International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Highly Sensitive PIN Accessibility for ATM using Biometrics And Human Body Communication

Dharani R*, Vaishnavi Sri R#1,Arul Priya M #2, Priya B#3
#Department of Information Technology,
Panimalar Institute of Technology
Chennai, India
*dharani.rit@gmail.com [1]vaishnavisri21@gmail.com
[2]arulpriyam30@gmail.com [3]priyasribhagavan@gmail.com

May 22, 2018

Abstract

Automated Teller Machine Frauds have increased over the decade. It has become difficult for the user to overcome from the ATM PIN attacks. With the evolution of Mobile Technology, Smartphones and Wireless devices can be used for PIN authentication and transmission but they require network connectivity and only an active user can perform successful transactions though they provide security. The proposed model uses biometrics and Human Body Communication to provide security and prevent PIN attacks. The PIN Transmission is performed by a RedTacton based smart security card that replaces the ATM cards and PINs. Thus, the proposed method is secure against all types of PIN attacks such as Card Skimming, Card Cloning and Shoulder-Surfing attacks.

***Key Words*:** RedTacton; Personal identification number; Skimming attack; Pin Authentication; Shoulder-Surfing attack; LCD; ATM; MEMS Sensor

1 INTRODUCTION

PIN Authentication is an important process in any ATM Transaction. A Personal Identification Number (PIN) is a sequence of digits that verifies the identity or authentication of a person when it is successfully provided. PINs are simple , easy to remember and reproduce. From the perspective of security, PIN authentication in ATM is vulnerable to all types of attacks such as brute force or guessing attacks, shoulder surfing, card skimming and card cloning attacks. Security of credit and debit card authentication is at the precedence to protect ourselves from the attackers who are well-versed in various technologies [6]. Researches have analysed various types of debit card frauds [13]. Card-less transactions have become popular, where users can use additional personal devices, such as mobiles phones to perform the financial transactions [4,10]. ATM frauds are increasing day by day. As per RBI, over 25800 banking fraudulent cases were stated in 2017. These Cases involving about Rs 179 crores related to credit/debit cards were noted in 2017. Incidents of about 200 people losing around Rs 10 lakhs to ATM frauds(Card Skimming and Cloning Attack) have occurred within a week.

A. PIN ATTACKS

1) Shoulder-Surfing Attack:In a shoulder-surfing attack (SSA) or Observation Attack, the attacker attempts to observe the 4 digit ATM PIN over the users shoulder, and reproduces it after stealing the Users Card or with the duplicate of the original Card. The attacker may fix a mini camera on the top of ATM terminal or near the Keypad to record all the PIN entries[7,14].

2) Skimming Attack: A Skimmer device is a device that reads and stores magnetic stripe information when a card is swiped. Attackers fix a skimmer device in the ATM Card Slot which collects all the card details. Duplicate card is created and Attacker uses it along with acquired PIN for performing the Bank Transactions [5].

3) Snooping Attack: In this attack, the Attacker or the fraudster covertly watches to another persons conversation regarding ATM pin and tries to withdraw cash.

4) Brute-Force Attack: In this attack, the attacker guesses a users PIN by trying some possibilities of the four digit. This attack is called Password Guessing or Brute-Force Attack.

5) Card-Cloning Attack: Cards contain magnetic strips and that are duplicated with card cloning devices [5].

Researchers have analyzed the ways, the users card information are exposed to attackers [13]. Multiple researches have also been conducted to detect fraudulent card transactions [8,11]. Research on shoulder-surfing resistant PIN entry has been continuing from the past [7]. Wearable devices and mobile phones have been employed in emerging PIN authentication technologies [12]. However, such devices are also considered as an opportunity for more complex attacks by malicious users. With the evolution of Mobile Technology, Smartphones and Wireless Devices can be used for PIN authentication and transmission but they require network connectivity and only an active user can perform successful transactions though they provide security [9,10].

