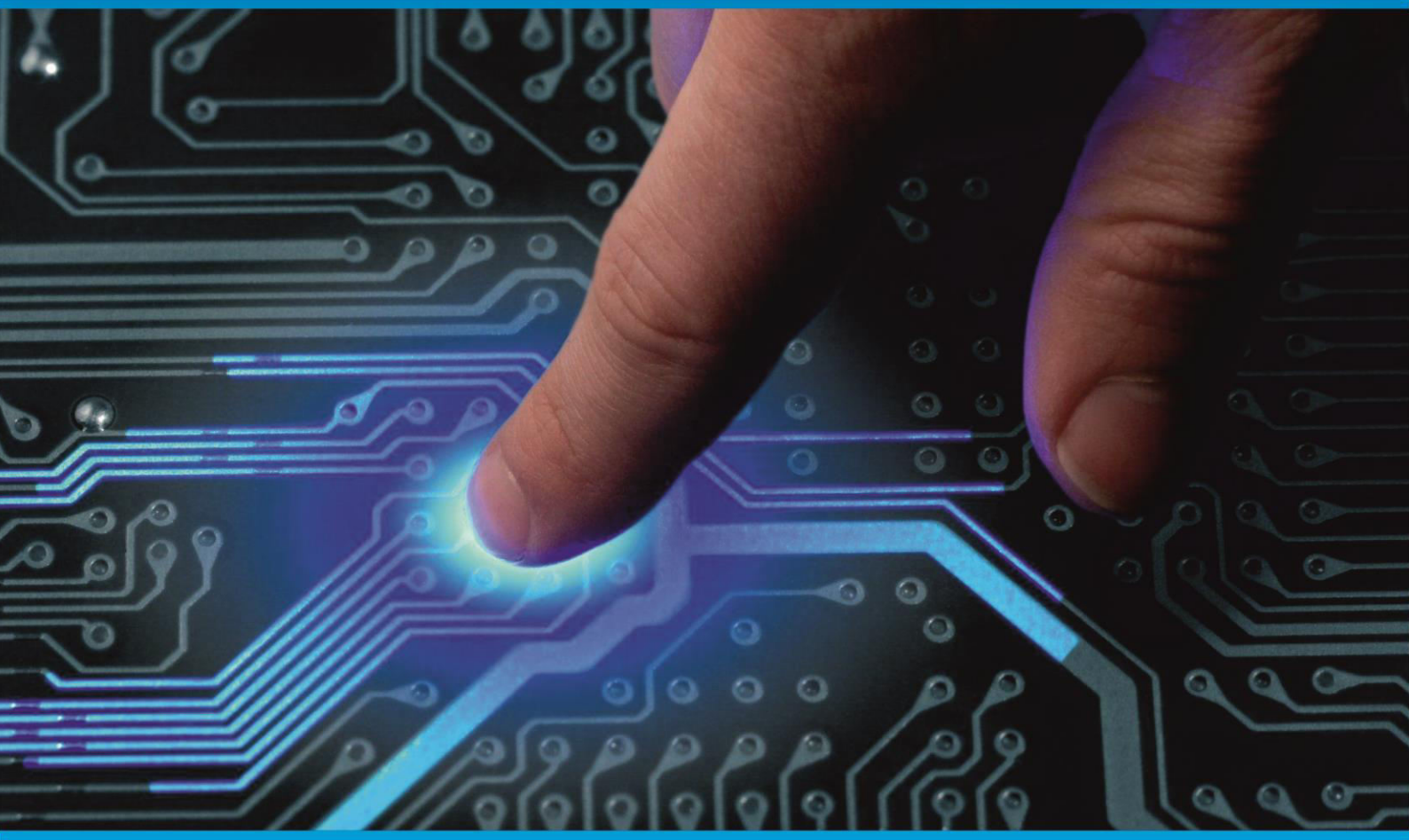
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 2, February 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902013 |

