IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

ATM Transactions Security using Biometric Authentication

Kranti S. Bhoyar
Department of Electronics and Telecommunication Engineering
Mauli Group of Institution, College of Engineering and Technology, Shegaon, Maharashtra, India
krantimauli@gmail.com

Abstract: *Due to advanced development in science and technology, innovations are being built-up with strong security. But on another side, threats are also imposed to destroy the security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still in trouble due to thefts and frauds. The existing banking system uses ATM card and a PIN which increases threats of stolen cards, Personal Identification Number (PIN) cannot provide protection against identity theft. Anyone carrying the card can access the account if they know ATM card PIN. To overcome these threats hybrid system which consists of conventional features along with additional features like face recognition, biometric finger print recognition and one-time password (OTP) is used. Database holds information about a user's account details, images of his/her face, finger print ID and a mobile number which enhance security to a large extent. First, the user needs to place finger on finger print sensor. If system is unable to identify authenticate finger, a live image is captured automatically through a webcam installed on the ATM, which is compared with the images stored in the database. If it is identical with stored image, an OTP will be sent to the corresponding registered mobile number. This OTP has to be entered by the user in the text box. If the user correctly enters the OTP, the transaction can proceed. Thus, the combination of face recognition algorithm or finger print authentication and an OTP reduces the chances of fraud and free a customer from remembering complex passwords. It finds the valid or invalid user and avoid the wrong person to access the ATM.*

Keywords: ATM, Biometrics, Fingerprint Authentication, Face Recognition, PIN, OTP

I. INTRODUCTION

ATM is an automated teller machine that provides facility of financial transactions to the customers, anyone can withdraw cash anywhere at any time of day and night. When debit or credit card is inserted into the ATM, it reads the information encoded on the magnetic strip on the back of the card. That magnetic strip is encoded with unique card number, expiration date and personal identification number (PIN). ATM card is basically a hard copy to access information of account. The ATM then asks for PIN to verify authorization to access account funds and information. When PIN is verified, the ATM communicates with bank to access account information. It can then display account balance or distribute cash from bank account balance. Online banking need to possess high level security in order to provide safe, consistent, online environment which guarantees secure data transmission and identity of both bank and customer.

Digital transaction is cheaper for banks to provide and it enables more customer-centric strategies, empowering users to access banking services whenever and wherever they want. But it also creates new vulnerabilities. Customer awareness of online security risks is often poor and there are possibilities to leak confidential data to criminal groups that can then be used to fraudulent transactions. Today we observe lack of security in ATM transactions. If an ATM card is lost, it can be misused .Many of the people even after having knowledge of not to share OTP with others, commits that mistake. When there are multiple ATM machines in ATM, there will be more than one person inside the ATM and there is a chance of noticing PIN which can be used to fraudulent transactions. Traditional manual methods of fraud monitoring and detection have neither the capacity nor the speed to meet the challenge facing banks today. This study focuses on the security beyond existing mechanisms.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

II. LITERATURE SURVEY

M. Srilatha[1], In this paper, alphabet technique is used. During the account opening, security code and unique security alphabet is provided by the bank to the user. Various alphabetical keywords are generated during the access of ATM card by user, to enter security PINs. If the hacker tries to access the account, a notification is sent to the user as a SMS in mobile.

Murugesan M [2], By comparing the image taken in front of the ATM machine to the images of database, the users are verified. If the user is authentic the new image is used to train the model for further accuracy, a web link is sent to the registered mobile number who owns the ATM card, to verify the access of the user to his/her account only then the user is considered as a authentic user. Histogram algorithm and Machine learning techniques are used to identify the personals using the machine.

Nischal Bansal [3], This paper focus on mobile banking and ATM withdraw money, Customers, who wants to withdraw the cash, will login in their Mobile banking and withdrawal of cash just like ATM machine using "Cash withdrawal" feature. After cash withdrawal is completed on Mobile, transaction is not completed actually and there is no change in account balance; because customer did not get any cash yet. For security reason, a new password (OTP) is provided to complete the transaction on ATM machine, it has many disadvantage user must have activated mobile banking, must have smart phone with banking app.