In this paper , we propose a Highly Sensitive PIN Accessibility for ATM using Biometrics and Body-Based

Networking to avoid the PIN attacks and Card Cloning. Biometrics is added to ensure User Authentication at the ATM. ATM Pin is transmitted through human body and RedTacton. Human Body Communication is performed using the RedTacton Technology. RED-meaning Warmth and TACTON-meaning action caused by touching. RedTacton is a HAN(Human Area Networking) Technology. Human body produces small electric charges all the time. Red Tacton uses weak electric field over human body surface to transmit and receive the signals at very high speed of 10Mbps[half dupex communication]. RedTacton has more benefits than Wifi, Infrared, Wired Transmission. Wifi has less security and can be easily hacked. So, RedTacton can provide maximum security as well as data transfer without any physical connections. As soon as the human body comes in contact with the RedTacton , the signals start to travel. When the contact is taken off, the transmission stops. RedTacton is made up of electric field sensor working with a

electro-optic and laser light. Electro-optic sensor is present in the RedTacton which allows the signal to pass through any two parts of the body. Communication can occur through any body surfaces such as hands, arms,feet,face and legs. During communication, displacement current is produced by the electrons in the body because the body is subjected to minute electrical fields. Since RedTacton is wrapped with insulating film, so it does not affect the body of the person. So, Human Body can used as an effective transmission medium for PIN transfer to prevent all the PIN attacks.

2 WORKING PRINCIPLE

The RedTacton transmitter prompts a weak electric field on the surface of the body. The RedTacton receiver intellects changes in the weak electric field on the body caused by the transmitter. RedTacton emphasis upon the fact that the optical properties of an electro-optic crystal varies in propotional to the changes in weak electric field. The electric field stimulated toward the body by the RedTacton transmitter's signal electrode is represented by Ea. Electric field Eb induced from the body can follow a return path to the transmitter. Since the user stands on ground, electric field Ec escapes from the body to ground, from the feet. The electric field Es that reaches the receiver is denoted as Es = Ea - (Eb + Ec). The received electric field combines with the electro-optic crystal and modifies the crystal's optical properties. This change is identified by laser light and is altered into digital data by a detector circuit.

The principle used in RedTacton is Electro-optic effect and Amperes circuital law. The Amperes circuital law states that when there is a change in the electric field made by the transmitter then flow of electrons occur in body. In Electro-optic effect, laser is passed through an electro-optic crystal, which bends light in propotional to the strength of the field across it. The extent to which the optical properties of an electro-optic crystal are transformed is noticed by laser light because laser light deflects acccording to the strength of the field across it and the deflections are measured.

The result obtained is converted to an electrical signal in a optical receiver circuit.The transmitted data can be retrieved by the photonic electric field sensor.This technique called as electric field photonics is used in the RedTacton.

A. Features of RedTacton

1) Communication by touch: Actions like touching,stepping etc are used for operations like START and STOP of the equipment, locking and unlocking etc.

2) Any Media: Other than the human body, conductors or dielectrics or both in combinations can be used as transmission media. For eg water and other liquids, various metals, certain plastics, glass, etc.

3) Broadband Feature: Bandwidth does not degrade even with duplex operations.

4) Transmission Speed: Increase in the number of users does not affect the transmission speed [17].

B. Applications of RedTacton

Moving the pictures stored in camera to laptop by estabilishing a contact between the laptop and camera, exchange business cards just by a hand shake, exchange telephone numbers etc [18].

C. Advantages of RedTacton

High Speed Communication is possible between any two points of the body. Body-based networking is more secure

than other broadcast systems, such as Bluetooth which have high range of about 10m. When compared to other technologies, Network congestion due to fall in transmission speed in multiuser environments does not occur. So it is superior than Infrared technology Wi-Fi. Transfer of data is fast, feasible and more importantly reliable.

