Secure PIN Authentication for ATM Transactions using Wireless Devices

[1]V.Varalakshmi, [2]Mrs.P.Kanimozhi
[1]PG Scholar, Department of Computer Science and Engineering,
[2]Associate Professor, Department of Computer Science and Engineering,
IFET College of Engineering, Villupuram.

Abstract - **Now-a-days many unauthorized access and theft takes place in ATM machines. In general, all the keypad based authentication system has several possibilities of password guessing by means of shoulder movements and skimming device attacks. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. At the same time the growth of mobile technology, with regard to availability of services and devices like Smartphone's has created new phenomenon for communication and data processing ability to do Daily Works. One such phenomenon that has emerged in the Social work Environment is BYOD (Bring Your Own Device), which means that users can use their personal device to access company resources for work, inside or outside organizational environment. This paper proposes a Wireless Pin Authentication Method (WPAM) for secure transactions using BYOD trend. In addition to that Kerberos authentication protocol is used for user's authentication. Hence, considered as a reasonable tradeoff between security, usability and cost. So, this paper mainly concentrates on providing efficient security to ATM against theft.**

Keywords - **Personal identification number, Skimming Attack, Pin Authentication, Shoulder surfing attack**

I. INTRODUCTION

Nowadays many unauthorized access, threats and theft takes place in ATM machines. Currently PIN numbers are used for security in ATMs. The crime rates are also increased with fleeting time and will never fall as attackers are efficient enough with all detailed criminal knowledge collected with them. The service provider must promote a stable security of user data for customer satisfaction. The goal is to protect ATM from theft using counter measures for security. As the ATM related security are public and published in newspaper and internet. So the security measures applied are known to both the regulator and attacker. Nowadays we use 4-Digit PIN code for safety and security for money deposition and transaction. But in real the PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or device attackers. The attackers now are technically knowledgeable they have every idea about the usage of the user. At first, the attacker will try hacking the 4-PIN code using finger prints plated in the number box. Then the hacker tries hacking the bar code of the card using the detector and a duplicate card of the user is framed for theft. Through this method the thief can withdraw our money without the regulators knowledge and initiate theft without any doubt.

Currently Personal Identification Number (PIN) is used for security in ATMs and authentication is provided by the Users entering (PIN). This PIN numbers can be hacked easily through specific fraudulent activities and it can be observed by human or skimming device attackers. So, this paper proposes a Wireless Pin Authentication Method (WPAM) for secure ATM transaction using Wi-Fi technology. In this method, customers use their own wireless devices (Laptop, Smartphone and Tablet) for ATM Transactions.

In general, all the keypad based authentication system has several possibilities of password guessing by means of shoulder movements and skimming device attacks. The main objective of this paper is to develop a secure ATM Transaction for users using their own wireless devices (Laptop, Smartphone and Tab).

II. RELATED WORKS

Several Pin Authentication Methods are discussed as follows,

Black and White (BW) Method [1]: where the regular numeric keypad is colored at random, half of the keys in black and the other half in white, which is called as BW technique. A user who knows the correct PIN digit can answer its color by pressing the separate color key. The basic BW method is expected to resist a human shoulder surfing attack. But if the selected halves were memorized or written on a paper for m consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could recognize a single digit of the PIN.

Fake Cursors Method [2]: To hide password entry on on-screen keyboards. The objective of the fake cursor is, adding overhead to the input to make it hard to monitor. The authors suggest several concurrent cursors that move in the exact same way to quickly reach objects on big screen spaces. In this system, only one cursor performs the actual input while the other cursors act as distraction for an attacker. That is, they do not move in line with the genuine cursor. Since the fake cursors move differently from the active cursor, users can identify it while attackers have Problems.

Biometric Voice Based Access Control Method [3, 9, 10]: A conceptual framework for use of intelligent voice-based access control in ATMs which is biometric approach. Research has shown that ATM user have encountered several problems in the past which include; chip distortion, card misplacement. Card fraud, etc. these entire problems are associated with using smartcard access control in ATM. To overcome these problems it is advisable that government should partner with banking sector to implement the use of biometric technique "intelligent voice-based access control" in ATMs, as this will eliminate completely the problems associated with smartcard access control

Attacks on Pin Entry [1]:

a. Shoulder Surfing Attack

In a shoulder-surfing attack (SSA), the attacker detects the logon procedure by looking over the user’s shoulder, and tries to recover that user’s PIN. The SSA may be done directly through the human eyes or by using any electronic devices such as fixing a skimmer device or mini cameras at ATMs.

b. Skimming Attack

A device that reads and stores magnetic stripe information when a card is swiped. Attackers can fixing a skimmer over the card slot of an ATM and store customers’ credit information without their knowledge. Later, this information can be retrieved and used to make duplicates of the original cards

c. Eavesdropping Attack

In Eavesdropping attack, the Eavesdropper secretly listening to another person’s conversation. In this attack the Eavesdropper secretly observing the users pin entry.

d. Guessing Attack

In a guessing attack, the attacker guesses a user’s PIN and inputs it to pass the test. The most common type of attack is password guessing. Attackers can guess passwords locally or remotely using either a manual or robotic approach. For example, a typical ATM permits three trials.