ATM Security System using Face, OTP and Vibration

Siddhesh Jadhav, Mayuresh Ughade, Pratik Patil, Ashish Baris, Prof. P.R.Patil

Department of Computer, KJEl's Trinity Academy of Engineering, Pune, MH, India

ABSTRACT: Automated Teller Machine (ATM) transactions are found safe, reliable and inevitable these days for fulfilling our financial commitments. Traditional approach for using ATM mandates involvement of Debit card. But however, people do experience times when their account lacks balance amount or they forget to carry card and struggle to complete transaction. We know that, parallel to ATM usage, mobile phones' usage has also been an inevitable trend. Establishing a connection between these e-gadgets has ignited a simple and effective approach to withdraw cash without the involvement of debit card which can be referred to as card less cash withdrawal. Face detection and Fingerprint is used for authentication of user. This along with OTP comprises three levels of security. When face and OTP are matched then customer's account will open in ATM machine. Vibration sensor interfaced with system via USB to TTL, alerts authority is someone tries to break into ATM forcefully.

KEYWORDS: ATM, Vibration sensor, Face and OTP

I. INTRODUCTION

The present day ATMs are using pin based security. When we are about to carry out the transaction, the pin number is fed as the input which is encrypted at the client side and the data is decrypted at the server side. When the comparison gets satisfied, we can carry out the transaction. As the technology is getting improved, the crackers are easily retrieving the data and hence the frauds are going on increasing. The data are made available on cloud [4], so that the transaction time gets reduced. When the data is available in the cloud, data can be easily retrieved for fraudulent activity, which is the biggest drawback. Hence the only way to secure the datum is to replace the computer generated numbers with the biometric security.

The needs for virtual card or card less ATM came to our mind after one of the authors left with disappointment at the ATM. He was unable to locate his ATM card from his purse. Hence access to his bank account for bank transaction was denied. When narrated his experience. One major conclusion came to our mind after hours of thought and reasoning as regards the need for ATM card before one can access his bank account through ATM, and major information that ATM card contain. Consequently, as a lecturer, researcher, computer/electronic engineer and computer scientist with keen interest in emerging new technology in electronic business, that EATM with virtual or no card can be design to enhance the efficiency of ATM usage. Also, In recent time many lapses (ranging from fraud, stealing, etc.) of ATM usage has been attributed to use of ATM such as card cloning, card damaging, card expiring, cost of issuance and maintenance, accessing customer account by third parties, waiting time before issuance card etc. all these can be a bygone issues if card less EATM can be design and implement in future.

II. LITERATURE SURVEY

An In recent years, cash withdrawal through ATM cards has seen an increase in the number of card related frauds; card cloning, shoulder surfing, fake keyboard, skimming etc. being a few of them. To combat these problems, Khushboo Yadav et al [1] proposed a Secure Cardless Transaction System- a method which would eliminate the usage of ATM PIN and physical cards altogether and hence provide a secure environment for cash withdrawal. The concept of User-Generated One Time Password (OTP) has been introduced in this project. With all these modification in existing systems, the robustness of the machines will increase.

Md. Al Imran et al [2] analyzed their protocol and found some flaws on this. This protocol doesn't specify what if it is off us transaction. Besides, customers get different categories of services but this protocol cannot determine which customer will get which category of services. That is why, inspired by this protocol we have proposed a modified model for getting same transaction facilities as exists which uses BPIN that will determine the bank identity (B) and a

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902013 |

random Personal Identification Number (PIN) and One Time Password for authentication of the customer instead of biometric fingerprint because of major disadvantage of biometric authentication. And obviously it will use no card for accomplishing the transaction.

"OTP Based Cardless Transction using ATM" [3] proposed a secure, robust and flexible biometric authentication system which combines two methods that use a Biometric and a proximity sensor. To increase the security level in ATM transaction this proposal integrates a biometric fingerprint technique along with a shuffling keypad method. Here the card is replaced with the fingerprint, which is registered during the opening of a bank account and PIN number is entered in a shuffling keypad. To avoid the shoulder-surfing attacks with or without concealed cameras in PIN entry, this approach uses a shuffling keypad which uses a proximity sensor to shuffle the keypad during the PIN entry. The system is tested with multiple users and has obtained 100% accuracy. This system avoids the misuse of electronic cards and supports a secure transaction.

