INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 07 ISSUE: 05 | MAY - 2023 IMPACT FACTOR: 8.176 ISSN: 2582-3930

Biometrically Secured ATM Vigilance System Using IOT

Mrs . Sanjitha S
Department of Information Science and Engineering
East West Institute of Technology
Bangalore,India
sanjitha94@gmail.com

Shalini S N
Department of Information Science and Engineering
East West Institute of Technology
Bangalore,India
shalininagaraju2000@gmail.com

Sushma E
Department of Information Science and Engineering
East West Institute of Technology
Bangalore,India
sushmas12806@gmail.com

Sapthami N K
Department of Information Science and Engineering
East West Institute of Technology
Bangalore,India
sapthamink23799@gmail.com

Sneha P
Department of Information Science and Engineering
East West Institute of Technology
Bangalore,India
sneha369741@gmail.com

***Abstract*— Automated Teller Machine (ATM) services are more popular because of their flexibility and easiness for banking systems. People are widely using their ATM cards for immediate money transfer, cash withdrawal, shopping etc. To provide high security we introduced fingerprint based customer authentication. The main objective of this project is to develop a single smart card ATM (Automated Teller Machine) for multiple bank accounts. It reduces the cost of inter banking transactions as interfacing different bank databases is a resource consuming thing. In this security system the non-authorized persons can enter by using this smart card (RFID) and Message Module based OTP (One Time Password) and keypads. User module is the interactive module through which the user can log into the system and perform the transactions of the user's choice. Though the proposed system provides the user a level higher convenience, efficient and user friendly.**

***Keywords*— *Biometric Authentication, microcontroller, fingerprint sensor, RFID, OTP (one time password)*.**

I. INTRODUCTION

An Automated Teller Machine (ATM) allows customers to perform banking transactions anywhere and at any time without the need of human teller. By using a debit or ATM card at an ATM, individuals can withdraw cash from current or savings accounts, make a deposit or transfer money from one account to another or perform other functions. You can also get cash advances using a credit card at an ATM.

The ATM is an electronic telecommunication device that provides financial transactions such as cash withdrawal, cash deposits, funds transfer, and payments of utility. ATM fraud has become a global issue that has dramatically increased in recent years. ATM fraud has an impact on both customers and bank operators. They are facing the issues of crimes and security threats to the existing card system. The existing ATM system uses PIN and ATM cards for authentication, which have several drawbacks. To steal ATM card and their information, criminals use some techniques such as ATM skimming, Cash trapping, Shoulder surfing, and Card trapping. Some customers use their phone numbers, birthdates as their PIN which can be easily guessed by Fraudsters or hacked by cybercriminals. Biometric authentication has solutions to these problems of ATM card and PIN. This is because the biological details are unique and cannot be duplicated by others.

In this paper, the proposed model uses the fingerprint for transactions which enables higher level of security, also uses multi account embedded cards which consist of multiple banks in single card which has reduces the risk of caring multiple cards and and remembering multiple password.