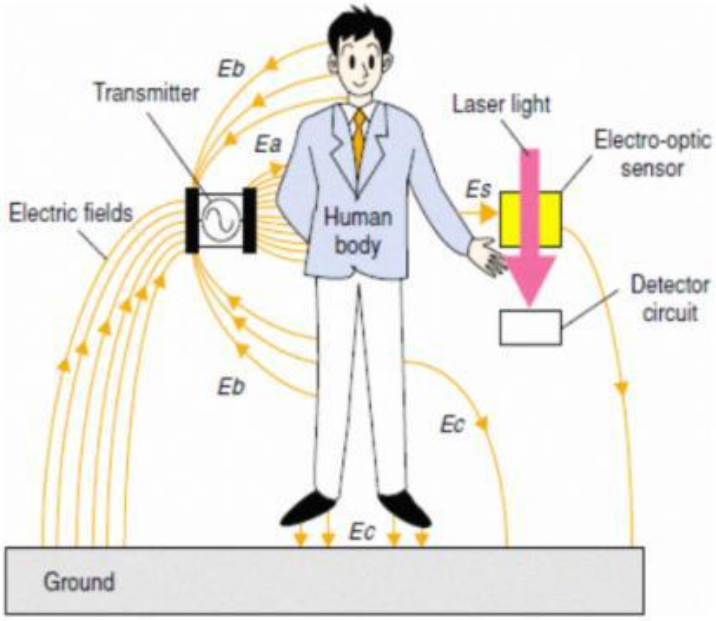

Fig.1. . Working of RedTacton

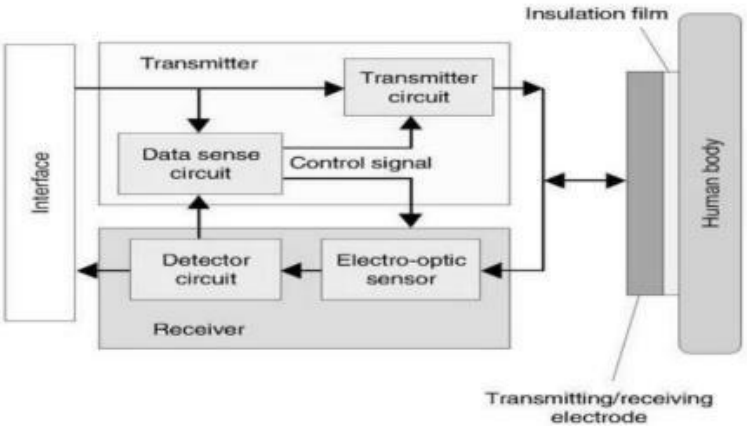

Fig.2. Block Diagram of RedTacton

3 PROPOSED SYSTEM

The main objective of the proposed system is to avoid PIN attacks and Card Cloning and to provide better Security in ATM Sector. The proposed model uses biometrics and Body-Based Networking to provide security. Biometrics is added to verify whether the user is authenticated or not. ATM PIN is transmitted through RedTacton and human body to the ATM Machine. Human Body Communication is performed using the RedTacton Technology. The Fingerprint Biometric and PIN Transmission to the ATM is done to achieve high level of security and protection. The proposed method is secure against all types of PIN attacks such as Card Skimming, Card Cloning and Shoulder-Surfing attacks. The PIN Transmission is done by a RedTacton based smart security card that replaces the ATM cards and PINs. If the correct PIN is transmitted to the ATM Machine then Password Correct is displayed in ATM or LCD display. The MEMS sensor is used inside the ATM Machine to monitor the ATM movements in case of any ATM theft. When vibrations exceed the threshold level in MEMS Sensor, shutter will be automatically closed and alarm will be generated via a buzzer. MEMS Sensor Value would be updated in the Server with the Bank location so that immediate action can be taken to avoid the theft .

4 DESIGN ANALYSIS

This section presents the security and architectural design analysis for the proposed SEPIA architecture with respect to the attacks. The proposed model uses biometrics and Body-Based Networking to provide security. ATM PIN is transmitted through RedTacton and human body to the ATM Machine. The Fingerprint Biometric and PIN Transmission to the ATM is done to achieve high level of security and protection. The proposed method is secure against all types of PIN attacks(Card Skimming, Card Cloning and Shoulder-Surfing attacks). The proposed system prevents Shoulder Surfing attacks as the ATM PIN is transmitted through human body so it is not exposed to the outside environment. RedTacton Security Card cannot be skimmed and cloned.

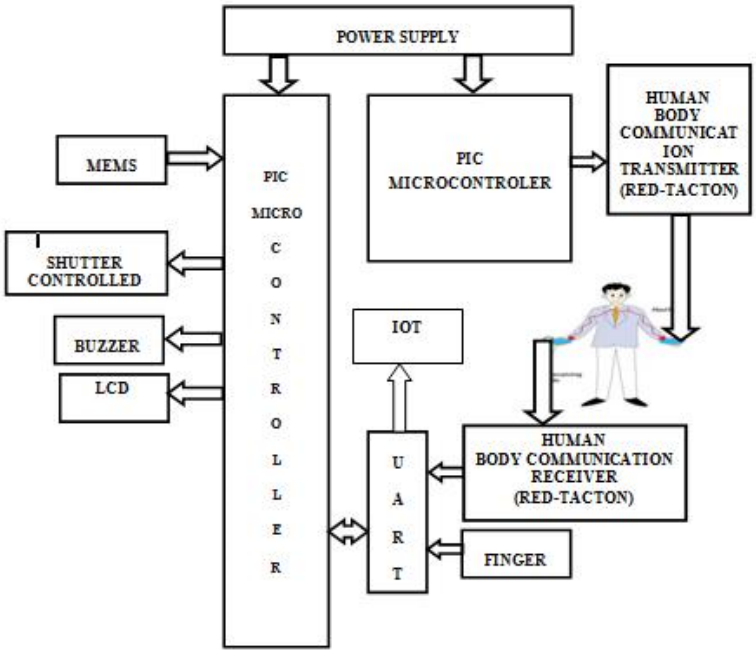

Fig.3. Architectural Diagram

Let us assume that a non authorized user steals the RedTacton from the authorized user. When the non-authorized user places the fingerprint for performing the user authentication, fingerprint matching is performed and the ATM will display unauthorized. So, the user cannot login to the system. If suppose the user cannot perform ATM Transaction in unexpected situations then a nominees fingerprint can also be included. If a user has lost the RedTacton Security Card then, the user has to go to the respective Bank that holds the users account to block the account as in case of Debit Card loss or theft.

