Two Level Authentication for Banking System

Ghodake Archana S.[1] Rundal Yojana M.[2] Gaikwad Pooja S.[3] Gholap Arakta V.[4] Prof. Shaikh I. R.[5]
[1,2,3,4]BE Student [5]Head of the Dept.
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]SND COE & RC Yeola, Maharastra, India

Abstract— In this system, we are going to add more security to Banking system. Now a days some problems like shoulder suffering can be occurs, use of skimming devices etc. so we can avoid such problem by using biometric authentication and GSM system. At the time of bank account registration when we create our bank account, banker's will collect the account holder's information like mobile number and fingerprint also for validation of account fingerprint will be scanned, if fingerprint get matched then OTP will be send on valid mobile number which is given when we register for the new account. OTP will be of 4 digit number which will only valid for single use. Next time we are not able use same OTP. Every time new OTP will received by account user. Hence level of security get increased.

Keywords: ATM, OTP, Authentication, Fingerprint Scanner

I. INTRODUCTION

In today's world, there are almost 2 million ATMs around the globe. Although use of the ATM machines has declined in recent years, like because more people make shop using credit and debit cards instead of cash, the ATM continues to have a place in modern culture. Today's all sell from airline tickets to movie tickets to medicine. But the only compulsion is ATM card usage for all transactions. We are proposing a method which completely foils this restriction. The ATM card which is made of plastic and the magnetic stripe. The stripe having all the information about the account user but if the magnetic stripe is get scratched then all data will be lost. This is the disadvantage of ATM card, we can avoid this problem by using the biometric authentication and GSM system. In existing multiple problems can occurs like losing the ATM card. It also has number of drawback like forget pin, losing card, stolen card, breaking card and so on. Because of all these problem different type of frauds can be happens. User get service 24*7 hour from ATM, so the ATM system must be provide more security and fraud less. So, this project will helps us to overcome all the problem occurred in ATM. For this we will use biometrics system i.e. fingerprint scanner. First user will scan the fingerprint if it matches then system will shows account list that the user have in different banks. After validating the user 4 digit OTP will be send to the user. The OTP will valid for particular time, which will be unique that means next time we cannot use same OTP. Every bank account holder will have his mobile phone no registered with the bank account. This alone is sufficient to prove identification and authentication of bank user. Bank's server will have a GSM device attached in order to receive and send SMSs. OTP will be send only on registered user mobile number.

II. PROPOSED SYSTEM

In our project, we propose to add more security to the current ATM systems. By using Biometric Authentication and GSM technology, we can overcome many of the flaws introduced by our current ATM system such as shoulder surfing, use of skimming device, etc. The idea of using fingerprint and OTP in ATMs as a password instead of the traditional pin number is that the users will be more relieved as their accounts cannot be accessed by others and can maintain secrecy. We also have OTP feature along with the fingerprint authentication which will definitely not allow any criminal to use the password for any kind of frauds as the OTP is valid only once. The proposed system is divided into following module, and they are used along with each other to provide more services as follows:

A. Fingerprint Module:

This module is used for purpose of authentication the step is to verify provided fingerprint matches which is register in the database at the time of account registration.

B. Max 232:

This module is used for serial communication, this module is used to connect fingerprint module with PC /LAPTOP and GSM Module.

C. PC/Laptop:

It is used store the database of account user which are registered in bank, using Java and MySQL language.

D. GSM Module:

In order to send OTP, GSM technology is used with the help of GSM Modem. A GSM Modem which accepts a SIM card because it is specialized type of modem, and operates over a subscription to a mobile operator, just like a mobile phone. From the mobile operator, a GSM modem looks just like a mobile phone.