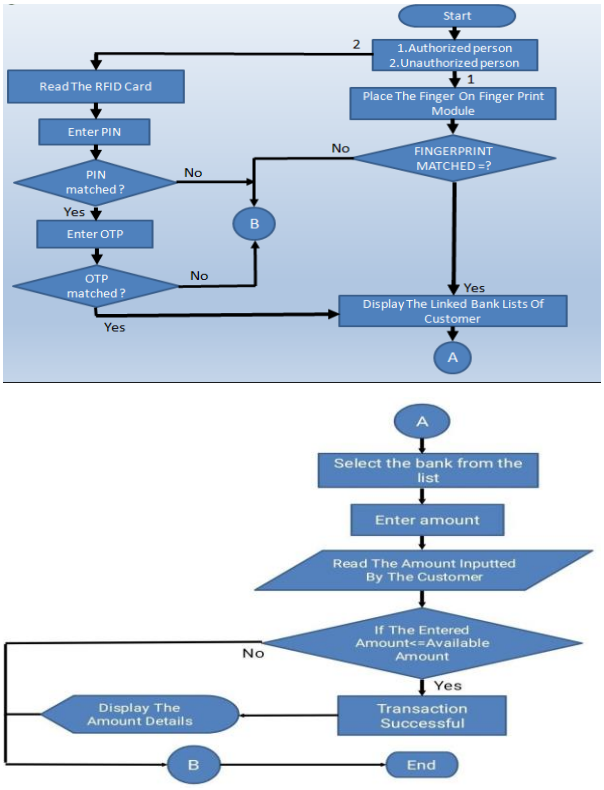


Fig.1.Flow Diagram of Biometrically Secured ATM System

II. LITRETURE SURVEY

1. "Dimaunahan, Ericson D Ballado, Alejandro H. Cruz, Febus Reidj G, Dela Cruz, Jennifer (2017)"

In this paper, the author proposed voice identification along with fingerprint authentication as a solution to existing automated teller machine security for visually impaired users. By using fingerprint authentication and voice recognition to perform ATM transactions, adds two tiers of security, and also provided ease of use of the system for people with visual impairments. They have used vector quantized mel frequency cepstrum coefficients and discrete wavelete transform extraction of the voice parameters for speech recognition to identify the user. To identify the unknown voice, the system checks out the extracted features of the unknown speech and then compares them to the stored extracted features. The process of feature extraction is done by using the mel frequency cepstrum coefficients and discrete wavelet transform and the feature matching is being modelled using the vector quantization.

2." Prakash Chandra Mondal, Rupam Deb, and Md. Nasim Adnan (2017)"

The author proposed a system that uses behavioral biometrics for authentication with more security. In this system, authentication is performed using three steps which include online handwriting signature verification, chip-based card, and PIN verification. This method does not involve the need for further enhancement like using physical biometrics (fingerprint, face images, etc).

3."Sweedle Machado, Prajyoti D'silva, Snehal D'mello, Supriya Solaskar and Priya Chaudhary (2018)"

In this paper, the author had proposed a system that uses a fuzzy vault system for the security of ATM pins and passwords using a user's fingerprint data. It involves encryption and decryption. In the encryption process, the minutiae points get extracted from the fingerprint which is encoded using a pin password. While obtaining the user's account the data encoded is deciphered using the same fingerprint International Journal of Scientific Research in Science and Technology impression to retrieve the pins and the passwords. The main benefit of this system is securing ATM passwords and pin with fingerprint data.

4."Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar (2018)"

In this paper, the authors had proposed the concept of Fingershield ATM, a biometric identification in the form of the fingerprint is implemented along with ATM which is integrated with smart card and database server. Despite the fact that user has to go through additional authentication time for fingerprint verification, the security was much improved and guaranteed by their system. Firstly, a smartcard is inserted into the reader, the program will ask for PIN from the user through the keypad. On successful PIN authentication, the program will then prompt fingerprint input. After successful fingerprint authentication, the user will proceed further or authentication will fail.

5."Inndranil Banerjee, Sjivangam Mookherjee, Sayantan Saha, Souradeep Ganguli, Subham Kundu, Debduhita Chakravarti (2019)"

In this paper, the authors had proposed a double layer security check. Firstly, the user inserts the RFID card after that user gives a fingerprint which is verified if there is a mismatch a message is sent to the user. If it's a match, the system further goes on with the level-2 security check i.e., the IRIS scanner. IRIS is the only part of our body that doesn't change from birth till our death. Iris scan is one of the most secured biometric systems it further increases the level of security along with the fingerprint and RFID card that acts as the secondary security check.

