AN ANDROID APPLICATION FOR ATM WITH A SECURED PIN-ENTRY METHODS

KAVITHA V, Dr.G.UMARANI SRIKANTH M.E, Ph.D

M.E. Computer Science and Engineering, Department of PG studies,
S.A. Engineering College, Chennai-600077
Professor & Head of the department, Department of PG studies,
S.A. Engineering College, Chennai-600077
kavitha2326@gmail.comgmurani@yahoo.in

ABSTRACT

One of the most commonly occurringproblems in the recent years are the ATM (Automatic teller machine) frauds. People lose their money due to lack of awareness. The major reason for such kind of actions is the attacks made on the 4-digit pin (Personal Identification Number)which is being used as a password for authentication in ATM.The attacks such as shoulder surfing and recording attacksare becoming more common in ATM. The PIN number is not given proper security to overcome such attacks.The proposed method uses the pin entry methods which are resistant to such attacks.The pin entry methods that used in the proposed system are black white method, improved black white method and session key method. The main aim of the proposed system is to create an android application which performs the ATM transactions that can be installed in a smart phone. The concept of virtual money is also used. The hash function is used to send the PIN securely through the public channels.

Key words: personal identification number; improved black white (BW) method; virtual money; hash function; shoulder surfing attack, Android application.

1. INTRODUCTION

An automated teller machine which is shortly termed as ATM is a well known and a commonly used concept in the recent years. As the usage of such things increases the disadvantages also increases. Some of the disadvantages are the increased attackers and the hacking technologies. The attackers had grown to a high number and new methods for hacking are also introduced.

To avoid the ATM frauds, awareness must be created among the people who use ATM. Every user who holds an ATM card will be given a password. This password is known as the personal identification number which is shortly termed as PIN. It is a 4-digit numeric password used for authentication in ATM.

The main aim of the hackers is the account number and the PIN. This information is gathered during the transaction process carried out by the user in the ATM. But, the user is not aware of such things. The shoulder surfing attack and the recording attack are commonly taking place in ATM. To avoid such hackers, the new pin entry methods are introduced in the proposed system.

The main goal is to create an android application which may perform the ATM transactions. This application can be installed in the smart phones containing the android operating system. This application must contain all the options which are available in an ATM. The virtual money concept is used in this application. This concept gives the money in the format of tokens or images. These tokens and images have the same value as the money.

When the virtual money concept is implemented and the android ATM application is installed in smart phones, every user can register and create the own new login and make the transaction from anywhere securely and safely.

2. ATTACKS ON PIN ENTRY

Some of the related attacks that may be performed on a 4-digit PIN number, which is commonly used as a security password in the ATMs are listed and explained below.

2.1 Guessing Attack(GA)

In a *guessing attack* (GA), the attacker guesses a user's PIN and inputs it to pass the test. A smart attacker might use the fact of non-uniform password or PIN distribution. The account of the user should also be considered, which may be allowed to fail several times until s/he inputs the correct PIN. For example, a typical ATM permits maximum of three trials. Therefore, the following definition for the security of a PIN-entry method is said to be against a guessing attack.

2.2 Shoulder Surfing Attack(SSA)

In a *shoulder-surfing attack* (SSA), the attacker observes the logon procedure by looking over the shoulder of the user, and tries to retrieve the PIN of the user. This SSA is most familiar in many of the common places. One best example is shoulder surfing attack during PIN entry at ATMs. This attack may be done directly through the human eyes or by using any electronic devices such as fixing a skimmer device or miniature cameras at ATMs.

2.3 Human shoulder surfingattack(HSSA)

The HSSA is also one of the types of the shoulder surfing attack,which is performed without any recording device or an electronic device is commonly known as a *human shoulder-surfing attack* (HSSA).This attack is mainly performed by a human by looking over the shoulder of another person to know his logon procedures and PIN. The HSSA is mainly performed by looking at the PIN during the entry process and trying to recollect it later. Now a day, the human hackers had become more powerful to retrieve the PIN that was shoulder surfed.

2.4 Recording Attack(RA)

The *recording attack* (RA) is a type of SSA where the human adversaries use a skimming device or miniature cameras to record the session and hack the PIN or any data of the user. Small cameras are fixed by the human adversaries to record the particular session such as PIN entry session, and then collect the data needed by playing the videos even from any place. These types of attacks are of great concern at ATM.

