IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Security System for Money Transaction that Avoid Stealing of Password

K.Armaan Ali[1],S.Surendiran[2] and S.Sarathkumar[3]

[1,2,3] **Department of Information Technology,Adhiparasakthi Engineering College, Melmaruvathur-603319, Tamil Nadu, India.**

Abstract

The aim of this project is to develop a system used for ATM security operations.Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. The security that is being currently used for ATM indeed has a few backdoors and it can be improved further. Using credit card and password, client's identity cannot be verified exactly. For the same reason biometric verification were introduced. Biometrics can be defined as the sense of organ and technology biological data. They identify the physiological and / or behavioral characteristics that can be utilized to verify the identity of an individual. Of the various existing biometric technologies finger print based recognition is found to be more secure. In the recent years the finger print recognition is updated to a certain extent. In this system, bankers will collect the customer finger prints and mobile number while opening the account. These details will be stored in a Smart card which will be used by the user to make transactions in the ATM machine. The customer has to insert the smart card in the ATM machine and then place his finger on the finger print module. The finger print is verified with the one stored in the smart card. If both the finger prints are identical then it generates a random 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer should be used as a password for further transactions. Otherwise it will send an alert message to the user and the banker. Even if someone stole the ATM card he can do nothing with that because he need the finger print and mobile phone of the user.

Keywords:*Smart card,Fingerprint,ATM ,Mobile, Random password.*

1. Introduction

In this modern world Automatic Teller Machine (ATM) is being used by many of us.Self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. The ATM provides customers with the convenient banknote trading. However, the financial crime case rises repeatedly in recent years. A lot of criminals tamper with the ATM terminal and steal user's credit card and password by an illegal method. If user's ATM card is lost and the password known by anyone, the criminal will draw allthe amount in the shortest period, which will bring huge economical loss to the customer. In some cases hacking methods are also used to find out the password of the user without the knowledge of the user. Hence it is necessary to go for an alternate method to make the banking more secure against such criminals and hacking.

2. The Primary Functions of the System

The embedded ATM client authentication system is based on fingerprint recognition which is designed after analyzed existed ATM system. The S3C2440 chip is used as the core of these embedded systems which is associated with the technologies of fingerprint recognition and current high speed network communication.The primary functions are:

2.1 Fingerprint recognition:

The masters' fingerprint information was used as the standards of identification. It must certify the human fingerprint before using ATM system.

2.2 Smart card:

A special smart card will be provide to the user which he will use instead of ATM card that contains his finger print and mobile number for future authentication.

2.3 Message alarming:

Different 4-digit code is given as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.

2.4 Two discriminate analysis methods:

Besides the fingerprint recognition, the password validation can be also used for the system. Thus the system can be highly protected if we use two discriminate analysis methods.

3. Hardware Design

The design of entire system consisted of two part which are hardware and software. The hardware are designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are:
The S3C2440 chip is used as the core of whole hardware. Moreover, the modules of display, keyboard, fingerprint recognition are connected with the main chip (S3C2440). The SRAM and FLASH are also embedded in the system.

3.1 SRAM and FLASH:

The 16-bit 29LV160BB- 70REC of FLASH chip and the 32-bit HY57V561620CT-6 of SRAM chip are connected with the main chip. Their functions are to store the current code, and also to store the information of fingerprint and the mobile number.

3.2 LCD module:

The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 image of 15 gray-scale or 3375 colours.

3.3 Keyboard module:

It can be used for inputting passwords.

3.4 Fingerprint recognition module:

Fingerprint recognition can be done by Atmel Company's AT77CI04B. The features are 500dpi resolution, anti-press, anti-static, anticorrosion.

3.5 Ethernet switch controller:

RTL8308B can provides eight 10/100 Mbps RMII Ethernet ports, which can connect remote fingerprint data server.

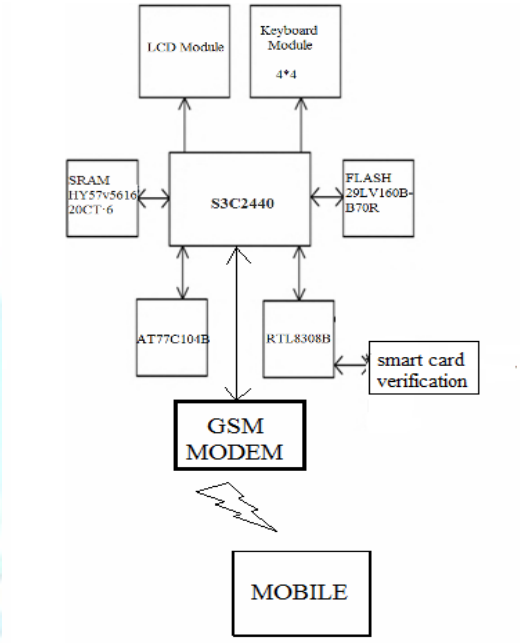

Fig.1Hardware Design

Before using the ATM terminal, the client's fingerprint feature will be connected to the smart card to match fingerprint data with the original data, if the result is incorrect, the system will generate an error message in the system itself. If the information is again is incorrect then it will automatically block the smart card and send alarm to the credit card owner and bank.

4. Software Design

The design consists of three parts that includes the design based on main program flow chart, the initializing ones, and the algorithm of fingerprint recognition flow chart.
This system of software is implemented by the steps as follows: Initially, the Kernel of Linux OS and the File system are loaded into the main chip. Then the system is to implement specific goal, such as verifying both ATM and GSM system, and then finally each module retune for ready to run commands. Before accessing the ATM system, the mobile number and fingerprint of the customer is required. First the system is required the card holder's fingerprint. If he success in this

authentication, the system would send the password to the Account holder and he will enter the same password in touch screen for accessing the ATM Terminal. If the Authentication fails then it send the alert message to the Account holder and Bank. The overall flow chart of software is shown in fig. 2.