5 IMPLEMENTATION

We have implemented a prototype for the proposed ATM system. The prototype consists of three modules: Fingerprint Recognition, Data Transfer using Human Body and RedTacton ,ATM Movement Detection.

A. Fingerprint Recognition

The use of fingerprint recognition is to verify whether the user is authenticated or not. It includes enrollment,identification and verification. Initially user places the finger print to the ATM. The fingerprint biometric system converts the fingerprint into a packet of data or sequence of characters. This packet of data is checked for verification each time the user places the fingerprint.Thus, fingerprint matching is performed by comparing the packet of data with all the data stored in the microcontroller. If there is a match, Fingerprint Matched is dispayed in ATM Machine or LCD display.

B. Data Transfer using Human Body and RedTacton

The use of this module is to transmit ATM PIN using human body and Red Tacton.After fingerprint verification, the user holds the RedTacton Transmitter and touches the RedTacton Reciever present in the ATM Machine. The RedTacton is connected with the microcontroller that stores the 4 digit ATM PIN. RedTacton continuously receives the signal from the microcontroller. If the correct PIN is transmitted to the ATM Machine then Password Correct is displayed in ATM or LCD display.

C. ATM Movement Detection

The use of this module is to detect movement in ATM and update value in server.The MEMS sensor used here is to monitor the ATM movements. When vibrations exceed the threshold level in MEMS Sensor, ADC receives the analog signals from MEMS Sensor and converts it to digital data. Usig lcd command the digital data is converted into integer value to display the MEMS Sensor Value in lcd. The ouput pins are connected to buzzer and shutter so that shutter will be automatically closed and alarm will be generated via a buzzer Alert. MEMS Sensor Value would be updated in the Server.

6 RELATED WORK

Mr. S.Kumaresan , Mr. G.Dinesh Kumar, Mrs. S.Radhika have presented an analysis of PIN authentication frauds and loopholes exploited by attackers. They proposed a shuffled Automated Teller Machine keypad which displays the shuffled numbers in the Liquid Crystal Display keypad which confuses person who is standing near you to guess the password [3].

Sweta Singh , Akhilesh Singh , Rakesh Kumar have provided mechanism adding a limit on amount of cash and number of transactions such that if one need to withdraw a big amount OR attempts for multiple transactions , then it is necessary to present biometric [1]. Modern solutions for secure financial transactions involve card-less interactions, where users generally rely on a cloud based Bank Server-API over HTTPS to communicate with the User application ,ATM Terminal takes the loc_Id,Req_Id,Trans_Id to generate the QR Code [16].However, such solutions have also triggered an increase in Processing time for the transaction. Unfortunately, these QR Code designs for security will always have limited usability for general users, not suitable for people with less knowledge in smart phones and also Requires Network Connectivity [9]. There are numerous biometric-based authentication techniques, such as the fingerprint and face recognition based authentication, used to secure PIN entry and authentication for ATMs. Athanasios Papadopoulos,Toan Nguyen, Emre Durmus,Nasir Memon presented IllusionPIN (IPIN),a shoulder-surfing resistant PIN authentication by the technique of hybrid images to blend two keypads with different digit orderings in such a way, that the user who is close to the device is seeing one keypad to enter her PIN, while the attacker who is looking at the device from a bigger distance is seeing only the other keypad [2]. V. Varalakshmi, Mrs.P.Kanimozhi presented WPAM, which uses the WIFI Technology and wireless devices(Laptop,Smartphone,Tablet) in which User logins to Application, unique PIN is sent to mail id by which it resists all Keypad based attacks such as shoulder surfing and skimming device

attacks.These solutions rely on network connectivity and wireless device requirements at the ATM terminals and may not be a ready-to-deploy solution for secure PIN authentication [15].

