,compact in size, wide operating range, highly secured and reliable stand-alone unique system.

11. Applications

This project is used in following places: In all bank for Lockers, In all bank ATMs, In house, Schools treasury, Colleges treasury and in industries, VIP vehicles,in hospital, offices.Vehicle Security Applications.

12. Future Scope

In addition to this the future scope of this project is to develop smart bank Locker security system based on **"FACE", "IRIS and Retina"** Scanning for visual identification of the person.

References

[1] Sagar S. Palsodkar*, Prof S.B. Patil , "Review: Biometric and GSM Security for Lockers" Int. Journal of Engineering Research and Applications , Vol. 4, Issue 12(Part 6), December 2014.

[2] R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan , "Bank Locker Security System based on RFID and GSM Technology '', International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012

[3] P. Sugapriya#1, K. Amsavalli#2, "Smart Banking Security System Using PatternAnalyzer",International Journal of Innovative Research in Computer and Communication Engineering ,Vol.3, Special Issue 8, October 2015

[4] M.Gayathri, P.Selvakumari, R.Brindha "Fingerprint and GSM based Security System" International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[5] Mary Lourde R and DushyantKhosla "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and ElectricalEngineering, Vol. 2, No. 5, October, 2010

[6] Pramila D Kamble and Dr. Bharti W. Gawali "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[7] Ashish M. Jaiswal andMahipBartere "Enhancing ATM Security Using Fingerprint And GSM Technology", International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014

[8] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., "On line Ration card System by using RFID and Biometrics", International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

[9] 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 .

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

[11] M.P.Manjunath, P.M.Ram Kumar, Pradeep Kumar, NalajalaGopinath, Ms. Haripriya M.E, "NFC Based

Bank Locker System". International Journal of Engineering Trends and Technology (IJETT) – Volume23 Number 1- May 2015
[12] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication EngineeringVol. 4, Issue 7, July 2015
[13] 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.
[14] https://en.wikipedia.org/Radio-Freqency-Identification#tags.