ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Fingerprint and GSM based Security System

M.Gayathri[*1], P.Selvakumari[2], R.Brindha[3]
[*1,2,3] Department of Electronics and Communication, mCommunication systems, Sri Shakthi Institute Of Engineering And Technology , Coimbatore, India
gayathrimohan27@gmail.com

Abstract

The main purpose of this paper is to design and implement high security system. Security is a prime concern in our day-to-day life. Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. 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 authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate, and validate the user and unlock the door in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This high security system based on fingerprint, password and GSM technology which can be organized in bank, secured offices and homes.

Keywords: Fingerprint matching, GSM , Random number, Microcontroller.

Introduction

The technological advancement in the field of electronics and telecommunication has brought more and more arrangements in the domestic and industrial environment. security systems can avoid the unauthorized entry of peoples into the protected area and it stores the details about the authorized peopled entered in the area on the computer through a wireless transmitter. Up gradations in this system can be done easily to improve the efficiency of the system. Security systems are the demands of the day, which helps to avoid theft and avoids unauthorized entry of peoples into the restricted area.Conventional security systems used either *knowledge based methods* (passwords or PIN), and *token-based methods* (passport, driver license, ID card) and were prone to fraud because PIN numbers could be forgotten or hacked and the tokens could be lost, duplicated or stolen. To address the need for robust, reliable, and foolproof personal identification, authentication systems will necessarily require a biometric component. Personal Safes are revolutionary locking storage cases that open with just the touch of your finger. These products are designed as secure storage for medications, jewelry, weapons, documents, and other valuable or potentially harmful items. These utilize fingerprint recognition technology to allow access to only those whose fingerprints you choose. It contains all the necessary electronics to allow you to store, delete, and verify fingerprints with just the touch of a button. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since there are no keys or combinations to be copied or stolen, or locks that can be picked. Galton [1] defined a set of features for fingerprint identification, which since then, has been refined to include additional types of fingerprint features. This powerful device uses the latest in fingerprint ID scan technology to make sure only authorized drivers with enrolled fingerprints can enter[6].

This primary (+ secondary) security system uses a combination of an enrolled Fingerprint plus the random number as a key to enable the process. A system is secured here by a password and finger print. A Finger print Scanner is used to store and read a particular Finger Print. Biometric fingerprint security has practical applications which can be used to help protect security or privacy concerns on a personal level. For example, fingerprint scanners and locking systems are designed to prevent unauthorized access to your personal data or information. Global system for mobile communication is mainly used for sending or receiving data such as voice and message. In this security system GSM plays a important role.

ISSN: 2277-9655
Impact Factor: 1.852

Through the use of GSM the user can receive random number. This random number can be used as password, this also another security for system. The rest of the paper is organized as follows: Section II briefly review related work. In section III describes the proposed system, IV describes block diagram and then following section describes hardware parts and the software final section includes conclusion and future work.

Related Work

In this section some related works are discussed below.The purpose of this project is to increase the security that customer use the ATM machine. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer, so to rectify this problem we are implementing this project. The fingerprint sensor used here is SM630. SM630 integrated fingerprint verification module is the latest release of Miaxis Biometrics Co., Ltd. It consists of optical fingerprint sensor, high performance DSP processor and Flash. It boasts of functions such as fingerprint enrollment, fingerprint deletion, fingerprint verification, fingerprint upload, fingerprint download, etc. The microcontroller used here is arduino board. The Arduino Uno is a microcontroller board based on the ATmega328. In this system both finger and password are used for security system. The password is a random number, so same password cannot used. Each time the user receive different password. The random number can be generated each the fingerprint of the user is matched and this number will be sent to user's mobile via GSM.

Proposed System

The existing security system either based on fingerprint or PIN number. Fingerprint alone has some failure for security system. In case of PIN number based security system, same PIN number is used again and again. Anybody can hack the PIN number. This security system also has some disadvantage.