6."Murugesan M, Santhosh M, Sasi Kumar T, Sasiwarman M, Valanarasu (2020)"

This paper represents the security of ATMs using facial recognition. The authors had used an RFID reader instead of an ATM card reader to identify the account details of the user. CCTV is used to recognize the face International Journal of Scientific Research in Science and Technology using a cascade and local binary pattern and if the face will match to the database, then after entering the pin, the transaction will proceed otherwise the system will send the link to the account holder it will show the snap of the person who is currently using his card and also enables three options for the user to choose one option – 'it's me', 'accept', 'decline'. If the user clicks on it's me then it will allow updating the image of an account holder and if an account holder clicks on accept then the system will allow the transaction and if the user clicks on the decline, it will terminate the transaction.

7." Adrian Fernandes (2020)"

In this paper, the authors had proposed biometric protection to overcome the PIN Number problem. A fingerprint scanner is used for authenticating the users where the user's fingerprint will authenticate it and further proceed for bank transactions. The user will enter an ATM card into the machine then the machine will ask for a fingerprint to verify the user. Here Fingerprint verification is done by the data stored in the Aadhar server. Therefore, fingerprint data is retrieved through the Aadhar server based on the Aadhar card in which the user's bank account. After the biometric check user will proceed with the transaction process. If the

user makes three consecutive attempts with an error the user account will be blocked.

III. METHODOLOGY

The information can be stored at a bank branch or Network Provider. The typical ATM has two input devices (a card reader and keypad) and four output devices (display screen, cash dispenser, receipt printer, and speaker).

While here our ATM system uses smart cards with PINs and fingerprint validation. The host systems can reside at a client's institution or be part of an EFT network. The EFT network supports the fingerprint authentication.
With the fingerprint reorganization method we also embedded the GSM technique. That the GSM modem connects to microcontroller and further transactions are performed this is the case when the main user uses the ATM for transactions.But when the nominee uses the ATM for transactions, the fingerprint of that nominee user doesnot match to the fingerprint that is stored at that sequence the main user will send the 4 digit code to the ATM system within the special characters at the end when ATM sends alert message and asks for the OTP. And when the nominee user enters the 4 digit OTP ,the system now compares the OTP entered is matching with the OTP that is sent by the main user, if the OTP matches the transaction will begin.

The user may do the transactions like fund transfer, cash withdrawal, mini statement, bill payment, balance enquiry. So the system is so safe and secure, and it avoid the security problems what we face in the previous works. To implement the proposed security for ATM terminals with the use of fingerprint recognition, we use the different hardware and software platforms.

I BLOCK DIAGRAM

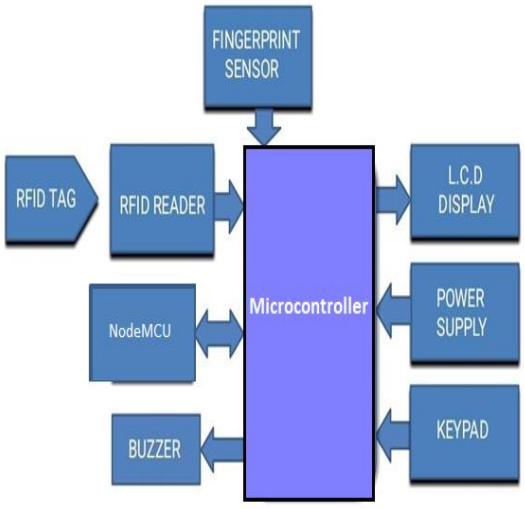


Fig.2.Block Diagram of Biometrically Secured ATM System

IV. RESULTS

Thus, the hardware and the software setups are linked together and processed for User authentication and security protocols. Tight security is maintained while the transaction process, as well as physical security, is also provided for the ATM environment, which leads to safe and secure ATM transactions

