National Conference on 'Innovative Research on Robotics, Circuits and Technology' (IRCT 2018)
Organized By : CIrcuit Branches of SCSVMV, (EEE, ECE, EIE & Mechatronics) , Kanchipuram, Tamil Nadu, India
In Assotiation with International Journal of Scientific Research in Science, Engineering and Technology
© 2018 IJSRSET | Volume 5 | Issue 1 | | Print ISSN: 2395-1990 | Online ISSN : 2394-4099

Session Key for secured ATM Transaction

M. Vinoth
Research Scholar, Department of ECE, SCSVMV, Kanchipuram, Tamil Nadu, India

ABSTRACT

Personalized identification number (PIN) entry method is highly unsecured due to various threats. To avoid these threats in bank transaction platform, we introduced two methods name STEGNO PIN and SESSION KEY which helps the user for safe bank transactions. In both the methods the main concept is to hide the pin numbers. In stegno pin we going to enter the pin number based on the shuffled position of the numbers in the virtual keypads, while in session key we going to achieve the secured traction by random generated symbols. User as the option to choose any one way of pin entry method through this applications .Once the pin number is entered then the application is redirects to the users banking service.

Keywords: Stegnopin, session key

I. INTRODUCTION

These personalized identification number (PIN) entry applications are increasing due to the development of touch screen which facilitates the implementation of pin entries interface on various commodities such as Automated teller machine (ATM), point of scale POS terminals, debit cards terminals, digital door lock, smart phones and tablet computers.

CONCEPT:

In this paper each ATM card will have separate four digit PIN number. The pin will be initially sent to the people as authentication on the time of their registry through this mobile application. We are going to hide the PIN by using Stegnopin or Session key method for secure transaction of money. Because nowadays transaction of money through mobile application is most popular and also less secure.

Requirements:

A) Hardware:

The software requirements are the specification of the system. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks, tracking the teams, and tracking the team's progress throughout the development activity.

- ✓ Windows 7 and above
- ✓ JDK 1.7
- ✓ Tomcat 6.0
- ✓ My sol. 5.0.

B) Software:

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It shows what the system does and not how it should be implemented.

- ✓ Hard Disk: 250GB and Above

- ✓ RAM : 4GB and Above
- ✓ Processor: I3 and Above
- ✓ OS: Gingerbread and above.
- ✓ No of Devices : 1.

VARIOUS ATTACKS IN PIN ENTRY:

- Guessing Attack.
- Shoulder Surfing Attack.
- Recording Attack.

A) Guessing Attack:

In guessing attack the attackers predict the user pin number and enter the number at an ATM machine so that they can get access to the banking account without the user's knowledge and the required transaction of money can be done. They can even block their account by entering the wrong pin more than thrice.

Figure 1

B) Shoulder Surfing Attack:

Shoulder surfing is a direct observation techniques to collect the data. This is an effective way to get information in the public places, because it's easy to stand next to someone and watch as they fill out any applications, using credit cards in shopping malls or ATM. Sometimes the vision-enhancing devices are also helps in this shoulder surfing attack, if subject is in far distance.

Figure 2

C) Recording Attack:

In recording attack the attackers use a skimming device or miniature cameras to record and hack the PIN (i.e.) Small cameras are fixed by the intruders inside the ATM to record the particular actions such as PIN entry, and the user gather all the required information even without their presence in that particular area. Such type of attacks is a great threat to society nowadays.

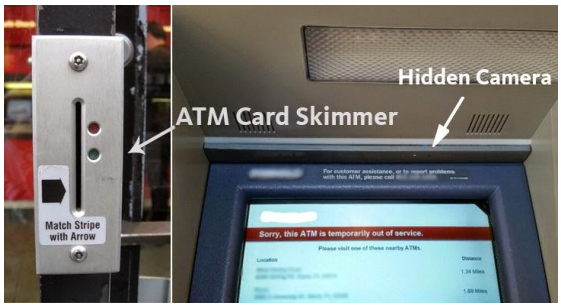

Figure 3

Why Android?

Android is the fast growing environment in which many kinds of applications are running successfully. This development of android is mainly for the easy access to the user with safe UI environments . Lets now learn some basic details about the android open source environment and also its applications.

Android:

Android is a Linux based open source operating system designed for use on cell phones, e-readers, tablet PCs and other mobile devices. For users of smart phones, Android provides easy access to social networking sites like Face book, Twitter and YouTube and smooth integration with Google products like Gmail, Google maps and Google calendar. Android has been adopted by a number of manufactures Motorola, Samsung etc.

