ATM SECURITY BY USING BIO-METRIC METHODS

Mala K

PG Student,
Computer Science and Engineering,
SSIT, Tumakuru, Karnataka.

Abstract:Security and authentication of individual is very importantnowadays, especially in bank system.The usage of the ATM for the bank transaction has increased over the decades, which havemotivated us to use biometric for personal identification to procure high level security and accuracy.This paper describes the replacement of ATM cards and pins by bio-metric authentication.Moreover the feature one time password imparts privacy to users and emancipates user from recalling pins. In this system, the genuine user's biometric are enrolled and are retained in databases, the transaction begin and the bio-metric are cross checked and thus distinguished from legitimate user and the fake ones. After the bio-metric cross checking the GSM module comes into picture, GSM module connected to microcontroller will send the 3 digit code that is generated by system to the legitimate user's mobile number which is one time password for that particular transaction. After the valid OTP is entered the user can do the transaction that he wants to do. If incase there is any fake access attempts during the authentication then the account is blocked. In this system the bio-metric that are used are fingerprint and iris recognition.

Index terms – Authentication, Bio-metrics,Global system for mobile communication (GSM), one time password (OTP).

I.INTRODUCTION

Rapid development of the banking system has increased the security alarm against fraud attacks on the bankingtechnology. One bankingtechnology that has impacted positively and negatively to banking activities and transactions is the advent of theautomated tellermachine (ATM).ATMis the electronic banking machine that is located in differentplaces, which helps the customerto do transaction without the help of bank staffs. With the help of the ATM one can do many banking operation like withdrawal of money, deposition of money, online payments and many more, which requires lot of time if it was to be done in the bank. The surplus of ATM not only increased in their number but also increased in the fraudulent attacks on it.This call for the strong security system as biometric system to be integrated into traditional ATM. In this paper we discuss some of the biometric measures as the means to enhance the security for both customer and bankers in the bank. Biometric authentication can be Fingerprint scanning, Face recognition, Iris scanning etc. But here we are introducing new technology which works the technology fingerprint recognition system and nominee for the main user and GSM technology, and to increase the authentication level we are introducing the iris recognition of the user.

Biometric technology provides strong and indisputable authentication. Because biometrics data are unique of a particular individual, cannot be shared, cannot be copied and cannot be lost. The fingerprint based identification is one of the most mature and proven technique. So we use the fingerprint for the identification purpose. And to add up the security we are introducing the iris recognition. Biometrics technologies are a secure means of authentication,the fingerprint and the iris scanned copy will be stored in the database of the bank when the cardholder or the nominee tries to access the account; they will have to enter the pin and need to enroll the fingerprint and undergo the iris scanning. In case of the iris recognition the user iris is captured by camera and matched with that stored in the database. After the authentication by biometric the GSM module comes into picture .The GSM technology is cellular network which means that mobile phone connect to it by searching for cells in the immediate vicinity. The GSM modems connected to the microcontroller generates the 3 digit code and send it to the main user mobile number or of the nominee's. The user can access the account after he/she enter one time password, after they can begin the transactions.

II. SYSTEM DEVELOPMENT

In the proposed system we present a fraud detection method using two biometrics (fingerprint and iris) to detect various types of illegal access attempts during the ATM transaction in the bank system. The objective of the proposed system is to enhance the security of the ATM transaction using biometric recognition framework. In this system ARM board is used for smart ATM access. The fingerprint for fingerprint recognition it captures the fingerprint of the person and compares it with the fingerprint of the legitimate user that stored in the database. If the person is a valid user the controller will display a message "VALID PERSON" on the LCD display. The USB camera is used to capture the eye image of the user. A GUI prepared in Mat lab is used for iris recognition. After iris authentication and matching if the person is a true user then the controller displays a message "IMAGE IDENTIFIED" on the LCD display. After the validation result of the person is true a 3 digit code is messaged to the customer's registered mobile number which was saved in the database during enrollment, if n case the legitimate nominee accessing then the same procedure repeats for them. This process is done through the GSM module which is interfaced to the ARM board. Depending

on whether the OTP entered is correct or wrong messages like" CORRECT CODE "or "REENTER CODE" is displayed on the LCD display. After the entered code is found valid the banking process begins and a message "BAL, DEP, WTD" for entering the option for the task to be performed is displayed on the LCD display. After the task is performed finally a message "TRANSACTION COMPLETED" is displayed on the LCD display.