3. DEVICES FOR ATTACKING ATM PIN

The attackers use many small devices which are attached to the ATM by the hackers to scan and store the user's card information. Some of the devices used by the hackers to attack the ATM PIN of the user are given below.

3.1 Skimming devices

The skimming devices are the small devices mostly used during the ATM card skimming. Card skimming is the process in which the illegal copy of the information from the magnetic strip of the user's ATM. The main information stored in the magnetic strip of the ATM card is the user name and the account number. These skimming devices are thin strip like device which scans the ATM card when inserted by the user and stores the information within it.

3.2 Pinhole Cameras

The hacker must know both the card information and the secret 4- digit numeric PIN of that particular card. The pin capturing is the method in which the hackers use various small devices to capture the PIN or the small camera may be attached to the machine which records the PIN- entry board while the user types the PIN for transaction. It is a process in which the camera or any imaging devices are attached to ATM to fraudulently capture the PIN numbers. Once captured, the electronic data is put on to the fraudulent card and the captured PIN is used to withdraw the money from accounts.

4. THE EXISTING SYSTEM

The existing system of the secure PIN entry methods have also concentrated on the shoulder surfing attacks. The list of existing methods says how important it is to provide security to the PIN entry system. The main aim of these methods was to provide the total security to the PIN entry. But, the existing methods did not provide the intimate security. Some of those methods are discussed below.

4.1 Delayed Oracle Choices(DOC)

If the oracle responds slowly then the partitions are exposed longer to the observer. When the exposure is longer, it is easier for the observer to manually record a partition. In the delayed oracle choices approach, n rounds are displayed consecutively with a predetermined exposure period of 0:5 seconds. The display is cleared subsequently and only then do the left and right input buttons appear. Using these buttons, the oracle must consecutively input the colouring that his PIN digit had in these n rounds. The oracle has only a limited period of time to determine the colour of the current PIN digit in each round, and the colour sequence must be memorized. This procedure is repeated until all PIN digits are entered.

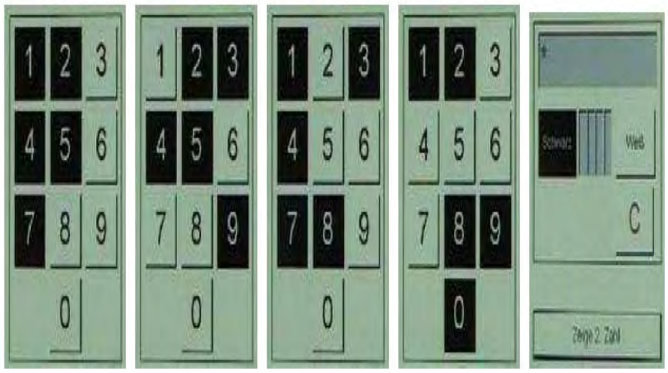

Figure 2: The above sequence illustrates the DOC. Appears subsequent to the display of the four patterns. The oracle must enter the sequence of colours of the correct PIN digit**.**

4.2 The basic BW method

The basic BW method partitions a set of ten digits into two randomly selected halves, of which one is selected according to the user's key entry in each and every round. If the selected halves were written on a paper for m,consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could identify a single digit of the PIN.

The grouping pattern is a method of dividing the set of digits 0-9 into two halves, one half with black color keys and other with white color keys. The user is not supposed to press the PIN number key directly, instead press the black or white button given below, corresponding to the PIN number. This may take about more than 16 rounds to completely enter the 4-digit PIN. This method reduced only a part of SSA.The major disadvantages of this method are that it uses the perceptual grouping concept which the hackers can easily trace out the PIN number of the user. Only two colors are used which makes the way easier to find the user PIN number. This method even takes more number of iterations which makes the PIN entry method of the user complex.

The structural format of the basic black white method is shown below in the Figure 3, for a single digit entry. Here the single digit is assumed and considered as "1". Corresponding to the assumed digit the color button is pressed.

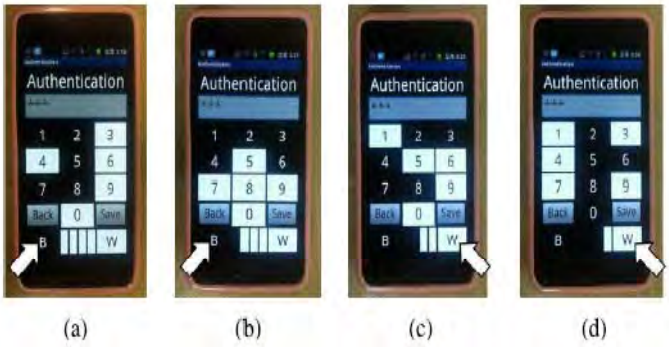

Figure 3: An example round to input 1 in IOC, where the user enters "Black," "Black," "White," and "White" in sequence. (a) Stage 1. (b) Stage 2. (c) Stage 3. (d) Stage 4.