An automated teller machine (ATM) is an electronic telecommunications device that helps customers of banking departments in transactions and transfer of money in their accounts. The customer enters their unique personal identification number (PIN), i.e. stored in the chip of the card. Due to an increase in the installation of ATM and the number of ATM cardholders, the number of cases of fraudulence has also increased radically. The advancement in technology has resulted in an increase in various skimming activities. So, developments are incorporated in the existing systems to make it more secure, convenient and reliable. The employed secured system must have high speed and must be durable. The design presented in [4] is unique because of biometric scanners such as Iris scanner and the two-way check with fingerprint scanner makes it more reliable. The iris scanner being the primary security check lets the system access the further steps for transaction. Fingerprint scanner embedded in the ATM card acts as the secondary security check for the system. The transaction procedure is successful only if the input data by the card holder matches with the database. It consumes less energy that makes it suitable for use. The suggested modified system is pragmatic moreover economical when correlating to the alternative existing classification and affirmation processes of ATMs.

Nowadays iris recognition is getting more popular in terms of security. Iris pattern is more stable with ages, uniqueness and acceptability. Because of its high reliability and good rates of recognition, iris recognition is therefore used for highly secure locations. With the arrival of ATM banking has become much easier and it has also become more accessible. The product (ATM) it is manifold due to the highly increasing risk of intelligent criminals. Due to which the banking services are in danger and not secure. This situation is getting progressed as huge progress is made in biometric recognition techniques like fingerprint and iris scanning. Customers password can be encrypted using selective article points. Therefore, a system is needed which is more secure and provides safe transactions and also help from various frauds. System described in [5] is more secure and fast and helps to provide better facilities.

The objective of [6] is to consider smart phone in Near-Field Communication (NFC) Card Emulation mode as an alternative to ATM cards. In NFC the distance between the respective devices needs to be very small (typically less than 4 cm) which makes NFC ideal for making payments and for other transactions involving sensitive/private data. In the proposed system, in order to authenticate at the ATM kiosk, the user needs to swipe his/her smart phone in front of the NFC reader. An ATM card is not required for authentication and the system will still have a stronger security compared to the system in which ATM card was used. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

Paper [7] aims is to prevent the crime related to ATM card frauds and secure transaction. In this paper, two options are included like One Time Password (OTP) and Fingerprint detection for a successful transaction. The user can use any of the two options mentioned above for ATM transactions. We know that the OTP is valid for only one transaction and a specific duration. Thus, the Global System for Mobile (GSM) is used for the generation of OTP and that OTP is sent to the mobile number to which the bank account is linked. In case, if the user does not have the mobile to which the bank account is linked or else the mobile is switched off or network problem the second option of fingerprint authentication can be used. The fingerprint of the user must be linked with the bank account so that the unique pattern of the fingerprint can be used to make a successful transaction. Hence this project will increase security and add privacy by making use of biomedical authentication that is fingerprint pattern detection. Therefore this added feature helps to reduce the crimes related to ATM cards.

The proliferation of ATM Fraud case in Indonesia is still the main concern for the society especially bank customers. In March 2017, a total loss of 5 billion rupiah was recorded as a result of ATM Frauds. While the only solution which

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902013 |

ensures security of ATM machines is a 6-digit PIN, there are still a lot of security cracks that can be used by the criminals to steal customer data and the 6-digit PIN itself. One of the most frequent method of ATM Fraud is skimming. Therefore, the authors bring the concept of Fingershield ATM, ATM Machine that implements biometric identification in the form of fingerprints which is integrated with smart card and database server. Fingerprint technology is powerful identification because of its unique characteristics of each of the minutiae. Despite the fact that customers have to add additional authentication time around 1.5 seconds for fingerprint verification, the security is much improved and guaranteed. Research "Fingershield ATM – ATM Security System using Fingerprint Authentication" [8] used experimental descriptive method. With this method, hopefully ATM Fraud can be minimized so that the customers can feel more secure while using ATM Machines. Based on implementation and test results which had been done before, Fingershield ATM functions run well and some security parameters have passed the test, as well as almost all specifications are met.