The proposed system is based on both fingerprint and GSM based. In this system, when the fingerprint is applied in the machine, it asks for finger print. If the finger print of the user is verified, further process can be processed otherwise LCD will display like " NO VALID ID" and buzzer will get alarmed .If the fingerprint is verified, then the user will get password immediately for the further process through GSM Modem. The user will process with the help of that Password. LCD Display is used to display the information about the system. For every time we will receive different random number as a password to our mobile[5].

Block Diagram

The block diagram consist of fingerprint sensor, LCD, arduino board and GSM. The fingerprint sensor and GSM modem connected to the arduino which serves as a client and server for the system. Once we give the fingerprint in the sensor the image of finger gets stored by having an address ID. By this process we can add more fingerprints in different address ID.

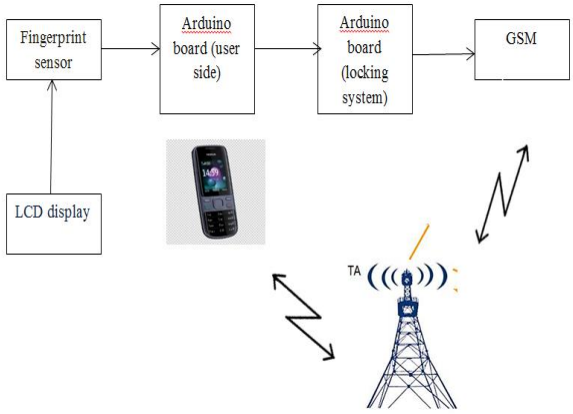

Fig 1. Overall block diagram

when we give the fingerprint in the sensor it will search for the corresponding address in the server. if the fingerprint is matched the user will get a random number as a password in his mobile through GSM modem which is connected with the arduino.by using that random number user can access the system[4].

Fingerprint Sensor

Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern [7].

These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies [2].

The three basic patterns of fingerprint ridges are the arch, loop, and whorl.

Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.

Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.

ISSN: 2277-9655
Impact Factor: 1.852

Whorl: Ridges form circularly around a central point on the finger.

Fingerprint sensor used here is SM630. Function includes fingerprint enrollment, image processing, minutiae extraction, templates storage, fingerprint verification (1:1) or fingerprint searching (1:N) under the command of HOST(PC or MCU). Sensor operating at voltage of 4.3V～6V and rating voltage is 6.5V exceeding this value will cause permanent damage. operating current will be less than 80mA.it has 768 templates.

A.Features

***Self-proprietary Intellectual Property*:** Optical fingerprint collection device, module hardware and fingerprint algorithm are all self developed by Miaxis.

High Adaptation to Fingerprints: When reading fingerprint images, it has self-adaptive parameter adjustment mechanism, which improves imaging quality for both dry and wet fingers. It can be applied to wider public.

Low Cost: Module adopts Miaxis' optical fingerprint collection device, which dramatically lowers the overall cost.

Algorithm with Excellent Performance: SM630 module algorithm is specially designed according to the image generation theory of the optical fingerprint collection device. It has excellent correction &tolerance to deformed and poor-quality fingerprint.

Easy to Use and Expand: User does not have to have professional know-how in fingerprint verification. User can easily develop powerful fingerprint verification application systems based on the rich collection of controlling command provided by SM630 module. All the commands are simple, practical and easy for development.

Low Power Consumption: Operation current <80mA, specially good for battery power occasions.

Integrated Design: Fingerprint processing components and fingerprint collection components are integrated in the same module. The size is small. And there are only 4 cables connecting with HOST, much easier for installation and use.

Perfect Technical Support: Miaxis is the leading company in the fingerprint verification industry. It has an excellent customer service team ready to offer powerful technical support in user development.

Fig 2. Fingerprint sensor SM630

ARDUINO UNO

The Arduino Uno is a microcontroller board based on the ATmega328 . It has 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started.

