International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 12
ISSN: 2454-4248
67 – 71

Emergency Mode for ATM Security by using Biometric Recognition and GSM Technology

Prof. Prashant Gadakh[1], Prof. Malayaj Kumar[2],
International Institute of Information Technology, Pune

Abstract: - Now a day there is an urgent need to improve security in banking region. The foremost objective of this system is to develop an embedded system, which is used for ATM system security application. With the advent of ATM though banking became a lot easier it even became a lot vulnerable or susceptible. Today, ATM is nothing more than Access Card and Personal Identification Number (PIN) for identification and security clearness. This kind of situation is unfortunate is unfortunate since tremendous progress has been made in biometric identification techniques, such as finger printing, retina scanning, facial recognition, iris scanning etc. This paper proposes the development of a system that integrates fingerprint recognition technology and GSM technology into the identify verification process used in ATMs. The development of such a system helps to protect consumers and financial institutions alike from fraud security. In this, Bankers has to collect the customer's finger prints and mobile number while opening the accounts then customer only access the ATM machine. The working of these ATM machine is when customer place finger on finger print module when it access automatically generates every time different 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 entered by customer then only customer can access his account.

Keywords:-*ATM terminal; Fingerprint recognition; Image enhancement; PIN; Security; Biometric; GSM MODEM.*

******

I. INTRODUCTION

The rise of various technologies in India has brought into force many types of equipment that aim at more customer satisfaction. Now-a-days in the self-service banking system has got extensive popularization with the characteristics offering high-quality 24 hours service for customers. One technology which is used in banking that has impacted positively and negatively to banking activities and transactions is the Automated Teller Machine (ATM). With an ATM a customer is able to conduct a several banking activities such as cash withdrawal, money transfer, paying phone and electricity bill beyond official hours and physical interaction with bank staff. Personal Identification Number (PIN) or password is one important aspect in ATM security system [1]. An ATM is mechanical system that has its root embedded in the accounts and records of banking institution [1]-[2]. It is computerized machine designed to deal out cash to bank customers without need of human interaction; it can transfer money between bank account and provide other basic financial services, such as balance enquiry, withdrawal etc. [3].

Using credit card and password, system cannot verify the client's identity exactly. In recent years, the algorithm that the fingerprint recognition continuously updated and sending the four digit code by the controller which has offered new verification means for us, the original password identification technology verify the clients' identity better and achieve the purpose that use of ATM machines improve the safety effectively [4].

II. SURVEY AND DISCUSSION

Onyesolu and Ezeani analysed the profile of participant which is shown in Table I. The range of participant was 20-53 years, 85 males and 78 females took part in the study [5].

No.	Profile	Description
1	Age	20-53 years old
2	Sex (Male: Female)	85:78
3	Bank account and ATM card	Depend on customer

Table I. Profile of participants.

Each of the participants own at least one type of bank account. This depended on the bank, the products offered and services provided by the bank.

Table II shows the use and reliability of ATM, 139 participants representing some customers and staffs of some bank, representing 85% of the population use the ATM while 15% of the population is yet to use the ATM. This 15% of the population is still having doubt about using ATM because of the issues and security associated with it. Such issues as inability of the machine to return a customer's card after transaction which may take days to rectify, debiting a customer's account in a transaction even when the customer is not paid and cash not dispensed, and "out of service" usually displayed by the machine whichmost of the time is disappointing and frustrating among others. 100% of the population is aware of one form of ATM fraud or another [5].

 ISSN: 2454-4248
67 – 71

No.	Question	Responses		Total	Percentage (%)	
		Yes	No		Yes	No
1	Do you use ATM?	139	24	163	85	15
2	Is password (PIN) secured in using ATM?	60	103	163	37	63
3	How long you been using ATM?			163		
	a. Less than a year	23			14	
	b. Greater than one year but less than 3 years	37			23	
	c. More than 3 years	103			63	
4	Have you ever heard of any ATM fraud?	163	00	163	100	00
5	Is anything being done about ATM fraud?	150	13	163	92	08
6	Are ATM transactions becoming especially risky?	145	18	163	89	11
7	Will you discontinue the use of ATM because of the security issues associated with it?	152	11	163	93	07
8	Would you prefer a third level security aside card and PIN?	163	00	163	100	00
9	Have you heard of biometrics as a means of authentication?	143	20	163	88	12
10	Have you heard of GSM MODEM/TECHNOLOGY as a means of authentication?	137	26	163	84	16
11	Do you think the use of biometric and GSM can improve ATM security?	163	00	163	100	00