In [9], a PIN is generated by the user and this PIN is made available to the ATM system by the means of a Subscriber Identity Module (SIM) in the user's Mobile Phone. This information is communicated to a Global System for Mobile Communications (GSM) module embedded into the ATM's functional framework. This method of security is more stable than the traditional methods presently in use. The method presented is dynamic due to the possibility of changing the User Defined PIN (UDPIN) in each and every transaction. Losing the access card no longer becomes a big problem to the user and the need for immediate deactivation is also eliminated. It can also be enhanced by including other security features without large number of modifications. A simple prototype employing this security function has been implemented and the results are verified. The proposed system has been tested extensively and proves to be a simpler and better security measure.

There is a tremendous increase in the ATM fraud incidents in recent years. Card fraud reports stated that $16.31 billion are the losses from payment card frauds in 2014, and expected to reach $35.54 billion in 2020. There is a real demand to find robust security methods, devices, and technologies to safeguard ATM transactions. Paper [10] proposed two steps model to complete ATM transactions using a closed end-to-end fraud prevention system. By adding a smartphone as an additional layer for ATM transactions and using legitimate user smartphone ID number to robust ATM secure transactions using the available technologies.

III. PROPOSED SYSTEM

Below figure represents the block diagram of the proposed system. Camera is used for authentication of user. We are using vibration sensor and camera of PC/laptop. First, the user will swipe the ATM card. A live image is captured automatically through a webcam installed on the ATM, which is compared with the image stored in the database. If it matches, an OTP will be sent to the corresponding registered mobile number.

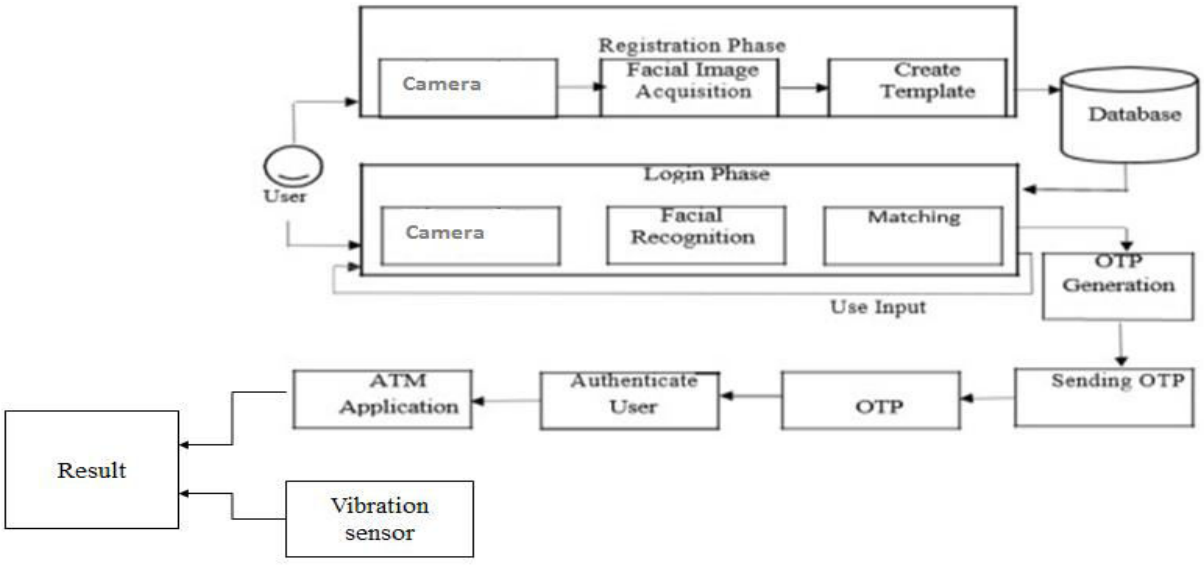


Fig.1. proposed system

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 2, February 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0902013 |

This randomly generated code has to be entered by the user in the textbox. If the user correctly enters the OTP, the transaction can proceed. Therefore, the combination of face recognition algorithm and an OTP drastically reduces the chances of fraud plus frees a user from an extra burden of remembering complex passwords. Vibration sensor is interfaced to laptop via USB to TTL module. Whenever a thief tries to forcefully break into the ATM, vibration sensor sends HIGH signal to system so that system can alert authority about same.