4.3 Session key method

The basic layout of our method comprises a horizontal array of digits from 0 to 9, mapped with another array of ten familiar objects such as ⬭ and ⧋, as shown inFigure 3. The proposed method may be applied to any case with $N \geq 2$ digits.

The basic layout of our method comprises a vertical array of digits from 0 to 9, mapped with another array of ten familiar objects such as + and / etc. The first round is the session key decision round, where the symbol is selected and the remaining three rounds are PIN-entry rounds. Here, ten randomly arranged objects are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK."

In the example shown where the PIN is 2371, the user recognizes symbolas the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the *i*th digit

of the PIN is entered in the *i*th round for $i = 2, 3, 4$.This method is also known as the linear key board method and it is considered to be one of the weakest methods as it can be easily hacked using GA and RA.

Figure 4: Example of a session key decision procedure and a PIN-entry procedure for PIN 2371, in which the session key is given as ⬭ . (a) Session key decision round. (b) Challenge in a PIN-entry round. (c) User's response.

5. THE ARCHITECTURE DIAGRAM

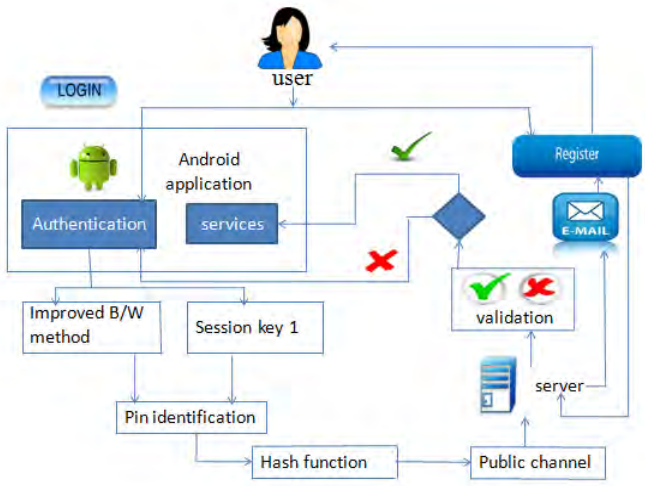

Figure 6: The Architecture Diagram

The application diagram shows the model or the workflow of the application that is been created. First, the user must register into the application. There, the user will be asked to enter the basic details such as name, password, email id, etc. Once that form is submitted, the registration will be partially completed and a unique PIN will be sent to the mail id of the user which is entered during the registration process. When the user id verified, registration phase will be completed successfully. Then, the user can login into the application with the user name and the password selected by the user during the registration process. Once the user is validated, the user gets the access rights of the service.

The user is given three options for the PIN entry such as BW method, IBW method and session key method. Any one method may be selected for entering the PIN to the application. The user's PIN is validated. Then, the ATM transactions can be performed by the user by using the application which is installed in the smart phones.

The ATM transactions include the deposit, withdrawal and balance checking. All actions can be performed in the android ATM application where the money will be in the form of tokens or images by using the virtual money concept. All kind of online transactions can be done with those token itself and it can also be exchanged into money at the exchange centers specially developed for this particular purpose. Many public threats such as theft can also be avoided.

6. THEPROPOSED METHOD

The advanced method of the Black White (BW) method, which is the Improved BW (IBW) method, is proposed by extending BW method. The proposed algorithm uses four digits which israndomly generated in a method where each digit block is combined with the bicoloured keys, to prevent the shoulder surfing attack by extracting the PIN digit after all the user iterations got completed.

6.1. The Improved Black White Method

The improved method BW method consists of two colors on the single key. A single key is divided into two halves, each half containing different colors. The user has an option to choose an upper half color or the lower half color. Even if, the shoulder surfing attack or a recording attack is been attempted during the PIN entry in this method, those human adversaries will find it difficult to guess the right PIN.