III. PROPOSED SYSTEM

The main objective of this system is to develop a secure ATM. In general, all the keypad based authentication system having several possibilities of password guessing by means of shoulder movements. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. Automated Teller Machines (ATMs) security is the field of study that aims at solutions that provide multiple points of protection against physical and electronic theft from ATMs.

Authentication of users at automatic teller machines (ATMs) is mostly dependent on PIN-based verification. This paper proposes a Wireless Pin Authentication Method (WPAM) for secure ATM transaction using Wi-Fi technology. In this method, customers use their own wireless devices (Laptop, Smartphone and Tablet) for ATM Transactions[13].

Wi-Fi is commonly called as wireless LAN, it is one of those networks in which high frequency radio waves are required for transmission of data from one place to another. Wi-Fi operates on several hundred feet between two places of data transmission. This technology only works on high frequency radio signals. Otherwise, it will not work properly. Nowadays this technology is used as office or home network and in many electronic devices.

Wireless LAN or Wi-Fi is divided into three main parts on which its whole working depends and all of its applications also depend on these parts i.e. infrastructure mode, ad hoc network and mixed network. Kerberos authentication protocol is used for user’s authentication. It works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos protocol messages are protected against eavesdropping and Replay Attacks.

In the proposed model, the personal device performs the following functions:

- The personal device authenticates the user to the service outlet.
- As an added security user may need to authenticate himself to the personal device, so that a misplaced device is unusable by a fraudulent. The personal device acts as an interface for the user to access the services.
- The personal device provides information (signed by the service provider) about the user so as to obviate the need of the service outlet to communicate with the server.

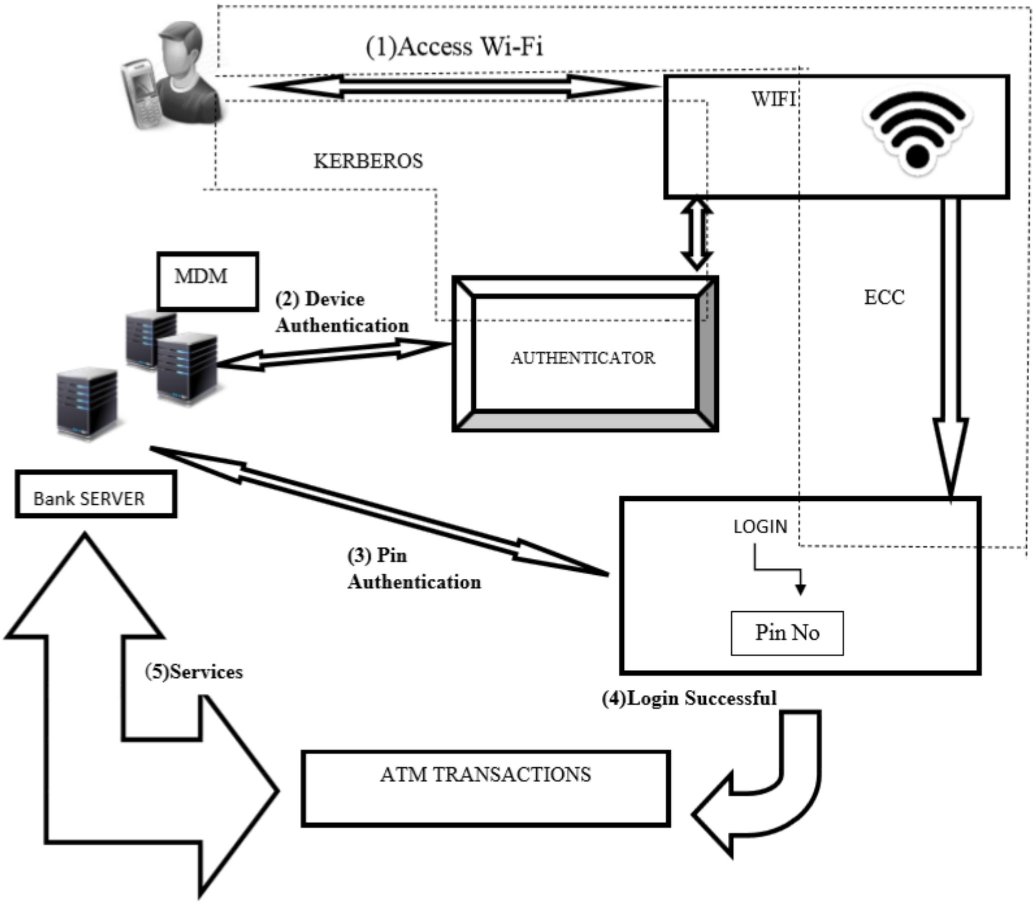

Figure. 1 Proposed system

Steps in the proposed model:

