Securing ATM Transaction with OTP and Facial Recognition Features

Rutuja Naval[1], Ankita Khot[2], Samruddhi Khedekar[3], Manjushree Sangale[4]
B.E. Student, Department of Computer Engineering, NBN Sinhgad School of Engineering, Ambegoan, Pune[1,2,3,4]

Abstract: *To avoid the ATM robberies and wrong person misuse the ATM in order that we will make them to the lead their life safely and securely. The proposed system is meant supported the intelligence system to make sure that the ATM usage with none hesitation and make the planet to be a component of digitization. Once customer inserts the cardboard into the ATM, then a session is started, the system starts face detection using the camera installed in the ATM and create a short-lived identity database for the customer and user face verification is performed on the ATM. Valid user would continue the conventional process but the Invalid user cannot be accessing the ATM card so that they give the secondary password to the system automatically therefore the unauthorized person would continue the transaction.*

Keywords: ATM, Security, Fraud, Face Recognition, LRR, OTP, etc.

I. INTRODUCTION

The present ATM security authentication technique it is dependent on the pin-based verification. Factors such urgency, memorization of pins, speed of the interaction, unintentional pin sharing effects of the system diversely. Cards with magnetic chips is easy to clone. The security and vulnerability are the opposite sides of the same coin, an automated machine becomes vulnerable due to a weakness of its security. Automated teller machine manufactures go on adding and strengthening security features of Automated teller machine so that customer can carry banking transactions without any difficulty and fear of siphoning of amount from their account and the same frauds works with similar speed to crack the innovated security feature so that they can have access over the Automated teller machine to exploit the accounts of bank customers.

In order to provide an authentic security solution to the people, the concept of ATM security. system based on face verification is emerged. The Project work is a basically focused on Design and Implementation of face verification-based ATM Security System using LRR algorithm. Limitations of a existing system are overcome in our proposed system. In order to make any transaction, system will provide to option to process. First Self user, where in system will ask for "Verify Face" and allow to process transaction if it matches with image store in banks database otherwise system will reject the transaction after couple of warnings.

II. LITERATURE SURVEY

[1] ATM Security Using Fingerprint Biometric Identifier: An Investigative Study (Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani)

The growth in electronic transactions has resulted in a greater in demand for fast and accurate for user identification and authentication. Access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge of like a social security number and a password are not all together reliable.

[2] Face detection is based ATM security system using embedded Linux platform (Jignesh J. Patoliya, Miral M. Desai)

In order to provide a authentic security solution to the people, the concept of smart ATM security system is based on Embedded Linux platform is suggested in this paper. The study is focused on Design and Implementation of the Face verification based on ATM Security System using Embedded Linux Platform. The system is implemented on the credit card size is Raspberry Pi board with an extended capability of open-source Computer Vision (OpenCV) software which is a used for Image processing operation. High level security is framework is provided by the consecutive actions such as initially system is capturing the user face and validate the user face is verified properly or not.

[3]. Enhancing ATM security via face recognition (K John Peter; G. Gimini Sahaya Glory, S. Arguman, G. Nagarajan, V. V. Sanjana Devi)
A facial recognition system is an application for automatically verifying a user from a digital image or a video frame from the video source. Proposed paper uses face for recognition technique for verification in ATM system. For face recognition, there are two types of a comparisons. The first is verification process, where the system is compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification this is the where the system compares the given individual to all the other individuals in the database and it gives a ranked list of matches.

[4] IBIO-A new approach for ATM banking system (V. Rajesh, S. Vishnupriya)
Security and Authentication is individuals is necessary for our daily lives especially in ATM. But the security is a provided with ATM systems has some back doors. It has been improved by using biometric verification of techniques like face recognition, fingerprints, voice and other traits, comparing these existing traits, there is still need for considerable computer vision. Iris recognition is a particular type of biometric system that is used to reliably identify a person uniquely by analyzing the patterns found in the iris.