Toward complexity, the color groups are made to look overlapping, so that adversaries experience severe difficulties not only in holding the groups in VSTM but also in separating them. The fundamental idea used for combining similarity and complexity is to split visually every numeric key into two halves, so as to be filled with two distinct colors simultaneously whereas each color fills half of the available keys, i.e. half of the keys in one color and others in different color [4]. So there exist four color groups on the numeric keypad and two colors for every numeric key. The adversary who launches covert attentional shoulder surfing may need to perceive four color groups, which will be a complex task. High Authentication Services are also provided by this method.

6.2. The Android Application for ATM

The ATM is considered as the highly defected area according to this paper. Hence, the ATM application is been moved to the smart phones for the purpose of privacy and security [5]. Now-a-days, smart phones are used by most of the people and it being converted as one of the basic needs. A logical survey says that, one of every five people in the world own a smart phone.

When such an application is moved to the smart phones, a large list of things has to be considered. It may be a good thought to create this process as an android application, yet many considerations has to be made. An ATM application is created as an android application which may be downloaded and installed easily in every android mobile from the play store.

When such ATM applications are created and implemented, the transactions can be made with the smart phones and even there will be no need to use the ATM cards [5]. Each user will possess his/her ATM card but once registered in this application the transactions can be processed using smart phones. The user is given three options for the PIN entry. Any of the given method may be selected for entering the PIN to the application.

So, the entire ATM applications can be moved to the smart phones. All transactions can take place through this application which is developed for the devices that uses android operating system. This application may help the user to make all the transactions simpler and easier for the users.

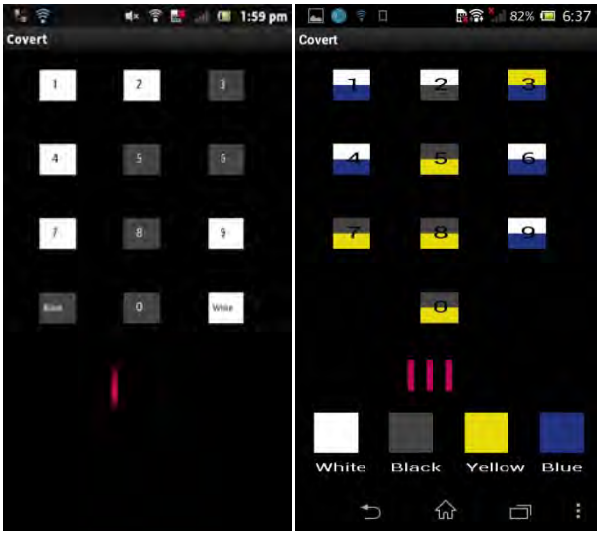

Figure 7: The Structure of BW and Improved BW method

When the application (.apk file) is installed in the smart phone, it can be initiated. The home page of an application asks for the ip address. The user should enter the ip address of the system in which the server is maintained. After verifying the ip address, the application moves to the page with the sign up and login buttons. If the user is using the application for the first time, then enter using sign up button. There the details of the user such as name, username, password, email id, etc. Then the user will receive the randomly generated 4-digit numeric password through mail. The registration process is completed.

Then, the user enters the login button and gives the username and password. After verification, the banking service will be opened. The user will be given three options to enter the PIN number securely (Figure: 6 and Figure: 7). The User can select any one method and then enter the PIN. The first method is the BW method, the second is the IBW method and the last is the session key method.

The PIN number that is entered by the user is verified by matching with the database in the server. When the PIN is sent through the public channel, there are some possibilities of hacking it. So, it is converted into the hash function and sent through the public channel.

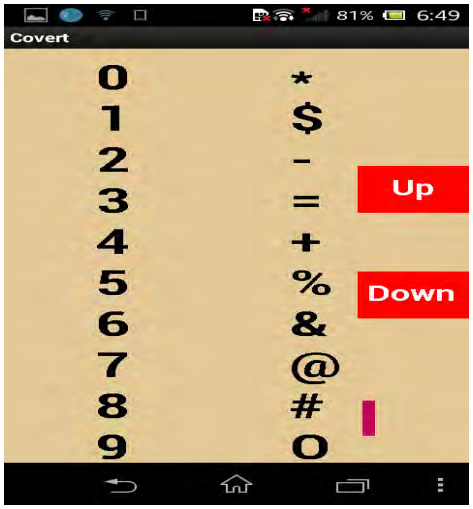

Figure 8: The Structure of Session Key method

When the PIN is verified the banking services will be opened for that particular user. The user can make the transactions such as PoS (Point of Sale), withdrawal, checking balance, mini statement, etc. The virtual money concept is used here and the tokens are generated which could have the same value of money.