- Registration of the user with the bank: After the registration, the wireless devices carries the public key of the user which has been signed by the bank as well as the public key of the bank. Optionally, the wireless device also carries an application which enables it to communicate with the ATM.
- Once that form is submitted, a unique PIN is send to the respective mail id of the user.
- Users connect the Wi-Fi enabled LAN in their Wireless Devices using the Pass code. So, Wi-Fi act as interface between wireless devices and ATM
- User authenticates himself to the wireless devices using his pin
- A wireless device authenticates itself to ATM by presenting the user's 'tickets' and responding on ATM's challenge. Kerberos authentication protocol is used for user's authentication. It works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.
- ATM authenticates itself to the Wireless devices by presenting its own 'tickets'.
- User now access the service of the ATM using the signed application

The proposed system includes the following modules:

A. Pin Authentication

The Wireless Device is authorized by authenticator and then Device gets connected to the ATM console. The users open the webpage and login their account using Pin no. Like usual ATM work stream, here PIN along with Account no is authenticated by Bank servers. Kerberos authentication protocol is used for user's authentication. It is secure and it implements mutual authentication, where a client verifies its identity to a server and a server verifies its identity to the client.

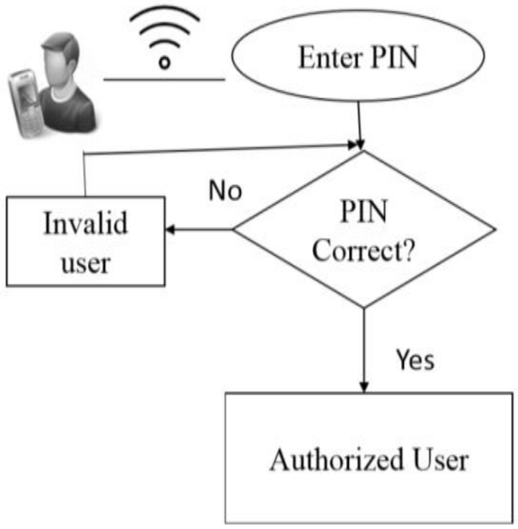

Figure. 2 Pin Authentication

B. Interaction Design

Interaction design (IxD) focuses on creating engaging interfaces with well thought out behaviors. Here, users are interacting with wireless devices and these devices interact with ATM Machine. This interaction is also called as Machine to Machine or Device to Device communication. It defines the structure and behavior of interactive systems. Interaction designers strive to create meaningful relationships between people and the products and services that they use, from computers to mobile devices to appliances and beyond. Elliptic curve cryptography (ECC) is used to provide a security for wireless devices communication.

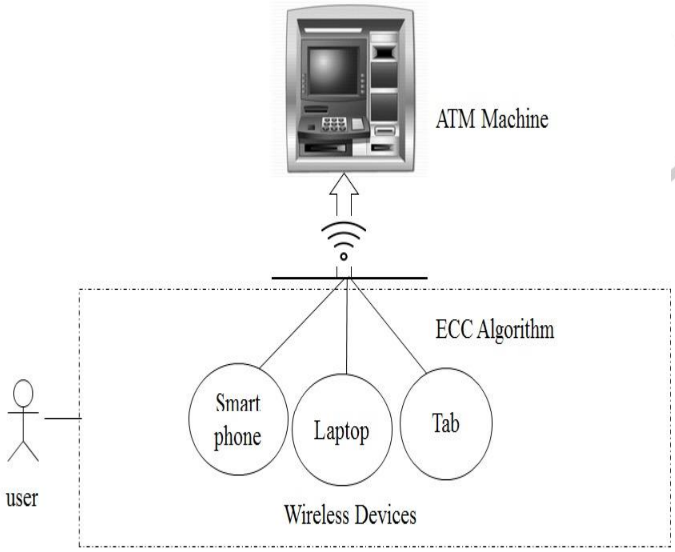

Figure. 3 Interaction design

C. ATM Transactions

ATM Transactions are performed after the User Authentication. Using the Wi-Fi Modem Interface these transaction logs can be updated periodically to the bank database server by the ATM. Following, ATM Transactions are performed: Withdrawal, Balance Inquiry, Transfer Funds and Deposit.

