I J C T A, 9(9), 2016, pp. 4061-4066

Random Pattern Security in Automatic Teller Machine

Nandhini J.[1], Nazreen Banu A.[2], Vinod S.[3], Insozhan N.[4] and Rajasekaran S.[5]

ABSTRACT

One of the most commonly occurring problems 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 attacks are 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. In our proposed method instead of using a single pin, a new pin is generated for every usage of the ATM by the user.

Key words: personal identification number; improved black White (BW) method; shoulder surfing attack; Mobile application; pattern matching

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. 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. 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.

In our proposed system once the user login into the ATM application which is developed the user is able to see a number grid which is displayed. The used task is to select a pattern location in the number in the number grid. Once the pattern is selected it is mapped with user account number into the bank database. If the user wish to change he/she can also change the pattern when the user enters into the ATM a number grid displays on the screen in the insertion of the ATM card. Now the user task is to see the number that is matched with the pattern selected before and now he/she should type the number that is mapped with the pattern. Once the authentication is done successfully he/she may proceed with the transactions.

[3,4] Assistant Professor

[1,2,3,4] Department of Computer Science and Engineering, Vel Tech Multi Tech Engineering College, Avadi, Chennai-62, Tamilnadu, India, *Emails: nandhini.raman20@gmail.com, nazreenbanu8@gmail.com, vinodsundaram.s@gmail.com sozhanme@gmail.com*

[5] Ph.D. Scholar, Department of Computer Science and Engineering, Bharath University, Chennai, Tamilnadu, India, *Email: rajasekaran009@gmail.com*

2. ATTACKS ON PIN ENTRY

Some of the related attacks that may be performed on a 4-digitPIN 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 Surfing Attack (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 secret4-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 coloring that his PIN digit had in these n rounds. The oracle has only a limited period of time to determine the color of the current PIN digit in each round, and the color sequence must be memorized. This procedure is repeated until all PIN digits are entered.

4.2. The Basic BW Method

The basic BW method partitions a set of ten digits in to 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 form, consecutive rounds and recalled to derive their Grouping Patterns, the shoulder surfer could identify a single digit of the PIN.

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 o and$, as shown in Fig 2. 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

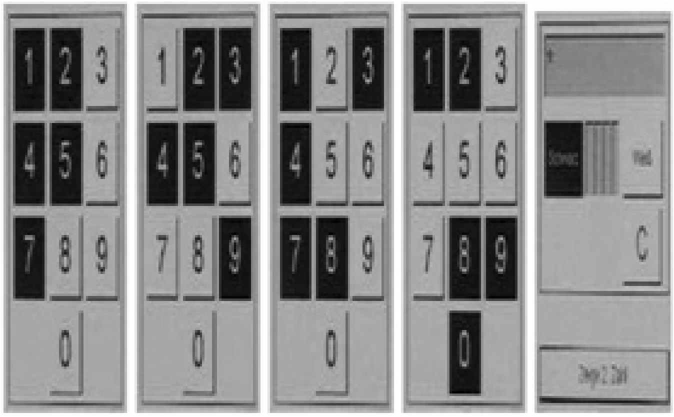


Figure 1: The above sequence illustrates the DOC. Appears subsequent to the display of the four patterns. The oracle must enter the sequence of colors of the correct PIN digit

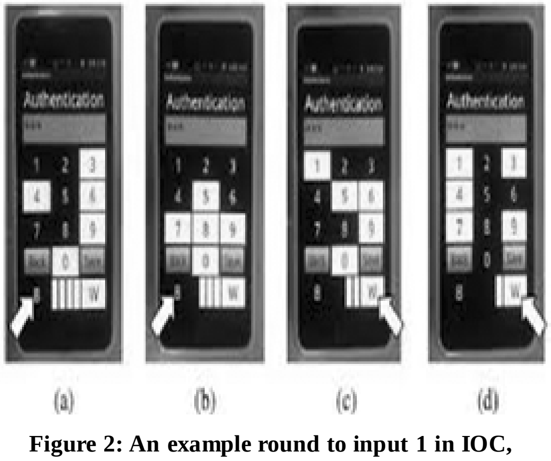


Figure 2: An example round to input 1 in IOC, where the user enters “Black,” “Black,” “White,” and “White” in sequence. (a) Stage 1. (b) Stage 2. (c) Stage 3. (d) Stage 4