The Uno differs from all preceding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to-serial converter. "Uno" means one in Italian and is named to mark the upcoming release of Arduino 1.0. The Uno and version 1.0 will be the reference versions of Arduino, moving forward.

Fig. 3.ARDUINO UNO

The Arduino Uno can be powered via the USB connection or with an external power supply. The power source is selected automatically.The board can

ISSN: 2277-9655
Impact Factor: 1.852

operate on an external supply of 6 to 20 volts. If supplied with less than 7V, however, the 5V pin may supply less than five volts and the board may be unstable. If using more than 12V, the voltage regulator may overheat and damage the board. The recommended range is 7 to 12 volts.

GSM Modem

A GSM modem is a wireless modem that works with a GSM wireless network. A wireless modem behaves like a dial-up modem. The main difference between them is that a dial-up modem sends and receives data through a fixed telephone line while a wireless modem sends and receives data through radio waves. A GSM modem can be an external device or a PC Card / PCMCIA Card. Typically, an external GSM modem is connected to a computer through a serial cable or a USB cable. Like a GSM mobile phone, a GSM modem requires a SIM card from a wireless carrier in order to operate.

***Operations*:**

- Reading, writing and deleting SMS messages.
- Sending SMS messages.
- Monitoring the signal strength.
- Monitoring the charging status and charge level of the battery.
- Reading, writing and searching phone book entries.

Here advanced low cost SIMCOM 300 modem is used for sending and receiving text message. Features include

- Works on frequencies EGSM 900 MHz, DCS 1800 MHz and PCS 1900 MHz
- SIM300 features GPRS multi-slot class 10/ class 8 (optional) and supports the GPRS coding scheme.
- CS-1, CS-2, CS-3 and CS-4.With a tiny configuration of 40mm x 33mm x 2.85mm ,
- SIM300 can fit almost all the space requirements in your applications, such as smart phone, PDA phone and other mobile devices
- This GSM modem is a highly flexible plug and play quad band GSM modem for direct and easy integration to RS232.
- Supports features like Voice, Data/Fax, SMS, GPRS and integrated TCP/IP stack.
- Control via AT commands(GSM 07.07,07.05 and enhanced AT commands)

Fig 4. GSM modem

- Use AC – DC Power Adaptor with following ratings · DC Voltage : 12V /1A
- Current Consumption in normal operation 250mA, can rise up to 1Amp while transmission.

Communication

During USB communication data is transmitted as packets. Initially, all packets are sent from the host, via the root hub and possibly more hubs, to devices. Some of those packets direct a device to send some packets in reply.After the sync field, all packets are made of 8-bit bytes, transmitted least-significant bit first. The first byte is a packet identifier (PID) byte. The PID is actually 4 bits; the byte consists of the 4-bit PID followed by its bitwise complement. This redundancy helps detect errors. (Note also that a PID byte contains at most four consecutive 1 bits, and thus never needs bit-stuffing, even when combined with the final 1 bit in the sync byte. However, trailing 1 bits in the PID may require bit-stuffing within the first few bits of the payload.)

This is a very useful and convenient data / charging cable for all the devices with mini USB 5-pin port. The universal USB 2.0 to mini USB 5-pin cable is perfect for your devices to transfer data or charge. It is a great USB 2.0 male to mini 5-pin male cable to replace the damaged one.

Software Program Testing

Installing drivers for the Arduino Uno with Windows7, Vista, or XP:

- Plug in your board and wait for Windows to begin it's driver installation process. After a few moments, the process will fail, despite its best efforts
- Click on the Start Menu, and open up the Control Panel.

ISSN: 2277-9655
Impact Factor: 1.852

- While in the Control Panel, navigate to System and Security. Next, click on System. Once the System window is up, open the Device Manager.
- Look under Ports (COM & LPT). You should see an open port named "Arduino UNO (COMxx)"
- Right click on the "Arduino UNO (COmxx)" port and choose the "Update Driver Software" option.
- Next, choose the "Browse my computer for Driver software" option.
- Finally, navigate to and select the Uno's driver file, named "**ArduinoUNO.inf**", located in the "Drivers" folder of the Arduino Software download (not the "FTDI USB Drivers" sub-directory).
- Windows will finish up the driver installation from there.