Highly Sensitive -Pin-Accessibility for atm using human body communication can work with currently supported hardware on ATM and fingerprint based User Authentication. With the introduction of face recognition devices as the Google face recognition, usability of such secure systems can be leveraged greatly. However, Highly Sensitive -Pin-Accessibility for atm using human body communication does not rely on stored client certificates, and can be considered resistant to attacks even if the user loses the personal device. Moreover, the RedTacton service allows less processing Time because it uses human body to transmit and receive signals at very high speed(max of 10Mbps) and is secure against all types of PIN attacks and highly scalable without imposing any resource-hungry operations on the personal mobile or wearable devices.Thus it is suitable for all people.

7 CONCLUSION

There has been techniques used to provide security in the ATM Sector but security could not be achieved to a greater limit. When we compare RedTacton with other technologies, it can give a better security since there is no problem of attackers as our body itself acts as a safe and an effective transmission medium and therefore the ATM PIN is not exposed to the outside environment. So, Biometrics and Body-Based Networking can achieve a high level of security and protection against increasing ATM fraud rates. Thus, the most efficient way of preventing the PIN attacks and Credit Card Cloning is by the means of Human Body Communication. Credit Card Frauds can be minimized to a greater extent by using Red Tacton Technology.

ACKNOWLEDGMENT

We would like to thank our Head Of Department Dr. A. Joshi for encouraging us and sharing her pearls of wisdom with us. We thank Mrs. R. Dharani Asst. prof for her assistance and for the comments that greatly improved the manuscript. We thank each

and everyone who helped us.

References

[1] Akhilesh Singh,Sweta Singh,Rakesh Kumar , A Constraint-based Biometric Scheme on ATM and Swiping Machine 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)

[2] Athanasios Papadopoulos,Toan Nguyen,Emre Durmus,Nasir Memon,

IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images, IEEE Transactions on Information Forensics and

Security,2017

[3] G.Dinesh Kumar ,S.Kumaresan , S.Radhika , Design of Secured ATM by Wireless Password Transfer and Shuffling Keypad , International Conference on Innovations in Information Embedded and Communication Systems ICIIECS15 ,2015.

[4] G. Stanley, Card-less financial transaction, Apr. 21

2014, US Patent App. 14/257,588.

[5] Hong Guo, Bo Jin, Forensic Analysis of SkimmingDevices for Credit Fraud Detection, IEEE International Conference on Information and

Financial Engineering (ICIFE), pp.542 546, Jan. 2010.

[6] M. Dlamini, J. H. Eloff, and M. M. Eloff, Information security: The moving target, Elsevier Computers & Security, vol. 28, no. 3, pp. 189 198, May 2009.

[7] M.-K. Lee, Security notions and advanced method for human shoulder-surfing resistant pin-entry, IEEE Transactions on Information Forensics and Security, vol. 9, no. 4, pp. 695708, April 2014.

[8] N. Sethi and A. Gera, A revived survey of various credit card fraud detection techniques, International Journal of Computer Science and Mobile Computing, vol. 3, no. 4, pp. 780 791, April 2014.

[9] Rasib Khan, Ragib Hasan, Jinfang Xu, SEPIA(SEcure-PIn-Authentication-as-a-service), a secure PIN for ATM using wearable devices and mobile 2017 IEEE Transactions on Communication and Signal Processsing(ICCSP).

[10] S. N. White, Secure mobile-based financial transactions, Feb 2013, US Patent 8,374,916.

[11] S. Raj and A. Portia, Analysis on credit card fraud detection methods, in Computer, Communication and Electrical Technology (ICCCET), 2011 International Conference on, March 2011, pp. 152156.

[12] S. Safavi and Z. Shukur, Improving google glass security and privacy by changing the physical and software structure, Life Science Journal, vol. 11, no. 5, pp. 109117, 2014.

[13] T. P. Bhatla, V. Prabhu, and A. Dua, Understanding credit card frauds, Cards business review, vol. 1, no. 6, 2003.

[14] V. Roth, K. Richter, and R. Freidinger,A pin-entry method resilient against shoulder surfing, in Proceedings of the 11th ACM Conference on Computer and Communications Security. New York: ACM, 2004, pp. 236245.

[15] V.Varalakshmi, Mrs.P.Kanimozhi, Secure PIN Authentication for ATM Transactions using Wireless Devices ,in International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), April 2016.

[16] Y. Liu, J. Yang, and M. Liu, Recognition of qr code with mobilephones, in Control and Decision Conference, 2008. CCDC 2008.Chinese, July 2008, pp. 203206.

[17] https://en.wikipedia.org/wiki/RedTacton

[18] http://www.circuitstoday.com/redtacton-technology