Kavita Hooda [4], This paper focuses on security of ATM system. It focus to design a module of an ATM simulator based on face recognition from 3 different angles in order to minimize frauds associated with use of ATM systems.

Krishna Nand Pandey [7], This paper focus on the solutions for the ATM security issues. It uses fingerprint or One Time Password (OTP) verification along with the use of ATM pin. The database of the customer including fingerprint and mobile number is maintained by bank. The ATM card along with its PIN will be provided. After entering the ATM pin, the customer will be asked to select 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 do 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 mobile number. This system has main drawback of lengthy process as well as if anyone with OTP and ATM pin can withdraw money as it optional to use finger print authentication.

III. PROPOSED SYSTEM

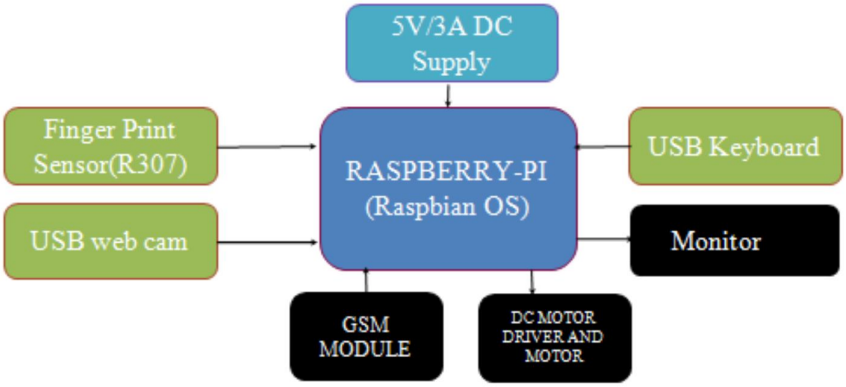

Figure 1: Block Diagram of ATM transactions Security using Biometric Authentication

3.1 Working Principle

This embedded system mainly consists of Raspberry – Pi, Web cam, Fingerprint sensor and DC motor to show the trailing movement Heart of the system is raspberry –pi, single board computer (SBC), which can handle complicated calculations and it's just credit card size computer. Raspberry –pi needs an operating system to do its work. Raspbian is the "official" operating system of the Raspberry Pi. Raspberry-Pi has USB ports to connect any USB peripheral like USB to serial converter and the port will act as UART, one can interface USB keyboard and mouse to the raspberry-Pi. In this system USB keyboard is attached to select options like balance check, withdraw cash etc. Keypad is used to insert required data during user registration. USB web camera is capable of taking high-resolution photographs, along with full HD 1080p video,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

and can be fully controlled programmatically .System uses web cam to capture images and forward that frames to the Open-CV for further processing. To select and open interfacing options the cursor keys are used, and then camera is selected to enable the camera.

R307 Fingerprint Module is used for fingerprint verification, it consist of high speed DSP processor, optical fingerprint sensor, high-performance fingerprint alignment algorithm, high-capacity flash chips and other hardware and software composition. R307 sensor is capable of storing 1000 unique id in its data base, in searching mode, as soon as user puts finger on sensor it search for the valid id, as it find the id it will inform the controller that it has found the valid id. The R307 fingerprint module has two interface TTL UART and USB2.0, USB2.0 interface can be connected to the computer; RS232 interface is a TTL level, the default baud rate is 57600 , can be changed, refer to a communication protocol . R307 fingerprint module is a fingerprint sensor with a TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person. TFT LCD monitor is interfaced with raspberry –pi with the help of HDMI to VGA converter, some of the TFT monitors come with HDMI port so it takes less efforts to connect display with the raspberry-pi, a display is needed to show user activities, user will be able to do interaction with the system with the help of attached keyboard to enter password and select some options that will be promoted by the system on screen.