III. DETAILED STUDY AND ANALYSYS

3.1 Fingerprint recognition

A customer will be authenticated his finger print and will be sent to the bank for validation as part of every transaction, which is one level of authentication procedure. This makes the developed ATM software further secure as compared to the software that authenticates the user merely by using a PIN or password which is used in the traditional system.

3.2. Iris recognition

A customer will be authenticated his irisand will be sent to the bank for validation as part of every transaction after the finger print authentication. This makes the ATM software further secure as compared to the software that authenticates the user merely by using a PIN or password. In the proposed system there are three waysof authenticationwhich makes the ATM more secure.

IV. HARDWARE REQUIREMENT

4.1. Arduino uno

Arduino is a prototype platform (open-source) based on an easy-to-use hardware and software, in this family of arduinobords we are using Arduino uno. It consists of a circuit board, which can be programed (referred to asa microcontroller) and ready-made software called Arduino IDE (IntegratedDevelopment Environment), which is used to write and upload the computer code to thephysical board(as shown in the fig 1). In this board we are using the Embedded C programming.

Fig 1: Arduino uno board

4.2. Rasberry pi

The Raspberry Pi is a credit-card-sized computer that plugged into your TV and a keyboard. It is a capable little computer which can be used in electronics projects, and formany of the things that your desktop PC does, like spreadsheets, word processing, browsing the internet, and playing games. It also plays high-definition video. Rasberry pi is required in this project as there are only two uarts (one uart is used for the serial pin connection and another for the finger print interfacing) in the Arduinouno and we need to do the iris recognition in the system hence another board is used, for this the programming is done in the python language.

Fig 2: Rasberry pi board

4.3. GSM module

A GSM is a type of hardware which accepts a SIM card, and operates over a subscription to a mobile operator, just like mobile phones do. From the mobile operatorperspective, a GSM looks just like a mobile phone. Whenever a GSM modem is connected to a computer, it allows the computer to use the GSM modem to communicate over the mobile network. While these GSM modems

are most frequently used to provide mobile internet connectivity all over, many of them can also be used for sending and receiving SMS and MMS messages, which is the specialized feature of them.

Fig 3: GSM module

4.4. LCD (Liquid crystal display)

LCD is the display is mostly used display technology. LCD's are common because they offer some real advantages over other existing display technologies. They are thinner and lighter and draw much less power than cathode ray tubes(CRTs) and are very easy to use. Here we use 20*4 LCD for this project.

Fig 4: LCD display

4.5. Keypad

A keypad is a set of buttons arranged in a block or "pad" which usually bear digits, symbols and usually a complete set of alphabetical letters which is portable. If it mostly contains numbers then it can also be called a numeric keypad, but now a days we see the model which has both of numeric and alphabet keys. The keypad Switches are connected in a matrix of rows and columns. The rows and columns of the matrix are connected to four output port lines and four input port linesrespectively.