[5] Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology. (Raj Gusain , Hemant Jain , Shivendra Pratap)
The objective of this paper is to design a bank locker security system in which is using face recognition process, Iris Scanner and Palm Vein Technology (PVR) for securing valuable belongings. A face recognition is a system which identifies and authenticates an image of an authorized user by using MATLAB software. The images of a person entering an unrestricted zone are taken by the camera and software that compares the image with an existing database of valid users. Iris Recognition system is uses generous characteristics present in user body. This technology is designed for biometric authentication in ATM's Immigration border control, public security, hospitality and tourism etc.

[6] Secured Banking operations with face-based Automated Teller Machine. (Olutola Fagbolu, Olumide Adewale Boniface Alese and Osuolale Festus)
With an introduction of the newest Automated Teller Machine (ATM) at Royal Bank of Scotland which an operates without a card or authentication by entering Personal Identification Number (PIN) to withdraw cash up to £100, a more secured ATM system can be a designed and implemented with a more secured feature of biometric facial recognition as PIN. Security is an essential issue in banking operations; with a coming of technology such as e-banking, mobile banking etc. security has become an issue that is needs utmost preponderance.

[7] Face Recognition as a Biometric Security for Secondary Password for ATM Users. A Comprehensive Review. (Lusekelo Kibona)
Authentication is an important aspect in a system control in computer-based communication. Automatic Teller Machines (ATMs) are widely used in our daily lives due to their convenience, wide-spread availability and time-independent operation. In this paper, the author is tried to a review some framework used in a dealing with security attacks posed to ATM users and found that there are some attacks related with a using card-based security

application so there is a need to mix up another secondary security after the primary stage has been cleared and that secondary stage is facial recognition security system is an explained in an algorithm developed in this paper.

[8] One touch multi-banking transaction ATM system using biometric and GSM authentication. (Apurva Taralekar, Gopalsingh Chouhan, Rutuja Tangade, Nikhilkumar Shardoor)
Every individual has multiple bank accounts in a different bank, people's need to carry multiple ATM cards for a transaction, there may be different PINs for every account. In traditional system, ATM terminal customer recognition systems only rely on bank cards, security pin number, and such as identity verification methods which measures are not perfect and functions are too single and at times there are incidents where as we forget our security PIN number, lose our cards, cards get a stolen, stolen PIN numbers.

[9] A Survey on the Security of an ATM Transaction. (Joyce Soares, Dr. A. N. Gaikwad)
The previously used signature based on system was replaced by a pin number in an ATM system. But due to a risk of fraudulent activities the pin number was replaced by a biometric system. The biometric system is may be a fingerprint, iris, retina, veins, etc. In this system the cash would be a dispersed only if the user is an authenticated person. Further direct or spoofing attacks have a today motivated us to enhance
the security of the biometric system by using image quality an assessment for liveness detection.

[10] A SECURE ATM CARD VERIFICATION BASED ON FACIAL RECONGINITION AND OTP. (R Gayathri devi, G.Nagarajan and R Sureka)
ATM is a machine which is used for hand out and deposit money. ATM processor is an Automatic Teller Machine, In modern ATM machine the user will be insert a plastic ATM card which has magnetic chip or a plastic smart card which is has a chip which contains an unique card number and content of few security information such as an expiration date or CVVC. Each ATM card has unique number is called PIN number which provide authentication. Personal identification number has four digits which is randomly chosen. Sometimes it is also in a sequence order, it is based on an account which is provided by the bank.

III. SYSTEM ARCHITECTURE

A) Existing System
The present ATM security authentication technique is a dependent on pin-based verification. Factors such as urgency, memorization of pins, speed of an interaction, unintentional pin sharing affects the system diversely. Cards with magnetic chips are easy to the clone. The security and vulnerability are an opposite side of the same coin, an automated machine becomes vulnerable due to a weakness of its security. Automated teller machine manufactures go on adding and strengthening security features of Automated teller machine so that customer can carry banking transactions hassle free and without any fear of siphoning of amount from their account and the same frauds works with similar speed to crack the innovated security feature so that they can have access over the Automated teller machine to exploit the accounts of bank customers.