To show some trailing activities DC motor is used to show some mechanical movements are ongoing to order the dispense of cash, it's impossible to interface and supply current to the DC motor directly from the Raspberry-Pi as raspberry's GPIO's are not capable to supply current more that 20mA that called an sourcing capacity of GIO pins, Hence to drive the motor using raspberry- pi an driver IC like L293D is needed, The L293D is a popular 16-Pin Motor Driver IC. As the name suggests it is mainly used to drive motors. A single L293D IC is capable of running two DC motors at the same time, also the direction of these two motors can be controlled independently. The power supply requirements differ by Raspberry Pi model. All models require a 5.1V supply, but the current supply requirement generally increases according to model. All models upto the Raspberry Pi 3 require a micro USB power connector, while the Raspberry Pi 4 uses a USB-C connector.

3.2 System Flow

The flowchart shows the overall flow of the system. When bank customer is going to visit ATM station he/she has to go through the following flow.

1. At first step ATM machine wait for the user finger for doing further actions, while waiting it shows "PLASE PLACE FINGER ON SENSOR" message on LCD monitor and finger print sensor R307 will keep waiting for finger.
2. Once R307 sensor found the finger placed on it, immediately it start scanning it and if the sensor found any finger print ID related to placed finger in its data base of ID's, Sensor reply to the Raspberry-pi using UART protocol that the ID found. In case of the finger placed is not valid the R307 Sensor send the ERROR message to the Raspberry-pi.
3. By using response from the R307 sensor Raspberry-pi take action, if sensor returns ID it has found then raspberry-pi system will jump to generate OTP. Otherwise sensor returns the ERROR message and raspberry-pi will jump to the face detection step.
4. If system fails to verify the valid finger print, then system asks the user to show his face to the camera.
5. Once raspberry –pi find the face with the help of Open CV, it also find the name associated to the face, name that represented by the face detection algorithm is compared with the name that has been inside MySQL database, if there is name matched then raspberry –pi execute MySQL query and extract all information of that user like name, mobile number, account balance etc. Thus system verifies and validates the identity of the user and system will jump to generate OTP.
6. OTP verification is done with the help of randomly generated 4 digit code, this code is then forwarded to the registered mobile number that has been extracted from the MySQL database.
7. OTP generated by the system is valid only for 2 min, if user are not able to verify the OTP that has been received on registered mobile number, in this case user receives new OTP.
8. OTP is forwarded with the help of GSM module SIM800L that can be controlled using AT command.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

9. The OTP received by the user is entered into the ATM machine by pressing the keys on the keypad. After entering it checks whether it is a valid or not. If it is valid it allows the customer further access, user can choose the action like show account balance, withdraw cash etc.
10. The user can withdraw cash or carry out tasks related to its service in the ATM. After choosing any action, and after performing the action user returns to choose action menu.
11. When user select the withdraw action, the action indicated with the help of DC motor like ATM is dispensing cash, after valid transaction amount withdrawal, message is forwarded to the registered mobile no.
12. If user choose exit action, the session is ended.

