Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Security for Safety PIN Entry

Sivakani. R
Department of Computer Science and Engineering, Apollo Engineering College, Chennai, Tamilnadu, India

Abstract— In the modern world everything were computerized due to the technological development. The computerized world is full of frauds and crime so to reduce it we want to introduce new techniques. In the modern world everybody are using the ATM (Automated Teller Machine) cards for transaction in the ATM. All the banks placed the computerized ATM everywhere for full fill the needs of the customers. In the ATM center there is no safety for the people. Even though the state and central government has put so many rules for fixing the ATM the ATM fraud is not controlled. While using the ATM cards the PIN (Personalized Identification Number) is used multiple times at multiple systems for multiple sessions. The shoulder-surfing attacks can be done by observing the PIN entry. The shoulder-surfing can be done at distance using the binoculars and nearby using the cameras fixing on the walls etc., To avoid shoulder-surfing and for providing security we can use Steganography technique. Steganography is the technique used to concealing the message with another message. The secrete message can be hidden using another ordinary message. StegnoPIN technique is we are introducing to provide security. In this technique the PIN entered by the user can be hidden using the stegrography technique so the shoulder-surfing can be avoided. In this method tow keypads are used one is covered and another one is open. This can be done using the smart phones.

Keywords- ATM, StegnoPIN, Shoulder-surfing.

I. INTRODUCTION

The day-today activities are computerized due to the technological development. The computerized world is full of frauds and crime so to reduce it we want to introduce new techniques. In the modern world everybody are using the ATM (Automated Teller Machine) cards for transaction in the ATM. All the banks placed the computerized ATM everywhere for full fill the needs of the customers. In the ATM center there is no safety for the people. Even though the state and central government has put so many rules for fixing the ATM the ATM fraud is not controlled. While using the ATM cards the PIN (Personalized Identification Number) is used multiple times at multiple systems for multiple sessions. The shoulder-surfing attacks can be done by observing the PIN entry. The shoulder-surfing can be done at distance using the binoculars and nearby using the cameras fixing on the walls etc.,

Fig. No.:1 Shoulder-surfing attackers tracing the PIN[3]

To avoid shoulder-surfing and for providing security we can use Steganography technique. Steganography is the technique used to concealing the message with another message or image. The secrete message can be protected using another ordinary message. StegnoPIN technique is we are introducing to provide security. In this technique the PIN entered by the user can be hidden using the stegrography technique so the shoulder-surfing can be avoided. In this method tow keypads are used one is covered and another one is open. This can be done using the smart phones. To find indirect method for entering the PIN for supporting the user from the shoulder surfing attacks this method is developed using two keypad techniques using the steganoPIN. Steganography=hidden message + carrier + key. In steganography there are so many methods to protect the data which is sending from one user to the other from that we have choosen visual semagrams to hide the PIN from the attackers. In semagrams the PIN is protected using the symbols or signs. In this we have two keypads and the attacker doesn't know that there are two keypad. When we keep the hand in a cup shape we can see the original PIN and for the attackers it will be shown as sign or symbol, so that they cannot trace the PIN.

In the StegnoPIN method, the security is provided using the PIN authentication system for the ATM using smart phones. The authentication is done at the user side and a onetime password is generated for each PIN entry. The user

want to fold his hand as cup and keep on the keypad, the user can see the shuffled keypad, and the user want to enter the OTP in the regular keypad.

II. SYTEM ARCHITECTURE

When a user use the PIN in smart phone, first the user want to register their information and a e-mail will be send to them from the server in that their login id will be given, using the login id he/she can login frequently.

When a registered user login the authentication can be done using 2 way session key and steganopin method, in session key method, a random PIN is generated and is to be entered instead of using their PIN, it is OTP so the shoulder-attacking can be avoided.

The user is validated means then the transaction can be allowed to do by that user. The process is checked by four stages.