Table II. Use and Reliability of ATM

No.	Question	Biometric Characteristic	Responses	Percentage (%)
1	Which of these biometric characteristics have you heard of?	a. Fingerprint	120	74
		b. Iris	9	06
		c. Face Recognition	7 12	04 07
		d. Signature	2	01
		e. DNA	8	05
		f. Retina	5	03
		g. Voice		
		Total	163	100
2	Which of the biometrics characteristic will provide better security when integrate with ATM along with GSM Technology?	a. Fingerprint	101	62
		b. Iris	13	08
		c. Face Recognition	9 12	06 07
		d. Signature	12	07
		e. DNA	9	06
		f. Retina	7	04
		g. Voice		
		Total	163	100

Table III. Reliability of Biometric Characteristics

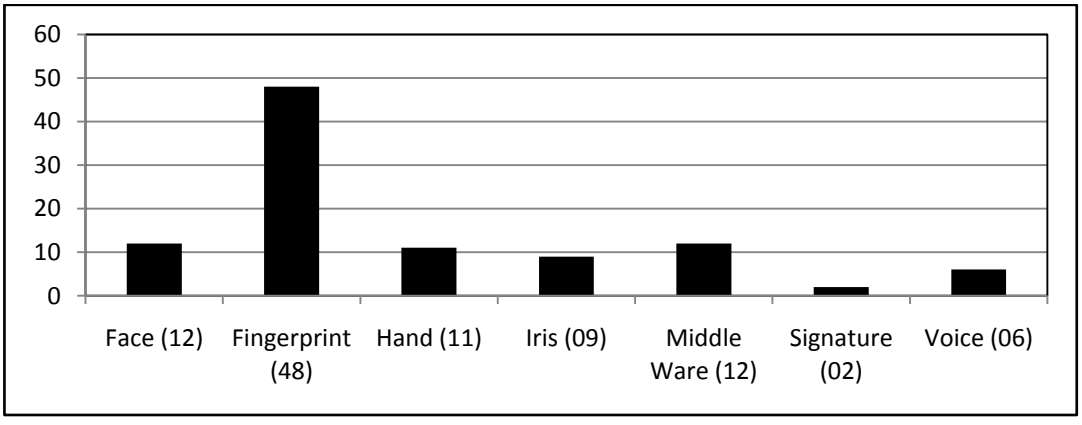

Fig1. Comparative survey of fingerprint with other biometrics.

 ISSN: 2454-4248
67 – 71

Table III shows the reliability and popularity of fingerprint biometric technology. 73% of the population is familiar with fingerprint biometric. 63% of the population strongly believed that with incorporation of fingerprint to the existing ATM card and PIN integrated with GSM MODEM, will provide a better security to the ATM.

III. FINGERPRINT BIOMETRICS

The use of fingerprints as biometric is both the oldest mode of computer-aided, personal identification and the most prevalent in use today.

In today's era, fingerprint is one of the essential variables used for enforcing security and maintaining a reliable identification of any individual. Fingerprints are used as variables of security during voting, examinations, operation of bank accounts among others. The result of the survey conducted by the International Biometric Group (IBG) in 2004 on comparative analysis of fingerprint with other biometrics is presented in Fig. 1.

The result shows that a substantial margin exists between the uses of fingerprint for identification over other biometrics such as face, hand, iris, voice, signature, and middleware [6].

References [7]-[10] adduced the following reasons to the wide use and acceptability of fingerprints for enforcing or controlling security:

a. Fingerprints have a wide variation since no two people have identical prints.
b. There is high degree of consistency in fingerprints. A person's fingerprints may change in scale but not in relative appearance, which is not the case in other biometrics.
c. Fingerprints are left each time the finger contacts a surface.
d. Availability of small and inexpensive fingerprint captures devices.
e. Availability of fast computing hardware.
f. Availability of high recognition rate and speed devices that meet the needs of many applications.
g. The explosive growth of network and Internet transactions.
h. The heightened awareness of the need for ease-of-use as an essential component of reliable security.