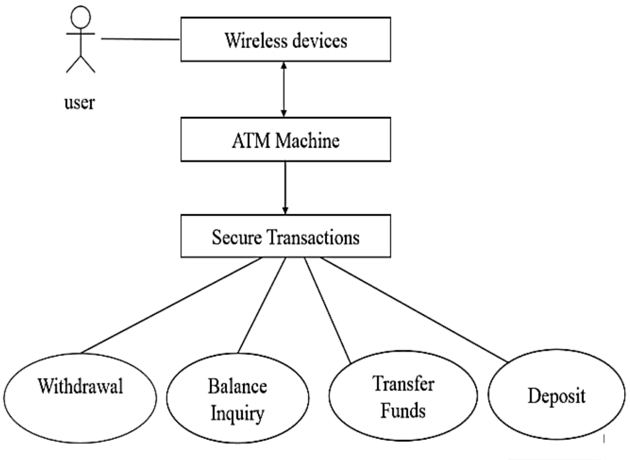

Figure. 4 ATM Transactions

IV. SYSTEM IMPLEMENTATION

Secure ATM Transactions will be implemented by J2EE software is the enterprise edition of Java and Oracle 12c (Server Edition). Oracle Database 12*c* presents a new multitenant design that makes it easy to combine many databases quickly and manage them as a cloud service. Then, the Wi-Fi IEEE 802.11 standard is used for wireless devices communication. This technology was designed to provide wireless connectivity to devices that require a quick installation, such as portable computers PDAs or generally mobile devices inside a WLAN network. The projected work describes about the wireless PIN authentication method (WPAM) using Wi-Fi technology. By this technology, users using their own wireless devices (Laptop, Smartphone and Tab) for secure ATM Transactions. So, this method provides a security to the PIN entry process from shoulder-surfing and Skimming attacks.

V. CONCLUSIONS

In general, all the keypad based authentication system has several possibilities of password guessing by means of shoulder movements and skimming device attacks. Shoulder-surfing is an attack on password authentication that has traditionally been hard to defeat. At the Same time the growth of mobile technology, with regard to availability of services and devices like Smartphone's has created new phenomenon for communication and data processing ability to do Daily Works. One such phenomenon that has emerged in the Social work Environment is BYOD (Bring Your Own Device), which means that users can use their personal device to access company resources for work. This project proposes a Wireless Pin Authentication Method (WPAM) for secure transactions using BYOD trend. In addition to that Kerberos authentication protocol is used for user's authentication.

REFERENCES

[1] Taekyoung Kwon, Jin Hong, "Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 2, Feb. 2015.

[2] Luca, E. von Zezschwitz, L. Pichler, and H. Hussmann, "Using fake cursors to secure on-screen password entry", In Proc. CHI, pp. 2399–2402, 2013.

[3] Oyeyinka.l.K, Akinwole.A.K," Automate d Biometric Voice-Based Access Control in Automatic Teller Machine (ATM)", International Journal of Advanced Computer Science and applications, VoI.3, No.6, 2012.

[4] Mun-Kyu Lee, "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PINEntry", In IEEE Transactions On Information Forensics And Security, VOL. 9, NO. 4, pp. 1556-6013, Apr. 2014.

[5] Hong Guo, Bo Jin, "Forensic Analysis of Skimming Devices for Credit Fraud Detection", IEEE International Conference on Information and Financial Engineering (ICIFE), pp.542 – 546, Jan. 2010.

[6] V. Roth, K. Richter, and R. Freidinger, "A Pin-Entry Method Resilient Against Shoulder Surfing", In Proc. Acm Conf. Comput. Commun Security, pp. 236– 245, Feb. 2004.

[7] AbdulrahmanAlhothaily, ArwaAlrawais, Xiuzhen Cheng, RongfangBie, "A novel verification method for payment card systems", In Springer-Verlag London, Volume 19, Issue 7, pp. 1145-1156, Oct. 2015.

[8] K. Jain, A. Ross, S.Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. On Circuits and Systems for Video Technology, Vol. 14, No. 1, pp 4-19, Jan. 2004.

[9] Vivek, K.Singh, Tripathi S.P, Agarwal "Formal Verification of Finger Print ATM Transaction through Real Time Constraint Notation (RTCN)", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. I May 2011.

[10] Sharma, Vijay Singh Rathore,"Role of Biometric Technology over Advanced Security and Protection in Auto Teller Machine Transaction", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 - 8958, Volume-I, Issue-6, Aug. 2012

[11] Zaid Imran and Rafay Nizami, "Advance Secure Login" International Journal of Scientific and Research Publications, Vol. 1, Issue 1, SSN 2250-3153, Dec. 2011.

[12] S.Sakurai, M. Yoshida, T.Munaka, "Improvements and Evaluation of Authentication Method for Mobile Phones ", Computer security symposium , pp.625-630, Oct, 2004.

[13] Prashant Kumar Gajar, Arnab Ghosh, Shashikant Rai, "Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies", Journal of Global Research in Computer Science, Volume 4, No. 4, April 2013