Limitation of existing system

1. **Shoulder Surfing**
   Shoulder surfing is a way of looking an over someone's shoulder, to get information. In a crowded environment, it is very easy and effective to stand beside a fellow and watch how PIN numbers are an entered at cards terminal.

2. **Spoofing**
   Spoofing is an impersonation, getting access and taking advantage of someone else's account.

3. **Skimming**
   This involves the use of card skimmer devices by fraudsters to get a card detail from the magnetic chip. These devices are usually an installed inside or over the top of an ATM card reader.

4. **Card Trapping/Phishing**

Card trapping and Phishing attempt to a steal card as the customer insert it into the ATM for transaction. A device is placed over or inside the card slot to a capture the consumer's card. These is devices are designed to prevent the card from being returned to the consumer after transaction.

Proposed System:

In order to provide a reliable security is solution to the people, the concept of ATM security system based on a face detection is emerged. The Area of work is a basically focused on Design and Implementation of a Face Detection based on ATM Security System using the LRR algorithm. Limitations of existing system is a overcome in our proposed system. In order to make any transaction, system will provide to option to process. First Self user, where in a system will ask for "Detect Face" and allow to process transaction if it matches with an Image store in banks database otherwise system will be declining the transaction after couple of warnings.
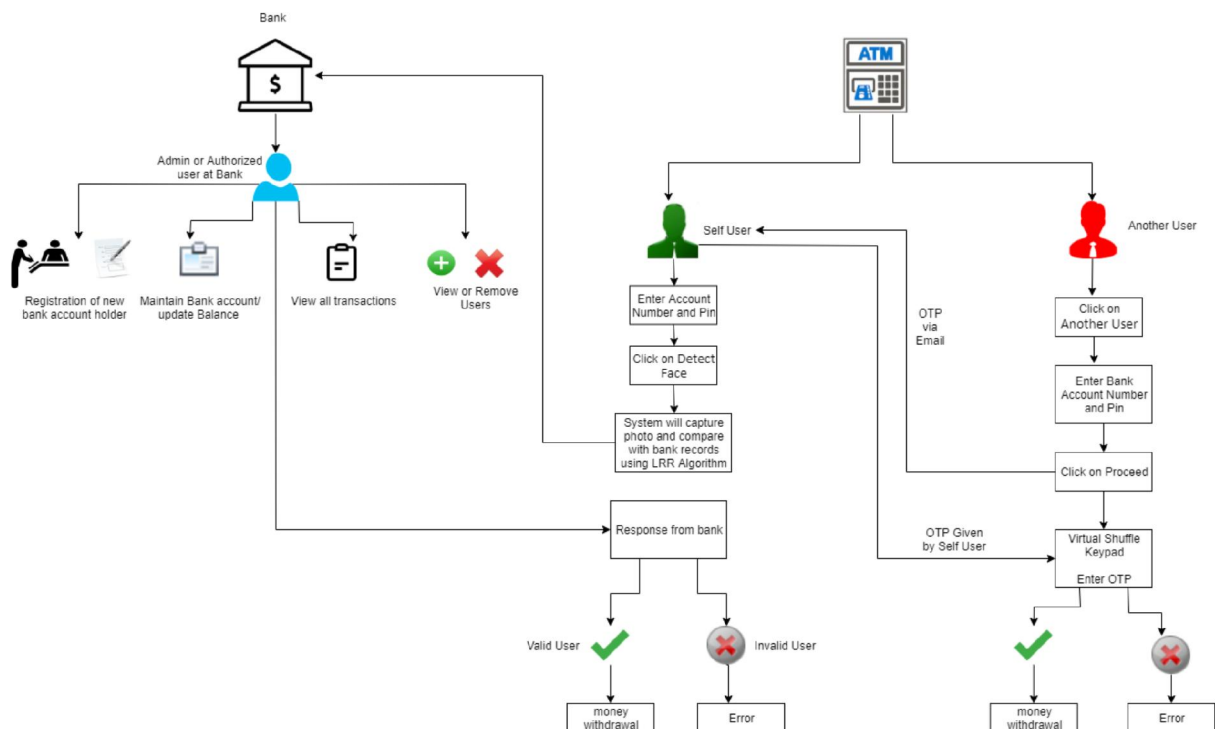
Figure 3.1: Proposed System Architecture Diagram