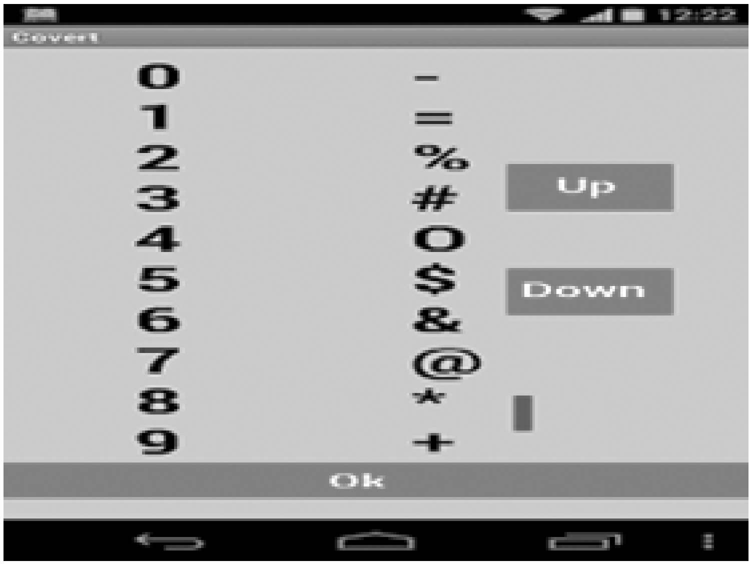


Figure 3: Example of a session key decision procedure and a PIN-entry procedure for PIN 2371, in which the session key is given as. (a) Session key decision round. (b) Challenge in a PIN-entry round. (c) User's response

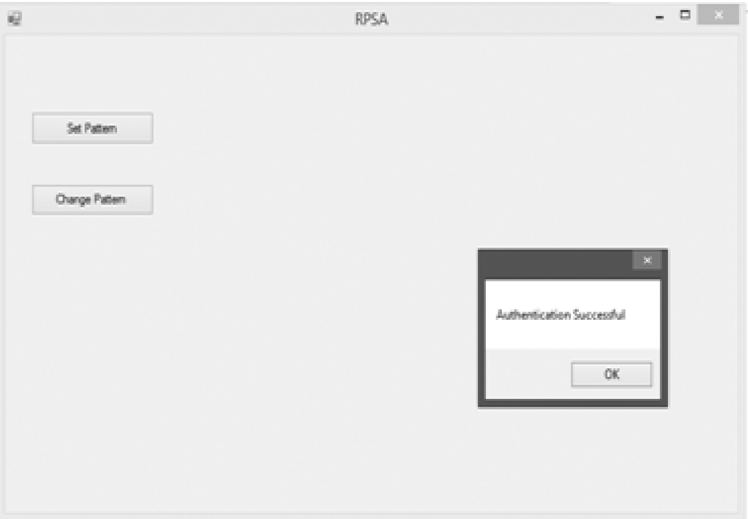
decision round, where the symbol is selected and the remaining three rounds are PIN-entry rounds. Here, ten randomly arranged objects are displayed to the user. The user recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK."

5. PROPOSED METHOD

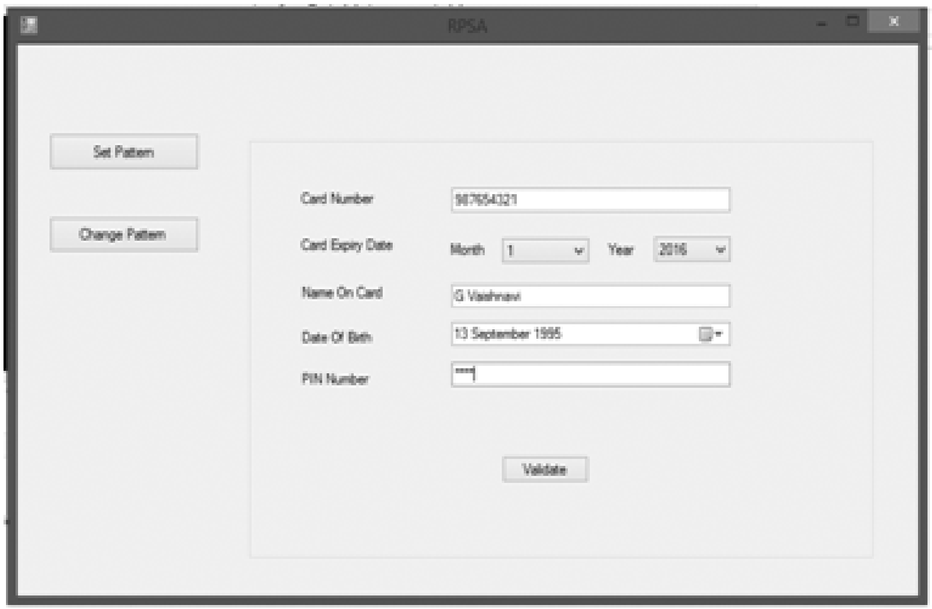
In our Random pattern security method the keys are statically mapped according to their location but the key values are dynamically mapped according to the pattern. Our proposed model consist of two part the first is the selection of the pattern by the user and mapping it with the account number, and the second part is the generation of unique pin for the every usage of the atm. Our simple idea can render the surprisingly fast and user-friendly PIN entry method with good resilience to shoulder-surfing attacks.