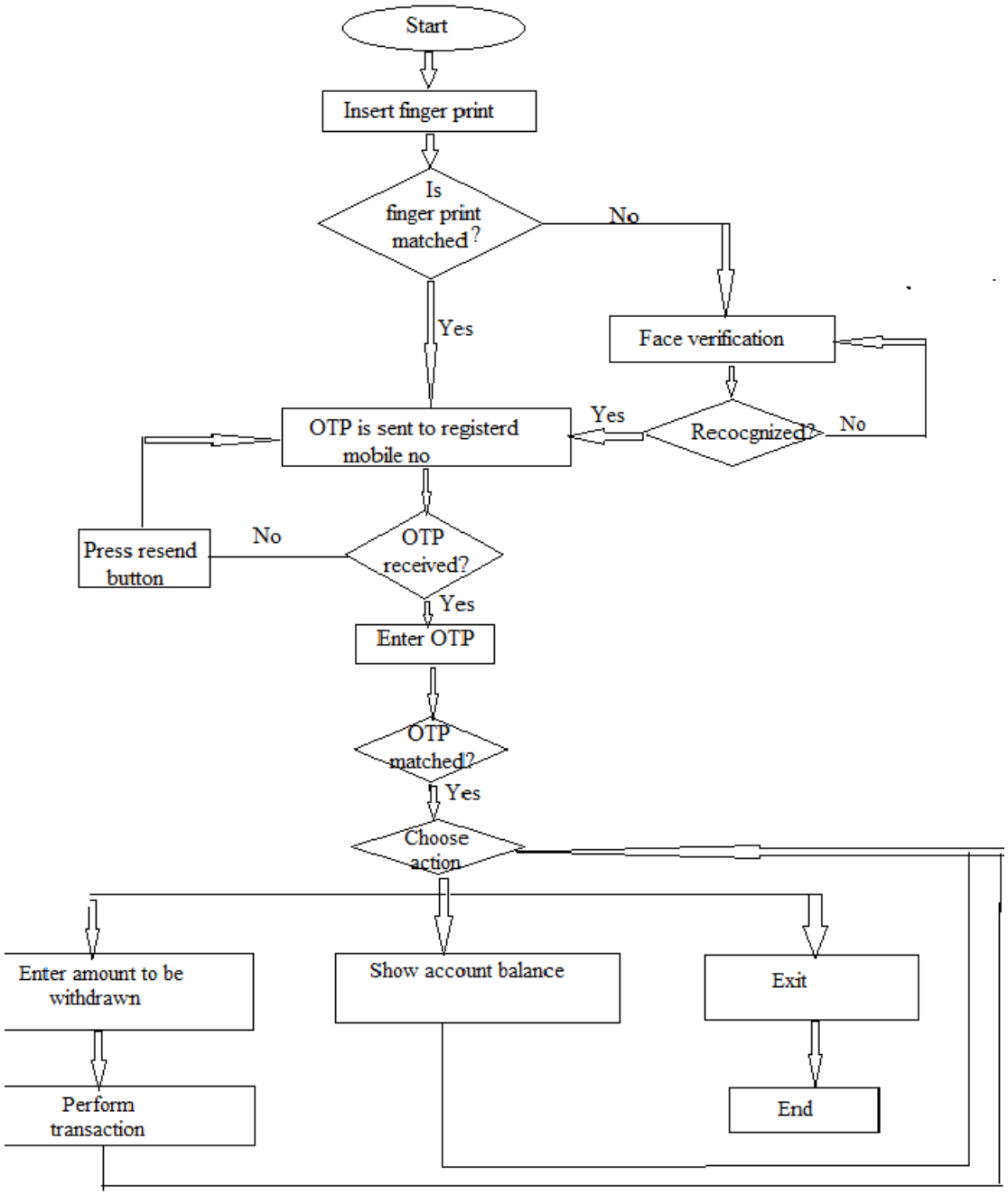

Figure 2: Flowchart

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

3.3 Open CV and Face Verification

Phases of face verification are:

1. **Face Detection and Data Gathering:** Dataset is created, where we store each id, a group of photos in gray with the portion that is used for face detection. Detecting faces in the image (photograph) or video stream is the first step. "Haar Cascade classifier" is used for detection of face. One of the primary benefit of Haar cascades is that its speed is higher than others classifier.
2. **Trainer:** After that, all the images in data is passed to this pre-trained network. Specific OpenCV function is used for it. The result is in a.yml file that is saved on a "trainer/" directory.
3. **Recognizer:** Here, face is captured on camera and if this person had his face captured and trained before, recognizer will make a "prediction" returning its id and an index, shown how confident the recognizer is with this match.