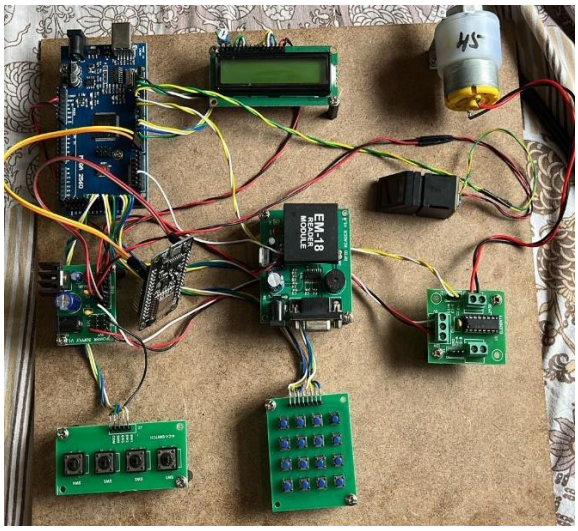
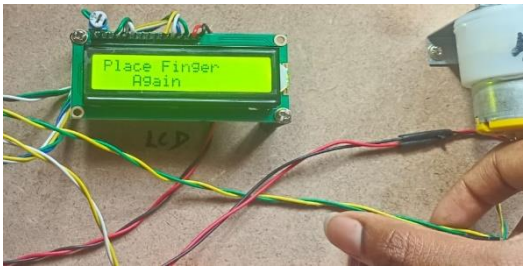


Fig.3.Working Demo model of the System

WORKING SNAPSHOTS

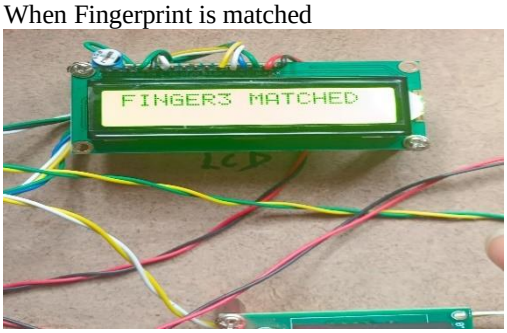
1. Storing Fingerprint



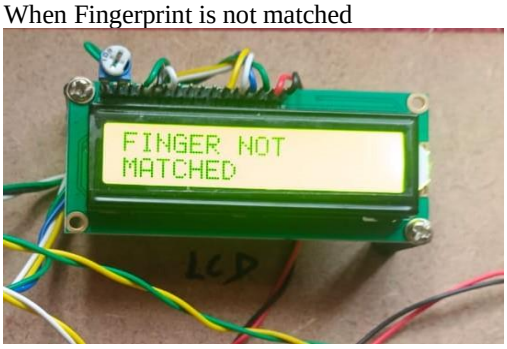
2. Scanning Cards

3. Fingerprint Authentication

When Fingerprint is matched

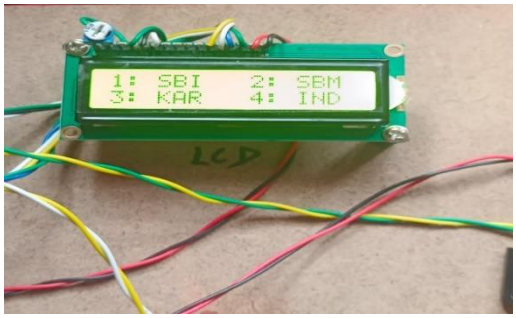


When Fingerprint is not matched

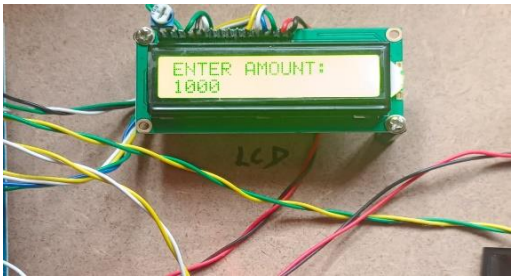


Asks for OTP from client when Fingerprint is not matched

4. Selecting Bank



5. Enter Amount



6. Showing Balance

V. CONCLUSION AND FUTURE WORK

The system we are using for handling multiple accounts here is more efficient than existing system. This Reduces transaction cost of handling multiple accounts of a single user. This make banking system more efficient than the existing system. Using this the users can perform transactions for all his bank Accounts using single smart ATM card with Enhanced security system such as OTP (one time password) and face recognition. Thus the user can manage his multiple accounts in various banks with the help of this single smart card which provides access and reduces the complex of managing more than one ATM card and passwords. This also leads to reduce cost of transaction charges that were on the customers for making transaction and decrease in their production of smart cards for each every account the user has. By implementing this ATM fraud i.e. skimming etc., can be avoided. This project can be implemented for office security Also to colleges, hospitals and also in parking system.Future research will help to do away with PINs