5.1. Selection of the Pattern by the User

In our first part the user should log into the pattern application using his account no and other details. Once the user is authenticated successfully then only he is further proceed to set or change his pattern. If the authentication is failed a authentication error is displayed



Authentication Successful



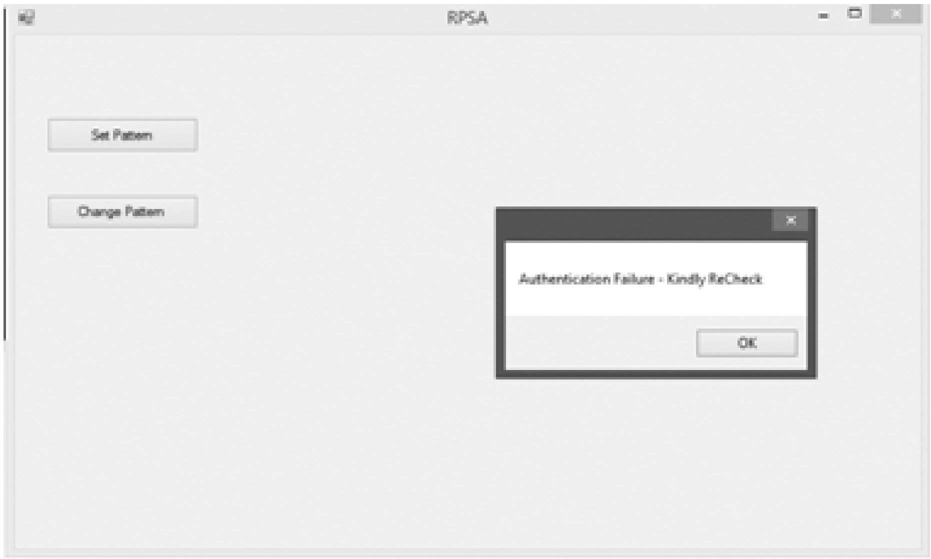
Card Number 987654321

Card Expiry Date Month 1 Year 2016

Name On Card G Vaishnavi

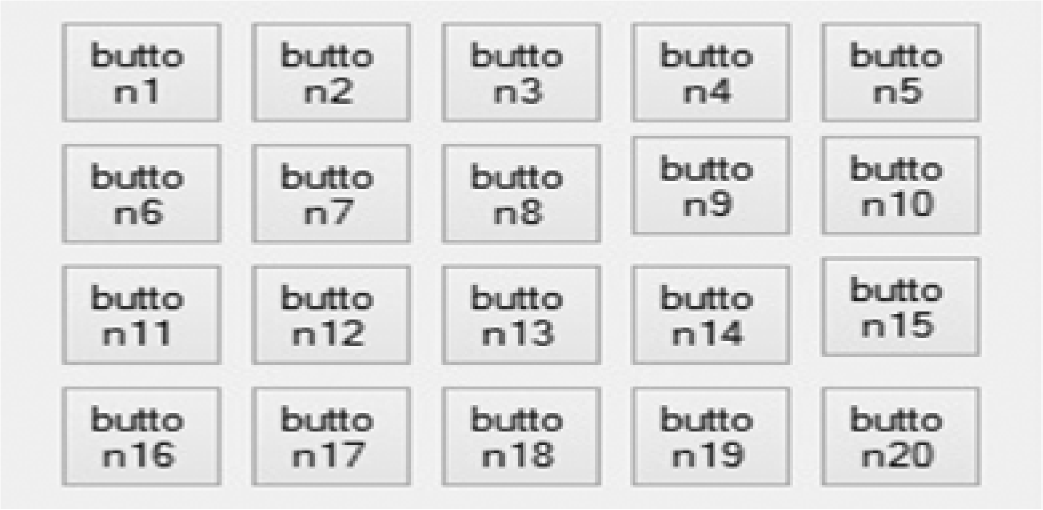
Date Of Birth 13 September 1995

PIN Number ****



Authentication Failure - Kindly ReCheck

Once the authentication is done the a grid is displayed on the screen the user has to select any location on the grid which is stored in the form of pattern and mapped with the user account in the bank database.



button1	button2	button3	button4	button5
button6	button7	button8	button9	button10
button11	button12	button13	button14	button15
button16	button17	button18	button19	button20

5.2. Pattern Mapping–Pin Entry Method

Now when the user inserts a ATM card in the ATM a number grid is displayed in the screen. The number in the grid changes for every 20 sec. Now the number that is present in the location of the pattern chosen already acts as a pin number in that session user should enter the pin number in that is present in the location of the pattern chosen before in the number pad once the number pressed is mapped and verified with the database then the transaction is successfully allowed to carried on. The user is also allowed to change the pattern using a mobile application developed if he feels insecure during every transaction.

6. CONCLUSION

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 because the pin changes for every 20 sec. It also uses a mobile application through which user is able to choose his pattern anywhere and anytime. As a result of the work proposed there will be benefit to human beings for the purpose of ATM security.

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.International Conference for”, Security & Privacy, IEEE, and 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