In the process of user providing the fingerprint, the AT77CI04B captures fingerprint images by sweeping the finger over the target area, will used for capturing the true image of fingerprint. This product embeds true hardware based 8-way navigation and click functions. The fingerprint information will be temporarily stored in SRAM and upload to the remote finger data server to compare through bank network. The result of process will be controlled by main chip (S3C2440).

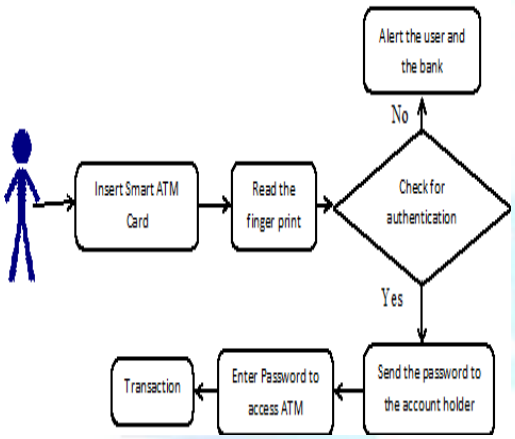

Fig.2 The flowchart of the Software design

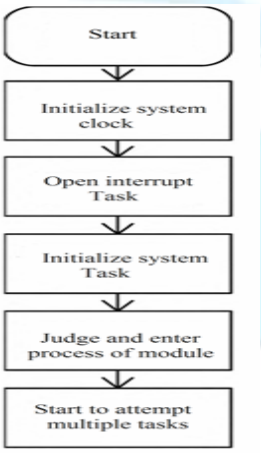

Fig.3 The flow chart of fingerprint recognition

The initializing process means that set the hardware and software and then starts the multiple mission modules, every module will be initiated according to the priority processes. At first, initialize the system clock, and execute the corresponding codes of open interrupt and the open interrupt task. Then, the system would decide and enter process of module. Finally, the system would start to attempt multiple tasks. The initializing flow chart is shown in fig. 3.

4.1The design of fingerprint recognition algorithm:

The design of algorithm based on fingerprint recognition is so vital for the entire system. We approach two steps to process the fingerprint image.

4.1.1 The detail of fingerprint recognition process

The first step was the acquisition of fingerprint image by the algorithm that mentioned above, and the results will be sent to the next process. Secondly, pre-processing the images are captured. After capturing the fingerprint image, it must be pre-processing. Generally, pre-processing of one's is filtering, histogram calculating, digital photographs and image binarization. Finally, the characteristics value was seperated, and the results of the above identifies would be compared with the information of owner's fingerprint in the smart card so as to verify whether the character is matched, and then the system display the results matched or not.

4.1.2 The design of fingerprint image enhancement

Fingerprint recognition module is an extremely important part of the system, the very high-quality images was the major factors of influencing the performance in the system. The algorithm of fingerprint recognition based on the algorithm of Gabor and direction filter was used. Fingerprint enrichment algorithm based on Gabor filter could be better to avoid noise and strengthen the definition between the ridge and valley, it could significantly improve the image enhancement processing capacity, but this algorithm was slow in dealing with the high capacity requirements.

5. GSM

Global System for Mobile Communications (GSM: originally from Group Special Mobile) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that 82% of

the global mobile market uses the standard GSM is used by over 2 billion people across more than 212 countries and territories. GSM differs from its predecessors in that both signaling and speech channels are digital call quality, and thus is considered a second generation (2G) mobile phone system. This has also meant that data communication was built into the system using the 3rd Generation Partnership Project (3GPP). GSM also pioneered a low-cost alternative to voice calls, the Short message service. GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world.
GSM uses a variation of Time Division Multiple Access (TDMA) and GSM is the most widely used of the three digital wireless telephone technologies (TDMA, GSM, and CDMA). GSM digitizers and compresses data , then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1,800 MHz frequency band. GSM is the de facto wireless telephone standard in Europe. GSM has over one billion users worldwide and is available in 190 countries.

5.1. Technical details:

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americans (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated. The rarer 400 and 450 MHz frequency bands are assigned in some countries, notably Scandinavia, where these frequencies were previously used for first-generation systems.

5.2. The Future of GSM

GSM together with other technologies is part of an evolution of wireless mobile telecommunication that includes High-Speed Circuit-Switched Data (DSCSD), General Packet Radio System (GPRS), Enhanced Data rate for GSM Evolution (EDGE), and Universal Mobile Telecommunications Service (UMTS).

6. Advantages

Using this system the people can take the amount from the ATM with high security. This system provides high security against key logging, shoulder surfing, dictionary attack. Even if the card has been stolen, the thief cannot do anything with that.

7. Result& Conclusion

The Implementation of ATM security by using fingerprint recognition and GSM MODEM took advantages of the stability and reliability of fingerprint characteristics. Additionally, the system also contains the original verifying method which was inputting owner's password which is send by the controller. The security features were intensifying largely for the stability and reliability of owner recognition. The whole system was built on the technology of embedded system which makes the system more safe, reliable and easy to use, which also provides enhanced security to the end users.

References

[1] Mr. Pennamkrishnamurthy,Mr. M. Maddhusudhanredddy Implementation of ATM Security by Using Fingerprint recognition and GSM
[2] Santhi.b, Ram kumar.kNovel hybrid technology in atm security using Biometrics
[3]Whe Dar Lin “A mobile-based marketing information management system”
[4] Lawan Ahmed Mohammed “Use of biometrics to tackle ATM fraud”.