IV. THE CHARACTERISTICS OF SYSTEM DESIGN

The proposed system is based on fingerprint recognition which is designed after analyzed existed ATM system. The S3C2440 chip is used as the core of this system which is associated with the technologies of fingerprint recognition and current high speed network communication.
The primary functions are shown as follows:

- Fingerprint recognition: The masters' fingerprint information was used as the standards of identification. It certifies the features of the human fingerprint before using ATM system.
- Remote authentication: System can compare current client's fingerprint information with remote fingerprint data server.
- Message alarming: different 4-digit code as a message to the mobile of the authorized customer without any noise, in order to access the Terminal.
- Two discriminate analysis methods: Besides the fingerprint recognition, the mode of password recognition can be also used for the system.

•GSM Modem: The working of these ATM machine is when customer place finger on the finger print module when it access automatically generates every time different 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 entered by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access.

V. HARDWARE DESIGN AND SOFTWARE DESIGN

The design of entire system consisted of two part which are hardware and software. The hardware is designed by the rules of embedded system, and the steps of software consisted of three parts. The more details are shown as follows.

A. HARDWARE DESIGN

The S3C2440 chip is used as the core of entire hardware. Furthermore, the modules of LCD, keyboard, alarm, fingerprint recognition are connected with the main chip (S3C2440).The SRAM and FLASH are also embodied in the system. There are some modules consisted of the system as follows:

• LCD module: The OMAP5910 is used in this module as a LCD controller, it supported 1024*1024 images of 15 gray-scale or 3375 colours.
• Keyboard module: It can be used for inputting passwords. • 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 storing the running code, the information of fingerprint and the algorithm.
• Fingerprint recognition module: Atmel Company's AT77CI04B be used as fingerprint recognition. It has a 500dpi resolution, anti-press, anti-static, anticorrosion.
• Ethernet switch controller: RTL8308B can provides eight 10/100 Mbps RMII Ethernet ports, which can connect police network and remote fingerprint data server.

 ISSN: 2454-4248
67 – 71

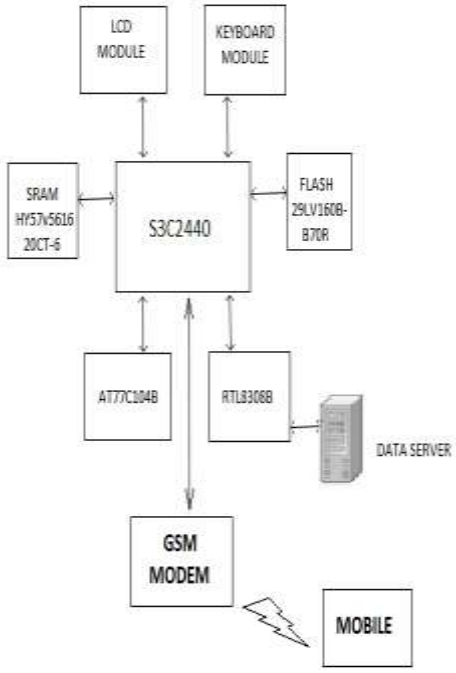

Fig2. The block diagram of hardware.

Before using the ATM terminal, the client's fingerprint feature will be connected to the remote fingerprint data server to match fingerprint data with the master's, if the result isn't correct, the system will call police automatically and send alarm to the credit card owner. The block diagram of hardware design is shown in Fig2.

B. SOFTWARE DESIGN

The design was component of three parts included the design of 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: first of all, the Linux kernel and the File system are loaded into the main chip. The next, the system is initialized to implement specific task, such as checking ATM system, GSM communication and so on, and then each module reset for ready to run commands. Before using ATM terminal, the mobile number and fingerprint of the customer is required for the system.