completely and dwarf ATM card authorization by introducing palm and finger vein authentication which is fast, accurate and difficult to fake. Since more than one bank accounts being added, the existing PIN security are not sufficient enough, so we can use a biometric scan in the smart card i.e. multi component card So that the user holds the card such that the face recognition on the biometric scan reader while he swipes the registered card and the image is authenticated at the real time. No one other than the user and their family can use the card. Only if the face matches the user can enter his PIN number otherwise the transaction will not be allowed until the user is authenticated

REFERENCES

[1] "Smart Card & Security Basics" -CardLogix, paper no.:710030 www.cardlogix.com

[2] "Smart card based Identity Card And Survey"-White Paper JKCSH (Jan Kremer Consulting Services).

[3] Chip-and-PIN: Success and challenges in reducing Fraud from Federal Reserve Bank of Atlanta"-Douglas King, Jan 2012.

[4] "Examining Smart-Card Security under the Threat of Power Analysis Attacks"- Thomas S.Messaerges member IEEE, Ezzat A.Dabbish member IEEE, and Robert H.Sloan senior member IEEE vol.51, No. 5, MAY 2002.

[5] "Secure Internet Banking Application"-Alain Hiltgen, Thorsten Kramp.

[6] Fingerprint Verification Using Smart Cards for Access Contol Systems, Raul Sanchez-Reilllo, IEEE AESS Systems Magazine , September 2002 "Benefits Of Smart cards versus Magnetic Stripe Cards for Healthcare Application"-Smart card Alliance 2011.

[7] Katakam Swathi, Prof.M.Sudhakar "Multi Account Embedded ATM Card with Enhanced Security" IOSR Journal of Electronics and Communication Engineering IOSR Journal of Electronics and Communication Engineering, Volume 10, Issue 3, Ver. I (May- Jun.2015)

[8] Tahaseen Taj I S, Dr Suresh M B"AN EMBEDDED APPROACH: FOR HANDLING MULTIPLE ACCOUNTS WITH SMART ATM CARD" International Conference on Computer Science, Electronics & Electrical Engineering-2015

[9] Nair Vinu Uthaman, Pratiksha Shetty, Rashmi, Mr.Balapradeep K N "MAASC Multiple Account Access using Single ATM Card" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 6, June 2014

[10] Youjung Ko, Insuk Hong, Hyunsoon Shin, Yoonjoong Kim"Development of HMM- based Snoring Recognition System for Web Servies" 2016 IEEE

[11] Ashutosh Gupta, Prerna Medhi, Sujata Pandey, Pradeep Kumar, Saket Kumar, H.P.Singh"An Efficient Multistage Security System for User Authentication" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[12] Archana.Darchanadheenadayalan, Aarthi.R Angelin.A " SECURED SMART CARD FOR MULTI BANKING" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 09761353 Volume 21 Issue 3 APRIL 2016. 634

[13] Sree Rekha G, V.K.Agrawal "A Scheme for Integrated Multi-banking Solution" International Journal of Computer Applications (0975 – 8887) Volume 29– No.7, September 2011

[14] Gokul.R, Godwin Rose Samuel.W, Arul.M, Sankari.C, "Multi account Embedded ATM card", "International Journal of Scientific and Engineering Research", Volume4, Issue-4, April-2013.

[15] Harshal M.Bajad, Sandeep E.Deshmukh, Pradnya R.Chaugule, Mayur S.Tambade, "Universal ATM Card System", "International Journal of Engineering Research and Technology", Volume-1, Isssue-8, October-2012.