After installation is completed ,programmer writes the program using C language and upload the program to board once the compilation is finished[4].

Hardware Implementation

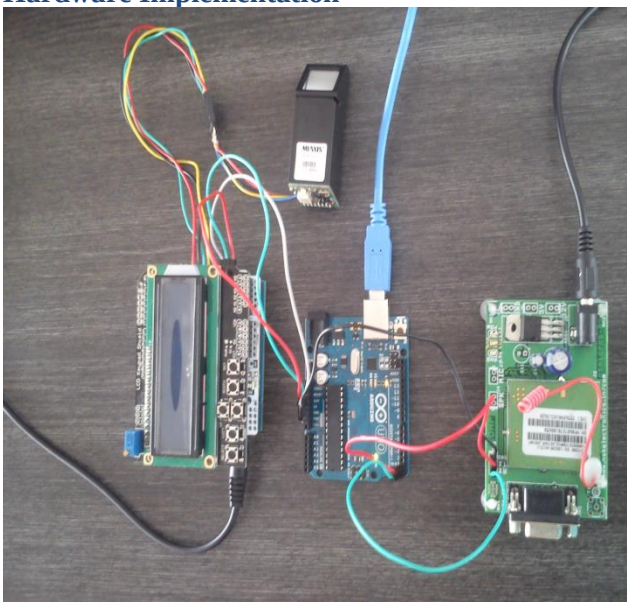

Fig 5. Overall setup

Fingerprint sensor and the arduino which is attached with LCD is connected and act as the user side system. Another arduino is connected to GSM modem. Both arduino and GSM is powered via power card. Fingerprint is already stored, every time we give fingerprint the comparison takes place and then if the fingerprint is matched means we get random number as a password in mobile through GSM.

Conclusion and Futurework

In this project we have implemented finger print techniques that can provide the high level security in areas such as home, office, bank etc., This project identifies a high level model for the modification of existing security systems using both security protocols as PIN & fingerprint strategy. Thus we designed the security terminal based on finger print recognition.

We have decided to develop a fingerprint mechanism to enhance the security features of the ATM for effective banking transaction for Indian banking system[3]. By using Intranet connection we can modify this security system as the ATM so that user can access ATM without the cards.This system when fully developed will definitely reduce the rate of fraudulent activities on the ATM machines such that only the registered owner of a card access to the bank account.

Acknowledgment

First and foremost, we wish to express our deep gratitude and indebtness to our institution and our department for providing us a chance to fulfill our long cherished of becoming Electronics and Communication engineers.

We wish to acknowledge with thanks the excellent encouragement given by the management of our college .We wish to express our hearty thanks to the Principal of our college and HOD. We are committed to place our heartfelt thanks to all teaching and supporting staff members, lab technicians and friends, and all the noble hearts that gave us immense encouragement towards the completion of our project. Finally we thank almighty for bestowing the gifts of life on us and also for providing us the necessary help through his lovely creations in this endeavor of us.

References

[1] Galton, F. Fingerprints. Mcmillan, 1982.

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

[3] Pramila D. Kamble, 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.

[4] V.Ramya1, B. Palaniappan, V.Sumathi, "Gsm Based Embedded System For Remote Laboratory Safety Monitoring And Alerting",

ISSN: 2277-9655
Impact Factor: 1.852

International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.6, November 2012

[5] Art Conklin1, Glenn Dietrich2, Diane Walz3,"Password-Based Authentication: A System Perspective", Proceedings of the 37th Hawaii International Conference on System Sciences –2004.

[6] Hugh Wimberly, Lorie M. Liebrock, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study", 2011 IEEE Symposium on Security and Privacy.

[7] http://biometrics.cse.msu.edu/fingerprint.html