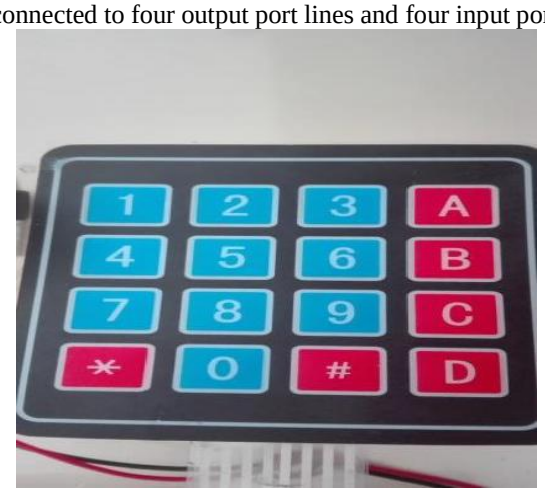

Fig 5: keypad

V. SOFTWARE DESCRIPTION

5.1. Embedded C programming

The 'C' Programming Language was developed for and implemented on the UNIX operating system, by Dennis Ritchie in the year 1971. One of the best features of C is that it is not tied to any particular hardware or system, it is portable. This makes it easy for a user to write programs that will run without any changes on practically all machines which add the flexible feature to the language. C is often called a middle-level computer language as it combines the elements of high-level languages with that of assembly language features. To produce the most efficient machine code, the programmer must not only create an efficient high level design, but also pay attention to the detailed advantage of the language.

5.2. Python programming

Python is a generally used, interpreted, interactive, object-oriented, and high-level programming language. It was created by Guido van Rossum during the years 1985- 1990.Like Perl, Python source code is also available under the GNU General Public License(GPL), where anybody can download and can use.Python is a high-level, interpreted, interactive and object-oriented scriptinglanguage similar to C++. Python is designed to be highly readable and easily understood. It uses English keywordsfrequently where as other languages use punctuation, and it has fewer syntacticalconstructions than other languages in the market

VI. RESULTS AND DISSCUSSION

6.1. Results for Fingerprint module

When a finger was placed on the NITGEN 3030 fingerprint recognition device it captured a 3D grayscaleimage after scanning the fingerprint and a 256×288 pixelsimage was stored in bitmap format in the database. When the same user's new fingerprint imagewas captured a new template of that query image was createdin the same manner as it was done during enrollment same has to be done to the nominee. Thisnew template was compared with the templates in the databaseand a message "VALID PERSON" was displayed on the LCDbut when another fake user went through the same process amessage "PERSON NOT IDENTIFIED" was displayed.

Sr. No.	FP	TP	AC	P
1	0.1	0.9	0.9	0.9
2	0.05	0.95	0.95	0.95
3	0.11	0.81	0.85	0.9
4	0.13	0.94	0.9	0.85
5	0	0.90	0.95	1
6	0.09	0.94	0.92	0.9
7	0.04	1	0.97	0.95
8	0.1	0.9	0.9	0.9
9	0.05	0.86	0.9	0.95
10	0.05	0.95	0.95	0.95

Table 1: Analysis of the proposed system.

6.2. Results for Iris Recognition

The eye image (iris) of a person was captured using a QHMPLPC camera and was stored in 640×480 pixels in bitmapformat. After capturing the query eye image a featurevector of the input pattern was obtained in the same manner asit was determined during enrollment of the bank customer. This feature vector wascompared with those feature vectors present in the database ifthe person was a valid person then after running the GUI,the message "MATCH"will be displayed on the monitor, else a message " NOMATCH FOUND" is displayed and the same is intimated to the bank authority. Investigations show that theiris recognition system used in this work provides about95.6% accuracy .Table 1 gives an idea of accuracy of thesystem output for the overall system after the several executions.

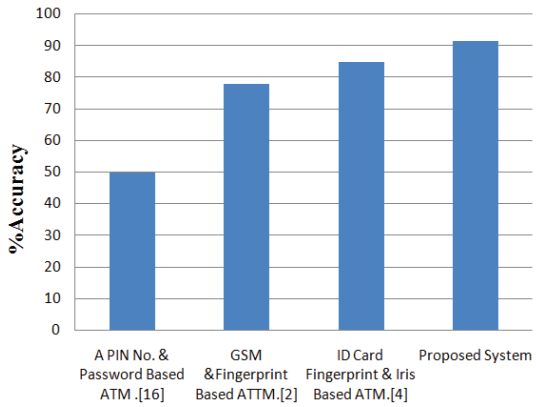

Fig 6: The graph of survey of security in ATM system

6.3.Results for OTP generation

After the valid biometric identification a message "ACCESS CODE" SMS was received on the user's registered mobile number simultaneously a message"ENTER THE CODE" was displayed on the LCD display. After the valid code was entered the system proceeded further towards the banking process. But when the wrong code was entered an SMS "UNKNOWN PERSON TRYING TO ACCESS" was received on the user's registered mobile number and the same is intimated to the bank authority.