7. CONCLUSION

The proposed method uses an android ATM application which can be installed in the android smartphones, along with the three pin entry methods for the user to enter the PIN securely. This will increase the security level of the password or the PIN number. This aspect gives a secure PIN entry method which mainly protects the PIN from various attacks such as SSA, GA and RA of the user.

This method shows that, even a well-trained human adversary may find it difficult to guess the PIN number even if they record the PIN entry session. As this method uses more than two colours (i.e. four colours), the PIN entry method is made protectable and entertain able for the users. This requires an inference with better optimization techniques, which can for example; reduce entry time taken by the user that may further improve the classification accuracy. The covert attention al shoulder surfing proposed in this paper is to our knowledge the first so phisticated counter-attack of human sagainstthe system, previously evaluatedtobesecure.

In addition to this, the methods which are explained in the existing system (such as black white method and session key method) is also implemented in order to find a better statistics to show that the proposed method is the more secure and the safety method. The experimental results of the existing BW method and the proposed IBW method are shown in the form of graph.

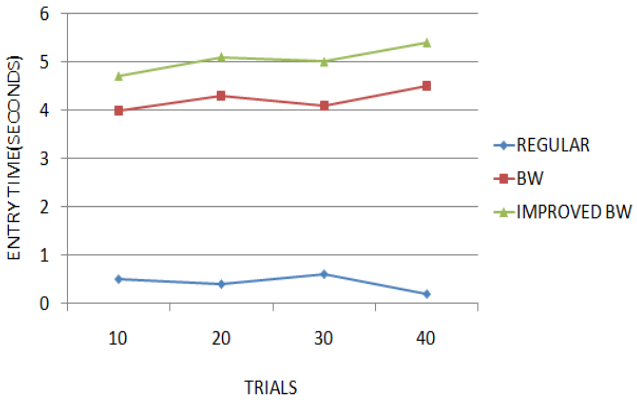

Figure 8: The graph for the comparison of PIN- entry methods

8. FUTURE ENHANCEMENT

Many forms of future enhancements can be done to this system. It is possible to upgrade the application and can make it adaptable to allenvironments. This may be done based on the optimization methods where

feasibility and the number of rounds taken for the PIN entry method can be minimized. It is also based on the OOD(object- oriented design) concept. So, any further changes can be easily adaptable. Based upon the arising security issues, the security of this application can be improved using latest and emerging technologies. This also includes the adaption of the selection bias in the future process

9. REFERENCES

[1] Taekyoung Kwon ; Sooyeon Shin ; Sarang Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected", Systems, Man, and Cybernetics: Systems, IEEE Transactions on Volume:44 , Issue: 6 , 2013.

[2] Taekyoung Kwon ; Jin Hong,"Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks", Information Forensics and Security, IEEE Transactions on Volume:10 , Issue: 2 , 2015.

[3] Drimer, S. ; Murdoch, S.J. ; Anderson, R. "Failures of Tamper-Proofing in PIN Entry Devices", Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for", Security & Privacy, IEEE , Volume:7 , Issue: 6 , 2009.

[4] Bianchi, A. ; Oakley, I. ; Dong-Soo Kwon, "Open Sesame: Design Guidelines for Invisible Passwords", Information Forensics and Security, IEEE Transactions,Volume:45 , Issue: 4 , 2012.

[5] Peipei Shi ; Bo Zhu ; Youssef, A. "A rotary PIN entry scheme resilient to shoulder-surfing", Internet Technology and Secured Transactions, 2009. ICITST 2009.International Conference, 2009.

[6] Taekyoung Kwon ; Sarang Na, "switchpin: Securing smartphone PIN entry with switchable keypads", Consumer Electronics (ICCE), 2014 IEEE International Conference, 2014.

[7] Jacomet, M. ; Goette, J. ; Eicher, A. "On Using Fingerprint-Sensors for PIN-Pad Entry", Electronic Design, Test and Applications, 2008. DELTA 2008.4th IEEE International Symposium, 2008.

[8] Perkovic,T.; Cagalj, M.; Rakic, N." SSSL: Shoulder Surfing Safe Login", Software, Telecommunications & Computer Networks, 2009. Softcom2009.17th International Conference, 2009.

[9] MichichiroKoibuchi, KenichiroAnjo, Yutaka Yamada, AkiyaJouraku, and Hideharu Amano," A Simple Data Transfer Technique Using Local Address For Networks-On-chips", Parallel and Distributed Systems, IEEE Transactions On Volume:17, Issue:2, 2015.