II. ANDROID ARCHITECTURE

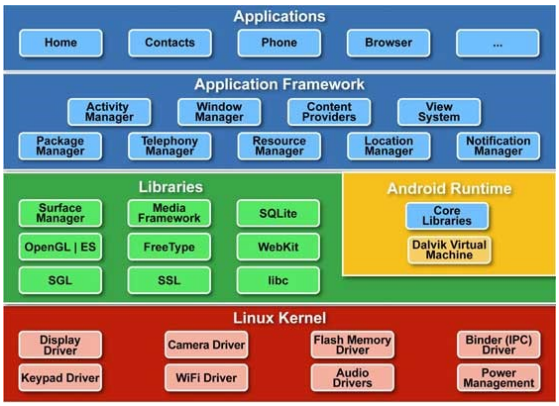

Figure 4

Applications of android:

- Android applications are composed of one or more application components (activities, services, content providers and broadcast receivers.
- Each components performs a different roles in the overall applications behavior and each one can be activated individually (even by othe applications).
- The manifest files must declare all components in the applications and should also declare all applications requirements such as minimum version of android required and any hardware configuration required.
- Non-code application resources (images ,strings, layout flies ,etc)should include alternatives for different devices configuration such as different strings for different languages

Flow chart:

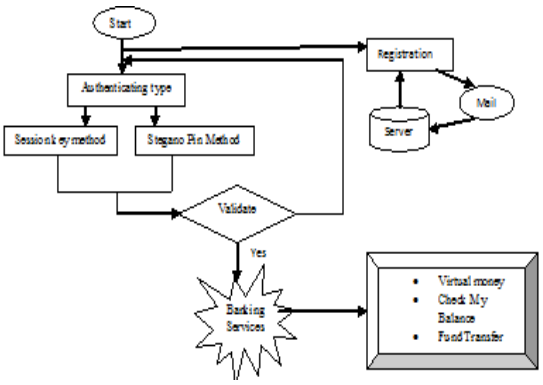

Figure 5

System Architecture:

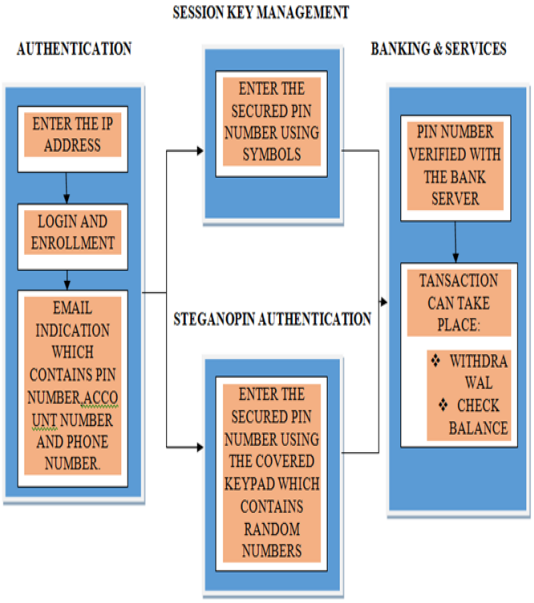

Figure 6

MODULES:

1. Authentication
2. Session Key management
3. SteganoPIN Authentication
4. Banking and Services

AUTHENTICATION:

User Registration is done and after that the user is able to access the ATM application in their mobile phones. Once their Registration is successfully completed, the user will be provided with the unique pin number which is sent to their registered mail Ids as the Mail Alert.

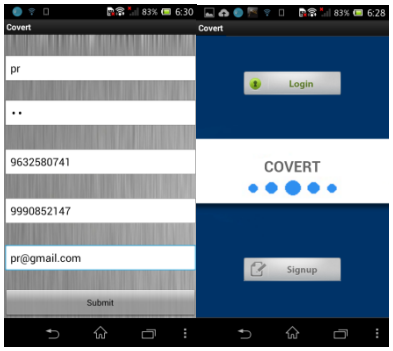

Figure 7

A) Mail Alert:

Mail Alert is just the form of authentication to the user which contain certain details like Account Holder Name, Pin Number, Account Number, and also the Amount present in their account which will helps in transaction

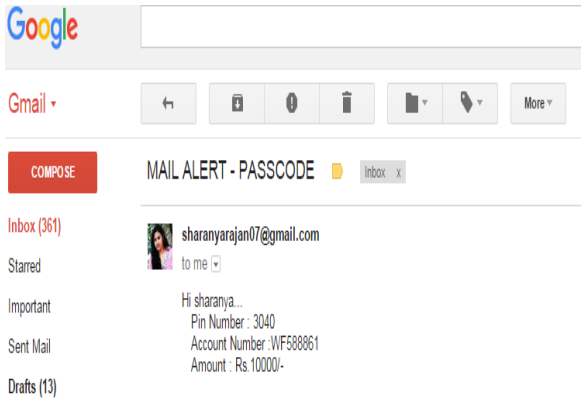

Figure 8

Once we get registered with the application we can use the same username and password for login. The pin number is used to access the services.