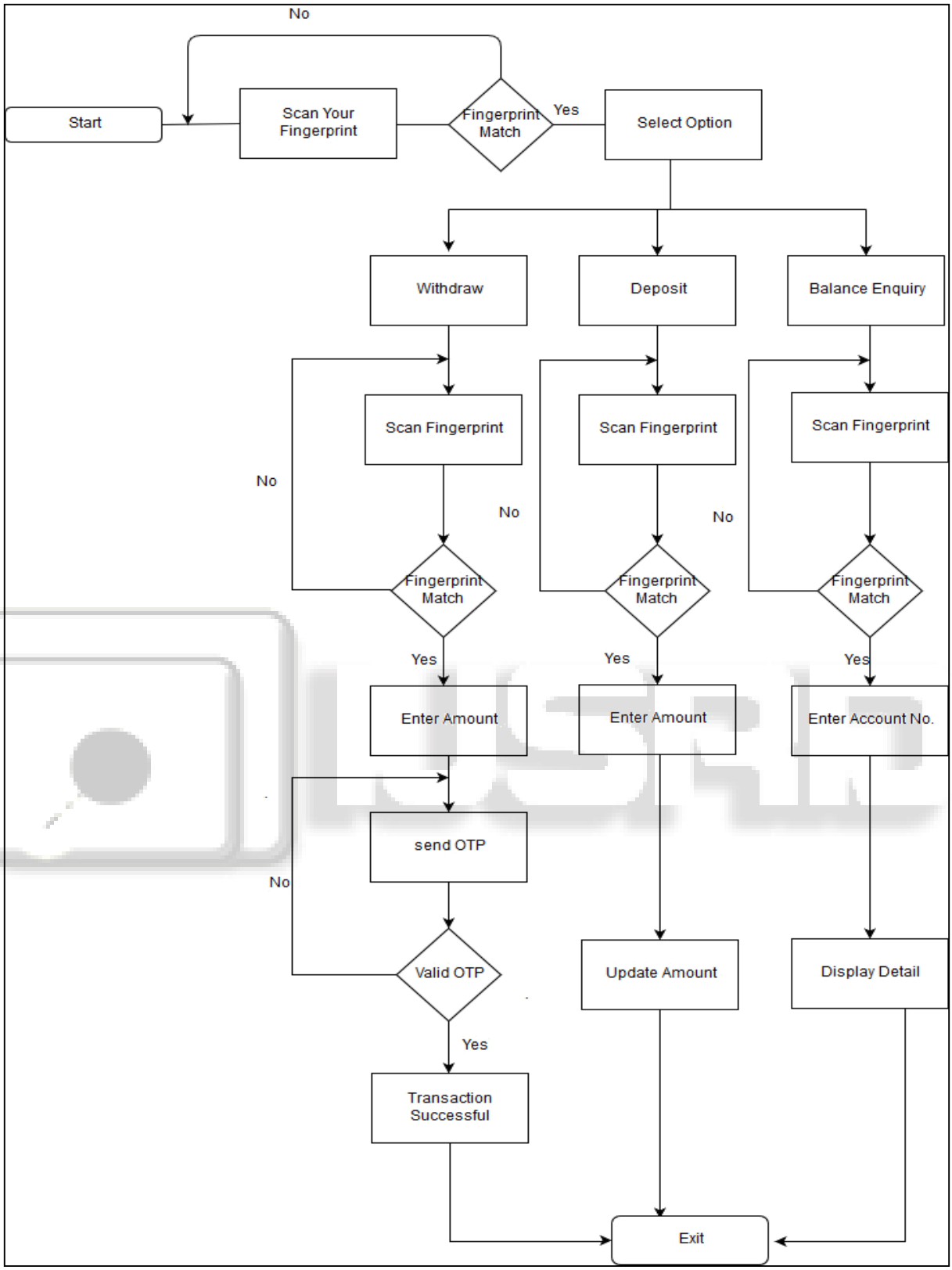


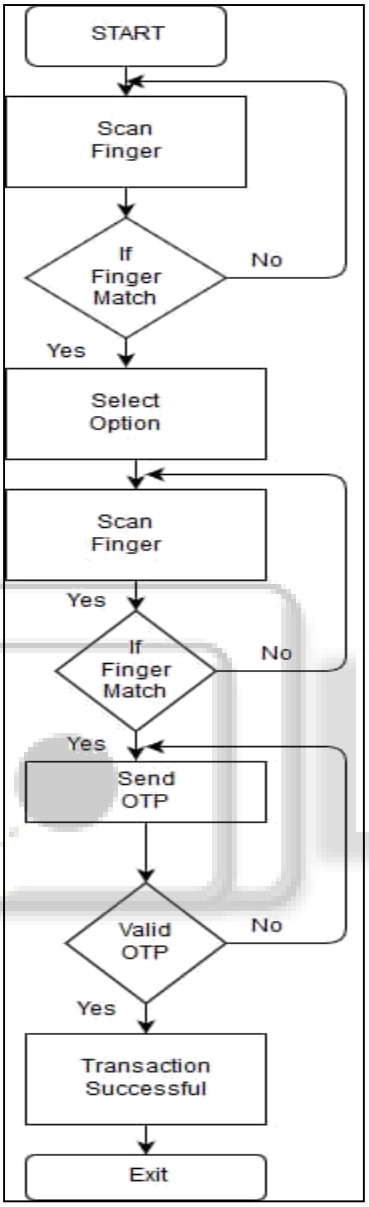
Fig. 1: System Architecture

III. METHODOLOGY

This project deals with the solutions related to the ATM security. We are going to make use of fingerprint or One Time Password (OTP) verification along with the use of ATM pin. In this system, the user can have third party authentication either temporary or permanent. In the whole process, the first party i.e. the banker will maintain a database of the customer including fingerprint and mobile number. The banker will provide the ATM card along with its PIN. For the transaction after entering the ATM pin, the customer will be asked to choose an option either fingerprint or OTP verification. The OTP will be sent to the registered mobile number of the customer through GSM module connected to the system.

After authorized verification the customer will be able to proceed for transaction else after three successive wrong attempts, the ATM card will be blocked for 24 hours and a message will be sent to the registered user mobile number.

IV. ALGORITHM DETAILS



V. SYSTEM IMPLEMENTATION PLAN

Here, we present Fingerprint identification system performance is measured in terms of the following parameters and were used to analyze the result of the designed Withdrawal ATM system.

A. False Rejection Rate (FRR):

The probability that a system will fail to identify an enrollee. It is also called type 1 error rate. This is as known as false nonmatch rate (FNMR).
FRR = NFR÷NEIA = 0 ÷ 1000 = 0
NFR = number of false rejection rates = 0
NEIA = number of enrollee identification attempt = 1000

B. False Acceptance Rate (FAR):

The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate. This is as known as false match rate (FMR).