Advantages:
1. Provide more secure banking experience.
2. Multiple option to withdraw money.
3. Shuffle keypad to add extra security level.

IV. SOFTWARE REQUIREMENTS SPECIFICATION

A. Functional Requirement

The System has following Module:

- ATM System
- User login
- Bank

1. ATM System

System provides an interface where end user has an option to make the transactions. First using the "self-user", where user is a prompted for face detects option and second is "Another user" where user is a prompted to enter the account number, OTP, shuffle keyboard.

2. User Login

User logins to the system using convenient option and make the transactions.

3. Bank

Al the users of ATM are registered customer of bank. Where all the required information of customer are stored like Profile picture, Mobile number, Name etc.

B. Software Interfaces

- Technology: Advance JAVA(J2EE)
- Front End: JSP, PHP
- Back End: SQLOG/XAMPP Server
- Operating system: WINDOWS 7 and above
- Server: Apache tomcat
- Browser : Internet Explorer, Firefox, Chrome.

V. CONCLUSION

Biometric Authentication with smart cards is a stronger method of authentication and verification as it is uniquely bound to individuals. An ATM model that is more reliable in providing security by using facial recognition Software along with OTP. We can have safe and secure transaction. If we use PIN number hackers can easily crack the PIN number by fixing the camera near ATM machine. ATM plastic card

consist of sixteen-digit serial number, while inserting the card in ATM machine the sixteen-digit number is scanned using some of the tools and it is stored in their database so, hackers can easily fix to those numbers in a duplicate plastic card and an enter the PIN number finally they process the transaction and they get a money.

So many of the transaction process goes wrongly by using PIN number This is avoided if we use Face recognition system. The security level is getting a secured. By the use of OTP concept, we can also have safer transaction. If a hacker tries to crack a PIN number, he/she is a supposed to enter the OTP. Definitely they will enter a wrong OTP, immediately an alert message is sent to the person phone number. Then the transaction process is got failed. It is really useful because in this concept we added two level security system.

REFERENCES

[1] Rupinder Saini, Narinder Rana, Rayat 'Comparison of various biometric methods', Institute of Engineering and IT, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I (March 2014).

[2] Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450- 2275 issue 21.

[3] A. Forouzan, Cryptography and Network Security, Tata McGraw Hill.

[4] Anil K. Jain and Arun Ross. Introduction to Biometrics. In Anil K. Jain, Patrick Flynn, and Arun. A. Ross, editors, Handbook of Biometrics. Springer US, 2008.

[5] Rafael C. Gonzalez and Richard E. Woods, Addison Wesley, Digital Image Processing.

[6] Ekenel HK, Stallkamp J, Gao H, Fischer M, Stiefelhagen R, Face Recognition for Smart Interactions, interact Research, Computer Science Department, University at Karlsruhe.

[7] Sezin Kaymak, "Enhanced Principal Component Analysis Recognition Performance".

[8] Vinay Hiremath and Ashwini Mayakar, Face recognition using Eigenface approach. "Enhanced Principal Component Analysis Recognition Performance".

[9] Aru, Okereke Eze, Ihekweaba Gozie, Facial Verification Technology for Use in Atm Transactions.

[10] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013), PP 22-29.