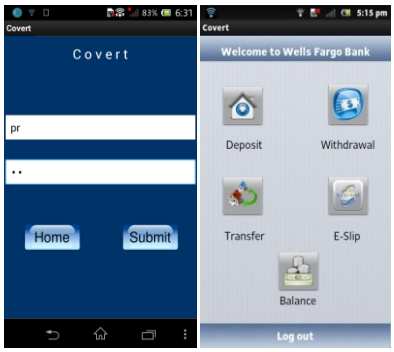

Figure 9

III. MODES OF ENTRY

In this process there is two method of pin transaction as we already mentioned before we can make any one of the mode of selesction as per the users wish. The two modes are as fallows:

- Stegnopin method
- Session key method

Figure 10

IV. SESSION KEY MANAGEMENT

In this session key method we are going to use the randomly generated symbols for the transactions. This method is designed in such a way that 0 to 9 digits arranged in vertical column and next to it another vertical column of ten symbols are arranged. The pin numbers is restricted to four digits which mean four rounds. The first round is session key decision round and the remaining three round are pin entry rounds. In each session key decision round the ten symbols are randomly generated, arranged and displayed so that attackers cannot guess the PIN number. For example, 2894 is the pin number the user selects the symbols next to each of the number 2,8,9,4 and Press "OK". In order to achieve this user is provided with the control buttons such as UP and DOWN, which helps the user to select the exact PIN without any flaws. .

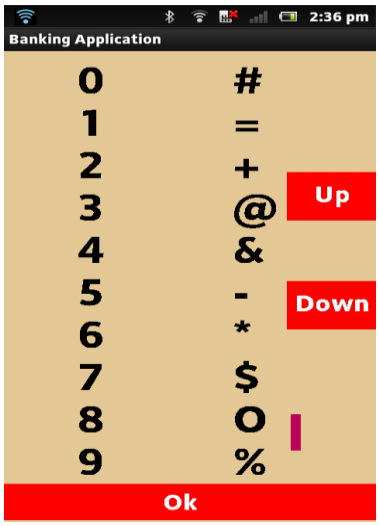

Figure 11

StegnoPIN Authentication:

The stegnopin system is uses two keypads one is the illusion and the other is response keypad. The response keypad appears in front of the user with regular layout and size. The illusion keypad appears in front of the user only when the screens senses the "P" shaped user cups. The illusion keypad help the user to select the position of the pin numbers, the keypad disappears once the "p" shaped user cups are removed. The illusion screen is also called as challenge keypads were the generated OTP by user registration are used. Finally the user enters the pin numbers on the regular keypads or response keypads based on the position of the virtual keys.

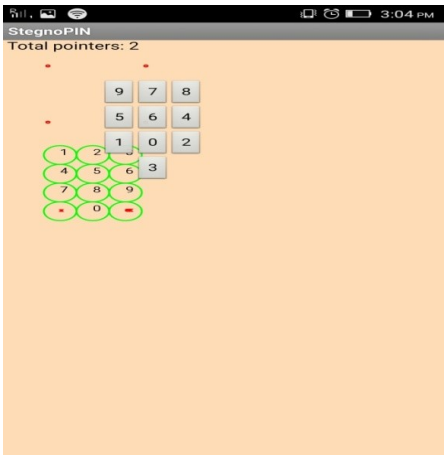

Figure 12

BANKING AND SERVICES:

Once the user has entered the OTP their respective pin number is identified. The pin number will be checked with the local database provided by the Sol. lite in order to continue the transaction, then one way hash method has been generated for the validation of pin entry which has been send to the server in the public channel so that the attacker cannot guess the pin by monitoring the channel .After verification the mobile app will provide a response to redirect the user to the services. In ATM services cash withdrawal and deposit and fund transfer can be done safely.

ADVANTAGES:

- ✓ Transaction of money is Safer.
- ✓ Security of PIN is also achieved.
- ✓ User Friendly Platform.

V. CONCLUSION

Our paper is proposed to minimize the attacks that prevail in ATM transactions. This mobile application will be more useful to this digital world which lacks in security. This is simple to install. Hence leads to the safer transactions of money between the bank and the customer.

VI. REFERENCES

[1]. Moving ATM Applications to smart phones with a secured PIN- Entry method Volume 17,issue 1,ver 11(Jan-Feb 2015),Pg 58-65(IOSR-JCE).

[2]. Defending Shoulder Suffering Attack in secured transaction using session key method Volume 4,issued 2,feb 2015 (IJSETR)

[3]. Convert additional shoulder suffering human adversaries are more powerful than expected,IEEE Trans.Syst,Man.Cybern,Syst,vol 44,no 6,pp.716-jun 2014

[4]. Switch PIN: Securing Smart phone PIN entry with switchable keypads. In Proc IEEE Int Conf.Consumer Electron, 2014, pp 27-28.