FAR = NFA÷NIIA = 0 ÷ 550 = 0
NFA = number of false acceptance = 0
NIIA = number of imposter identification attempts = 550

C. Response Time (RT):

The time period required by a system to return a decision on identification of a sample. The average response time of the designed system is 1.5 seconds.

D. Decision Threshold (DT):

The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict depending on the requirements of any given application.

E. Enrollment Time (ET):

The time period a person must spend to have his/her fingerprint reference template successfully created. The enrollment time of the designed system is one second.

F. False Positive Identification Rate (FPIR):

This occurs when the system finds a hit for a query fingerprint that is not enrolled in the system.
FPIR = 1 - (1 - FMR)\N
FPIR = 1- (1- 0)1000 = 1- (1)1000 = 1- 1 = 0

G. False Negative Identification Rate (FNIR):

occurs when it finds no hit or a wrong hit for a query fingerprint enrolled in the system. The relationship between these rates is defined by
FNIR = 1- (1 - FNMR)\N
FNIR = 1- (1-0)1000 = 1- (1)1000= 1-1 = 0
where N is the number of users enrolled in the system = 1000.
Where FMR = FNMR = 0 from system testing.

H. Average time of transaction using the designed system, (Normal process time):

50 Seconds.

I. Average time of transaction which using the feedback GSM mechanism.(Q-code and S-code):

2 minutes. Some other scenarios that were experienced in the designed system, for example in the case of using wrong fingerprint thrice for four of the above customers, Q-code were generated and sent to the customers' GSM phone numbers with which they were able to gain access into their accounts only after they have supplied the correct secrete code (S-Code) numbers.