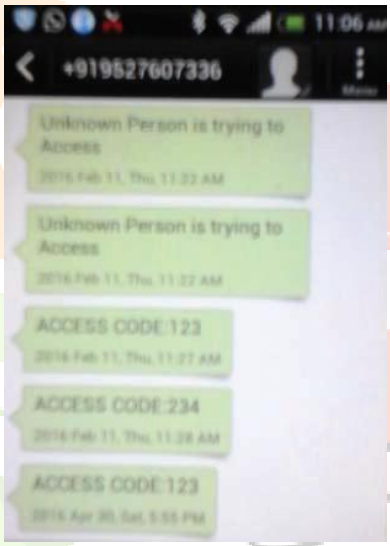

Fig 5: OTP message received on the mobile screen

6.4. Results for Banking Process

The system is fed with a default amount 999. So when awithdrawal of 100 was done the balance amount showed 899 on the display.

VII.CONCLUSION

The use of the biometrics integration to bankapplication has made theATM transaction system more reliable and secured. The OTP concept added to the system further enhances the security andavoids the need for us to remember passwords. Moreover the system is built on embedded technology which makes it userfriendly and non-invasive. Using this system the ATM terminal is secured from thief attacks. The Fig 6andTable.1 shows that the average accuracy of the overall systemis 91.6% and the average equal error rate is 0.076. The timetaken for the overall ATM transaction is less than 10 sec foreach user.

VII. ACKNOWLEDGEMENT

The authors Mala K would like to thank the anonymous referees whose help and technicalideas have improved the quality of this paper.

REFERENCES

[1].Anil K. Jain, Jianjiang Feng,Karthik Nandakuma, "FingerprintMatching", *IEEE* Computer Society2010, pp. 36-44, 0018-9162/10.
[2]. KhatmodeRanjit P, KulkarniRam Chandra V,"ARM7 Based Smart ATM Access and Security System Using Fingerprint Recognition and GSM Technology", International Journal of Emerging Technology and Advanced Engineering, Vol.4, Issue 2,Feb. 2014.
[3]. G.Udaya Shree, M. Vinusha"Real Time SMS-Based HashingScheme for Securing Financial Transactions on ATM terminals", International Journal of Scientific Engineering and Technology Research, Vol.2 Issue 12. Sep.2013.
[4]. D.ShelkarGoud, IshaqMd, P.J.Saritha,"A Secured Approach forAuthentication system using fingerprint and Iris", Global journal of Advanced Engineering Technology, Vol, Issue3-2012.
[5]. Kriti Sharma, HinanshuMonga, "Efficient Biometric IrisRecognition Using Hough Transform with Secret Key",International Journal of Advanced Research in Computer Science and Software Engineering. Vol.4, Issue 7, July 2014.
[6]. Ritu Jindal, GagandeepKaur, "Biometric Identification SystemBased on Iris, palm and Fingerprint for Security Enhancements", International Journal of Engineering Research and Technology, Vol.1, Issue 4, June 2012.
[7]. DeepaMalviya, "Face Recognition Technique: Enhanced SafetyApproach for ATM", International Journal of Scientific and Research Publications, Volume 4, Issue 12, December 2014.
[8]. Matsoso Samuel Monaheng, PadmajaKuruba, "Iris RecognitionUsing Circular Hough Transform", International Journal of Innovative Research in Science, Engineering and Technology, Vol.2, Issue 8, Aug.2013.
[9]. Fakir Sharif Hossian, Ali Nawaz, Khan Md. Grihan,"BiometricAuthentication Scheme for ATM Banking System using AES Processor", International Journal of Information and Computer Science Volume 2 Issue 4, May 2013.
[10]. R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Mateyand S. McBride, "A system for automated iris recognition", Proceedings *IEEE* Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 2011.