1. User registration
2. Session Key Management
3. SteganoPIN Authentication
4. Banking and Services

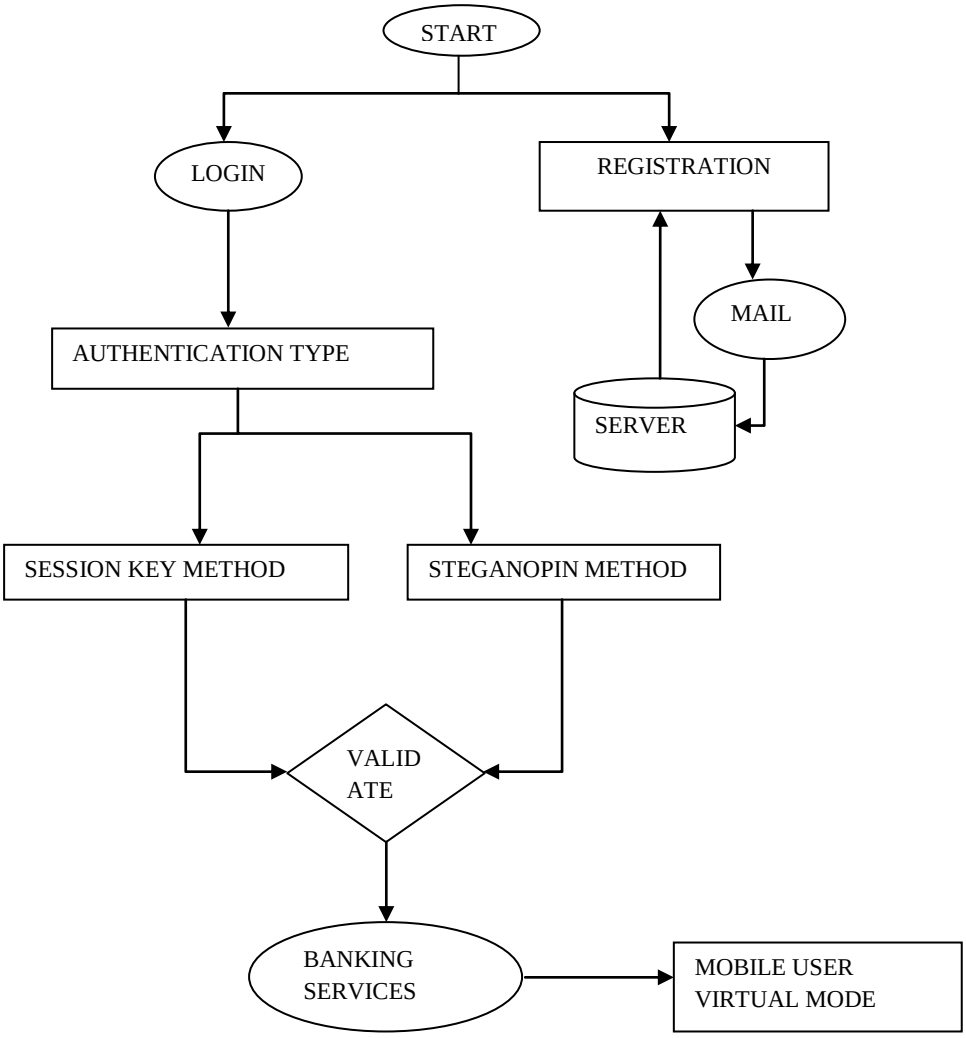

Fig. No.1: System Architecture

A. User registration

In the user registration part, for using this application the user is to register. The registration process is completed means that user will be considered as authenticated user and a mail will be send to the user, in that mail a unique PIN will be given. After validating that user will be allowed to access this application be giving the username and password.

B. Session Key Management

This is a type of PIN entry method. This method has a vertical array with digits from 0 to 9. That array value will be juxtaposed with another array with 10 symbols such as + _ ? / etc. Here we are considering the PIN numbers with 4 digits so we want to apply this with N>= digits.

In this example we need four rounds. In the first round the session key is decided and the remaining three rounds are the PIN entry rounds. In the session key round the symbols are arranged randomly for the display. The user wants to identify the symbol that is displayed below the digits in the temporary session and press ok. For each round the random

array of the symbols are given and the user needs to choose the symbols for the entry. The user can use the left and right buttons also. Every entry can be done by the user with different symbols but for a single OPT a particular symbol should be given.

C. SteganoPIN Authenication

SteganoPIN authentication can be done using the smart phone and tablet to sense the events on the keypad. The keypad does not appear immediately. The response keypad appears with regular layout. The keypad appears only when a user keeps the hand as a cup shape on the keypad closed. It has 2 keypads, one is standard keypad with regular layout and the other keypad is a random layout, and is called as challenge keypad. The user is to use this challenge keypad for the OTP.

D. Banking and Services

When a user enter the PIN using the pattern and is identified, then it will be checked with the local database. This is to provide security for the user and preventing from the hackers. After getting the PIN, OTP is generated and is given to the user so that the attacker cannot extract the PIN by monitoring the channel. The user is authenticated means then the user is allowed to do the banking service such as cash withdrawal, fund transfer etc.,

III. CONCLUSION

In this paper the PIN security using steganapin technique is discussed for protecting the PIN from the attacker and using session key generation also the protection is given for the PIN. This method is very useful to the user because the attackers cannot trace the PIN and it provide security to the user.

REFERENCES

[1] Taekyoung Knon, SteganoPIN:Two-Faced Human-Machine Interface for Practical Enforcement of PIN Entry Security , IEEE Transactions on Human-Machine Systems, 27 July 2015 pp.143 – 150.

[2] A. Parti and F. Z. Qureshi, ―Integrating consumer smart cameras into camera networks: Opportunities and obstacles, IEEE Comput., vol. 47, no. 5, pp. 45–51, May 2014.

[3] A. Greenberg. (2014, Jun.). Google glass snoopers can steal your passcode with a glance, Wired. [Online]. Available: http://www.wired.com/ 2014/06/google-glass-snoopers-can-steal-your-passcode-with-a-glance/

[4] T. Kwon, S. Shin, and S. Na, ―Covert attentional shoulder surfing: Human adversaries are more powerful than expected, IEEE Trans. Syst., Man, Cybern., Syst., vol. 44, no. 6, pp. 716–727, Jun. 2014.

[5] Q. Yan, J. Han, Y. Li, and R. H. Deng, ―On limitations of designing leakage-resilient password systems: Attacks, principles and usability, in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.

[6] B. Song, C. Ding, A. Kamal, J. Farrell, and A. Roy-chowdhury, ―Distributed camera networks, IEEE Signal Process. Mag., vol. 28, no. 3, pp. 20–31, Apr. 2011.

[7] J. Long and J. Wiles, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Boston, MA, USA: Syngress, 2008.

[8] A. De Luca, M. Langheinrich, and H. Hussmann, ―Towards understanding ATMsecurity—A field study of realworldATMuse, in Proc. ACMSymp. Usable Privacy Security, 2010, pp. 1–10. [9] J. Rogers, ―Please enter your 4-digit PIN, Financial Services Technology, U.S. Edition, vol. no. 4, Mar. 2007.

[9] V. Roth, K. Richter, and R. Freidinger, ―A PIN-entry method resilient against shoulder surfing, in Proc. ACMComput.Commun. Security, 2004, pp. 236–245.

[10] T. Matsumoto and H. Imai, ―Human identification through insecure channel, in Proc. Adv. Cryptol., 1991, pp. 409–421.