VI. RESULT AND DETECTION

The data collected from various modules are grouped and classified and stored on the Bank's server. Our aim is to maintain the history record of each and every user either it may be of its transaction details etc. This is decided as per the users requirement and then classified into various classes and

stored as separate for each and every unique identity or record.

- The system improves the security of ATM's.
- Use of OTP provides second level of security.
- Matching Mode: 1:1 and 1:N
- Storage Capacity: 256
- Average Search Time: <1sec
- Image Acquire Time: <0.5sec.

Input Images	Number of images used for recognition	Number of images recognized correctly	Accuracy (%)
1	8	7	90
2	8	8	100
3	8	8	100
4	8	8	100
5	8	8	100
6	8	8	100
7	8	8	100
8	8	8	100
9	8	8	100
10	8	8	100
Overall	80	79	99

VII. Conclusion

ATM machine increase the reliability of the bank by providing the easy access to the cash transaction by account user. We can withdraw the cash anywhere and anytime without waiting in queue. Hence, ATM card is used wildly but we have to face the fraud related to the ATM transaction. To make ATM transaction more secure we are using biometric scanning machine to identify the account holder. Finger is unique identity of each and every person so the use of Biometric Fingerprint scanner we can avoid ATM related fraud and misuse. The Security feature of system enhanced stability and reliability of owner recognition. The whole system designed by using technology of embedded system which makes the system more secure, reliable and easy to use.

VIII. Future scope

we can expand this project by adding a GPS module which sends the alert message to authority telling that at which the ATM is tried to be theft.

Today IOT is been implemented everywhere, so IOT can be also used for security purpose.

Sensors like Eye Sensor can be used to make the system more reliable.

Acknowledgement

Firstly I gladly thanks to my project guide and our HOD Prof. Shaikh I. R. for this valuable guidance for implementation of proposed system. We will forever remain a thankful for their excellent as well as polite guidance for preparation of this report and also thankful to other staff for their helpful coordination and support in project work.

References

[1] Dr. V. Vijayalakshmi, R. Divya and K. Jaganath, "Finger and Palm print based Multibiometric Authentication System with GUI Interface" International conference on Communication and Signal Processing, April 3-5, 2013, India, 978-1- 4673-4866-9/13/$31.00 ©2013 IEEE

[2] O. A. Esan and S.M.Ngwira "Bimodal Biometrics for Financial Infrastructure Security" I. O. Osunmakinde School of Computings, College of Science, Engineering and Technology, University of South Africa, UNISA Pretoria, South Africa, 978-1-4799- 0808-0/13/$31.00 ©2013 IEEE.

[3] RishigeshMurugesh, "Advanced biometric ATM machine with AES 256 AND STEGANOGRAPHYIMPLEMENTATION", IEEE Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University,Chennai. December 13-15, 2012, 978-1-4673-5584-1/12/$31.00©2012 IEEE.

[4] Rajesh. V and Vishnupriya. S, "IBIO-A New Approach/or ATM Banking System" 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Feb.13-14, 2014, Coimbatore, INDIA.

[5] G. Renee Jebaline and S. Gomathi , "A Novel Method to Enhance the Security of ATM using Biometrics" , 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT], 978-1- 4799-7075-9/15/$31.00 ©2015 IEEE

[6] A.Muthukumar and N. Sivasankari,"A Review on Recent Techniques in Multimodal Biometrics", 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA ,978-1-4673-6680- 9/16/$31.00 ©2016 IEEE

[7] UmmaHany and LutfaAkter,"Speeded-Up Robust Feature Extraction and Matching for Fingerprint Recognition", 2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015.Jahangirnagar University, Dhaka-1342, Bangladesh, 21-23 May 2015, 978-1-4673-6676- 2115/$31.00 ©20151EEE.

[8] Ms. Archana S. Shinde and Prof. VarshaBendre, "An Embedded Fingerprint Authentication System", 2015 International Conference on Computing Communication Control and Automation, 978-1- 4799-6892- 3/15 $31.00 © 2015 IEEE DOI