IV. IDRBT (THE INSTITUTE OF DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY)

This institute designed a network called NFS i.e. National Financial switch network which gives 24/7 access for inter connecting the ATMs in country through which it is possible to make transaction from any nationalized bank within the country, this network provides access to the user data which is stored in database at bank side, like user name, address, register mobile no, user ID, and biometric data i.e. images and fingerprint samples of the user which is already provided during enrollment at bank side.

V. CONCLUSION

This system is very helpful in case of card less transaction and it gives an alternate option of face or finger print verification, so it will be convenient to do transaction very well. These alternate options ensure the bank customer must get cash at ATM. It avoids the need to remember password. OTP verification is also used along with biometric or face verification this increases the authentication, it is also called as two step authentication. This system is more reliable and secured. The system is built on embedded technology which makes it user friendly.

REFERENCES

[1]. "Safety and maintenance of ATM system using Internet of things" M. Srilatha, G. Sai Meghamsh, AIP Conference Proceedings 2407, 01 December 2021.

[2]. "Securing ATM Transactions using Face Recognition" Murugesan M, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9 No.2, March -April 2020.

[3]. "Cash withdrawal from ATM machine using Mobile banking," N. Bansal and N. Singla, 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), New Delhi, India, 2016, pp. 535-539, doi: 10.1109/ICCTICT.2016.7514638.

[4]. "ATM Security" ,Kavita Hooda ,International Journal of Scientific and Research, volume 6,issue 4, April 2016, 159 ISSN 2250-3153.

[5]. "Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication" Frimpong Twum , Kofi Nti &Michael Asante, International Journal of Science and Engineering Applications ,Volume 5 Issue 3, 2016, ISSN-2319-7560

[6]. "Enhanced security for ATM machine with OTP and Facial recognition features" Mohsin Karovaliyaa , SaifaliKarediab, Sharad Ozac&Dr.D.R.Kalbanded, International Conference on Advanced Computing Technologies and Applications (ICACTA-2015).

[7]. "ATM transaction security using fingerprint/OTP", Krishna Nand Pandey, Md. Masoom, Supriya Kumar & Preeti Dhiman, International Journal of Emerging Technologies and Innovative Research , ISSN:2349-5162, Vol.2, Issue 3, page no.448-453, March-2015.

[8]. "Biometrics to Control ATM scams: A study",Ahmad Tasnim Siddiqui, International Conference on Circuit, IEEE, Power and Computing Technologies (ICCPCT), DOI: 10.1109/ ICCPCT32810.2014 . 05 March 2015.

[9]. Atm Security Improvement Using Finger Print" Neelam Verma, Rakesh Patel,Priya Bag Global Journal Of Engineering Science And Researches, oct 2014, ISSN 2348 – 8034, page 72-77.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, April 2022
Impact Factor: 6.252

[10]. "Implementation of ATM Security by Using Fingerprint recognition and GSM", Pennam Krishnamurthy, Mr. M. Maddhusudhan Redddy, International Journal of Electronics Communication and Computer Engineering ,Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X,(2012)

[11]. "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study" Onyesolu Mo, &Ezeani IM ,International Journal of Advanced Computer Science & Applications; 2012,Vol3,no.4,pp,68-72.

[12]. " Enhanced Atm Security System Using Biometrics" Prof.Selinaoko&Jane Oruh, ,IJCSI ,Issue,Vol.9 Issue,No.3,September 2012

[13]. "Fingerprint Matching", Anil K. Jain, Jianjiang Feng, Karthik Nandkumar, IEEE. Computer Society 2010,pp.36-44.0018-9162/10.

[14]. "Ridge Enhancement in Fingerprint Images Using Oriented Diffusion", Robert Hastings, IEEE Computer Society on Digital Image Computing Techniques and Applications, pp. 245-252, (2007).

[15]. "Fingerprint Recognition by Combining Global Structure and Local Cues", Jinwei Gu, Jie Zhou, and Chunyu Yang, IEEE Transactions on Image Processing, vol. 15, no. 7, pp. 1952 – 1964, (2006).