IV. CONCLUSIONS

The appropriation of the ATM as an electronic financial channel has decidedly affected the financial business overall since it is successful and helpful for bank clients. The appearance of ATM misrepresentation has anyway been a danger for some banks everywhere throughout the world and numerous banks currently mean to annihilate extortion expenses to the bank. The proposed framework can give a viable and serviceable arrangement that tends to the necessities of the administrative expert of the banks. The embraced innovation of the proposed framework is likewise less expensive to convey than the face discovery verification method since it uses the parts of the current framework. The model can likewise accommodate high withdrawal points of confinement to provide food for the requests of a money centered client base. When all is said in done, it will emphatically affect the financial business and the general public by lessening the rising dimensions of wrongdoings that are related with ATM exchanges.

.

REFERENCES

[1] James J Mc Andrews, The Evolution of Shared ATM Networks, Business Review, May/ June 1991
[2] Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar, Review Article: Biometric Template Security, Journal on Advances in Signal Processing Volume 2008, Article ID 579416.
[3] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi, Biometric Authentication: A Review, International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.
[4] Abdullah A. Albahdal and Terrance E. Boult, Problems and Promises of Using the Cloud andBiometrics ResearchGate publications, 17th November 2015
[5] Peter Peer and Jernej Bule, Jerneja Zganec Gros and Vitomir Struc., Building Cloud-based Biometric Services, Informatica 37 (2013) 115122 115.
[6] Nischaykumar Hegde Sharath K R, Card less ATM Cash Withdrawal: A simple and Alternate Approach (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1) , 2016, 126128
[7] Madhuri More 1 , Sudarshan Kankal2 , Akshaykumar Kharat3 , Rupali Adhau, Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using Human Fingerprints, International Journal of Advance Engineering and Research Development Volume 5, Issue 05, May -2018, 2348-6406.
[8] Harshad Joshi , Priyanka Keche , Isha Padiya GSM Based Anti-theft Transaction System, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 4, Issue 1, January 2015 Copyright to IJAREEIE 10.15662/ijareeie.2015.0401015 144
[9] Alebiosu M. Iyabode, Yekini N. Nureni, Adebari F. Adebayo, Oloyede A. Olamide, Card-Less Electronic Automated Teller Machine (EATM) With Biometric Authentication, International Journal of Engineering Trends and Technology (IJETT) Volume 30 Number 2 - December 2015
[10] Pranav Gebad1 , Prof. N. A. Dawande International Journal of Advanced Research in Computer and Communication Engineering ISO 3297:2007 Certified Vol. 5, Issue 7, July 2016 ATM Transaction without Debit Card
[11] Nachiket Sainis1 , Reena Saini Biometrics: Cardless Secured Architecture for Authentication in ATM using IRIS Technology International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2015
[12] Neenu Preetam. I, Harsh Gupta Cardless Cash Access Using Biometric ATM Security System, International Journal of Enhanced Research in Science Technology Engineering, Vol. 3 Issue 11, November-2014, Page — 13
[13] Priya Sharma, Pawan Kumar Chaurasia, Proposed Algorithm for Secured Transaction using 3-Tier Architecture, International Journal of Computer Sciences and Engineering Open Access Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693
[14] Priya Tawd, Dr. G. Prasanna Lakshm Enhancing Micro-ATMs and POS Terminals Authentication System Using Advanced Biometric Techniques, IOSR Journal of Computer Engineering (IOSR-JCE) 74 — Page
[15] Ojekudo Nathaniel, Macarthy Osuo-Genseleke, A Comparative Study of PIN Based and Three-factor Based Authentication Technique for Improved ATM Security, International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 05 — May 2018 Page 3749

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details