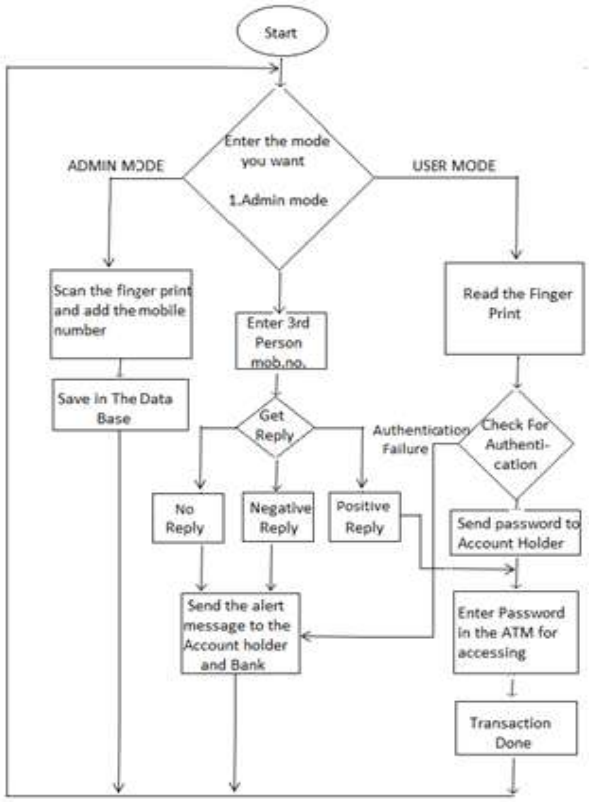

Fig3. The overall flow chart of software

First the system is required the owner's fingerprint. If all the recognition is right, the system would send password to the Account holder and he will enter the same password in touch screen for accessing the ATM Terminal. If authentication failure then it send the alert message to the Account holder and Bank. The overall flow chart of software is shown in Fig3.

VI. EMERGENCY MODE

Emergency mode is very important issue in this system. This is very useful when the owner of ATM card is not actually available at the time of accessing his own account. The service of Emergency mode is having proper cost and limitation according to rules of bank, so anyone can not misuse this facility.

A. Working of Emergency Mode

When third person wants to access ATM card without having presence of owner**,** then it has to press Emergency Mode button, after inserting ATM card.

After pressing Emergency button one text box will be open where a third person has to give his own mobile number.

Then bank will send a message to the owner of ATM card and ask whether authentication to the third person has to provide or not.

 ISSN: 2454-4248
67 – 71

ATM owner will reply to bank and reply can be of following type;

a) If owner gives positive reply then account is accessible to third person.
b) If owner gives negative reply then alert message will be send to bank and appropriate action will be taken on third person.
c) If owner does not give any reply to bank then alert message will send to owner of ATM and bank and appropriate action will be taken on third person.

VII. CONCLUSION

The development in electronic exchanges has brought about a more noteworthy interest for quick and precise client recognizable proof and confirmation. Access codes for structures, banks records and PC frameworks frequently utilize PIN's for ID and exceptional status. Customary strategy for recognizable proof in light of ownership of ID cards or selective learning like a standardized savings number or a secret key are not all together solid. ID cards can be lost, forged or misplaced; passwords can be forgotten or compromised, but ones' biometric is undeniably connected to its owner. It can't be acquired, stolen or effortlessly fashioned. The Implementation of ATM security by utilizing unique finger impression acknowledgment and GSM MODEM took favourable circumstances of the soundness and unwavering quality of finger impression attributes. Extra, the framework additionally contains the first checking techniques which were contributing proprietor's secret key which is send by the controller. The security highlights were upgraded generally for the strength and unwavering quality of proprietor acknowledgment. The entire framework was based on the innovation of implanted framework which makes the framework more protected, dependable and simple to utilize.

REFERENCES

[1] S.S, Das and J. Debbarma, "Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System", International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203, 2011.

[2] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, "Customers Adoption of Banking Channels in Hong Kong", International Journal of Bank Marketing, vol. 23, no. 3, pp. 255-272, 2005.

[3] B. Richard and M. Alemayehu, "Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. 11, no. 2, 2006. Downloaded March 15, 2012 from http://www.arraydev.com/commerce/jibc/

[4] P.K. Amurthy and M.S. Redddy, "Implementation of ATM Security by Using Fingerprint recognition and GSM", International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

[5] M.O. Onyesolu, and I.M. Ezeani. "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study", International Journal of Advanced Computer cience and Applications. Vol. 3, No. 4, 2012.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[7] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle."Generating Cancelable Fingerprint Templates", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007.

[8] B, Schouten and B. Jacobs, "Biometrics and their use in e-passport", Image and Vision Computing vol. 27, pp. 305–312. 2009,

[9] S.A. Shaikh and J.R. Rabaiotti,. "Characteristic trade-offs in designing large-scale biometric-based identity management systems". Journal of Network and Computer Applications vol. 33, pp. 342–351, 2010.