www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 10 Oct. 2016, Page No. 18707-18713

A Secure Pin Authentication Method against Shoulder Surfing Attacks

K.Kiruthika[1], D.Jennifer[2], K.Sangeetha[3], Jackulin.C[4], R.Shalini[5]
Panimalar Engineering College,
Chennai, Tamilnadu.
[1]*kiruthikaitdept@gmail.com*
[2]*pecjennifer@gmail.com*
[3]*sankrish2007@gmail.com*
[4]*chin.jackulin@gmail.com*
[5]*shalinirajendren@gmail.com*

Abstract: Users normally tend to reuse the same personalized identification number (PIN) for multiple applications. Direct PIN entries are highly susceptible to shoulder-surfing attacks as attackers can effectively capture user's PIN entry number with the help of concealed cameras. Indirect PIN entry methods proposed as counter measures are rarely deployed because they demand a heavier cognitive workload for users. To achieve fool-proof security and usability, a practical indirect PIN entry method called SteganoPIN is proposed. The human–machine interface of SteganoPIN comprises two numerical keypads: one shielded or hidden and the other exposed, designed specifically to physically thwart and protect against shoulder-surfing attacks. After locating a long-term PIN in the more usual layout, through the covered permuted keypad, a user generates a one-time password that can safely be entered in plain view of attackers. This enables the user to establish a secure transaction by means of a mobile app to the server by implementing the SteganoPIN method using multi-touch concept that is based on independent variable PIN entry system (Standard PIN, SteganoPIN).

The main objective of the project is to create an android application for coping with shoulder-surfing attacks using multi-touch concept in SteganoPIN method. Only after the user PIN entered in the shuffled keypad matches with that of the static keypad, the authentication is then confirmed.Thus, this method allows the user to perform a safe banking transaction through multi-touch SteganoPIN concept. By this method, when the user details are sent to the bank server, a unique MAC id is generated, which should match the user's PIN and MAC id registered in the bank. There are two keypads: static and challenged (or) shuffled key pads; the challenged keypad becomes visible only if the proximity sensor senses the user's cup-shaped hand gesture.

Keywords: SteganoPIN, MAC, machine, shuffled key pads, sensor.

1. Introduction

Shoulder-surfing attack poses a great threat for the users performing the banking transactions in the modern world [1]. These attacks are more common in the densely crowded areas especially in the ATM and POS systems. Many methods have been proposed in order to provide a secure platform free from shoulder-surfing attacks, but the attackers are more shrewed and smart in overcoming those methods through innovative counter measures. There are several studies in the literature which focus in this subject.

Ming Lei.et al. [2] proposed a virtual password concept involving only a minimum amount of human effort in creating a secure user's password in the online environment. It protects the user against phishing of the key logger and shoulder-surfing attacks. A virtual password is a password which cannot be applied directly but instead by generating a dynamic password which is submitted to the server for authentication. To generate a virtual password, a human computing effort is involved or a hand-held device which can be programmed to create the dynamic password is needed. By this way, one can generate randomized linear generation functions to secure one's password.

Huanyu Zhao and Xiaolin Li in 2007 [3] describes about a password authentication method by integrating textual and graphical modes of inputs. It is somewhat similar to that of convex hull-click method which involves using the expressions to create a pass triangle. For a personalized identification number (PIN) of four digits, the pass triangle must be selected using at least four attempts. This enhances the security to a greater extent than that of the CHC. Thus, a brute force attack is avoided. The main drawbacks of this method are that it takes long time to authenticate and it is very difficult to trace the pass triangle.

T. Perkvoic et al. in 2009 [4] proposed a novel method applying a novel PIN entry scheme called shoulder-surfing safe login (SSSL) to provide enhancement to the classical PIN method. The methodology uses is shoulder-surfing interface table. Here for every trial made by the user, a unique challenged id is generated for the PIN. In a 5 × 5 matrix, the static keypad is located in the center which covers an area of about 3 × 3 matrix from the center and the row and column surrounding the 3 × 3 matrix keep on changing for every event. The challenged id code is generated by the system. For every digit in a PIN there are eight directions in which the challenged key codes must be selected. However, there is an increased chance of threat from side channel and brute force attacks.

PeipeiShi et al. in 2009 [5] devised an alternative solution for convex hull click, which uses one- and two-variant methods. In the one-variant method, there are concentric circles equal to the number of PIN digits, which are divided into A sectors. The users should set up the PIN using their fingers which can be anywhere within the A sectors. If any one sector matches that of the user PIN, then the authentication is provided. On the other hand, in the case of two-variant methods, the given input is authenticated in two steps, for example, if there are four digits in a PIN, then the first two digits are authenticated by the same one-variant method as above followed by the authentication of the remaining two digits. In this method, the user's no longer required to memorize anything about the PIN. However, the drawback of this rotary method is that it is more susceptible to brute force

attack and that a surreptious video recording of this operation could easily reveal the users PIN.

Muhammad Shakir and Abdul Ayaz Khan in 2010 [6] proposed a method in lieu of the textual and graphical password method, which uses a formula method session. In this method, the user will first enter the textual password. Then the user should remember the formula which was registered with the user's account. The value calculated using the formula is called the token value. Once the token value is calculated, it should be added, subtracted, or multiplied based on the arithmetic operation assigned for each digit in the PIN to obtain a logical value. Logical values are those which are calculated from that of user's PIN, where each digit in the PIN has a unique value for a specific event, but this value keeps on changing for every session. The drawback of this method is that the user must have basic arithmetic computing knowledge.

Alexander De Luca et al. in 2010 [7], on the other hand, proposed a method in which the every digit in the keypad is assigned three alphabets randomly which keeps on changing for every trial made by the user, where the first alphabet of each digit indicates black, red, and white. In case of a four-digit PIN, the user must enter the alphabet which corresponds to that of black, followed by red for the second digit, then white for third digit and then again black for the fourth digit. The chance of error rate in this method is, however, quite high as the user has to memorize the challenged PIN for every session.

Andrea Bianchi et al. in 2011 [8] proposed a method to resist the shoulder-surfing attacks in mobile phones by simple method in which for every trial, the phone password keeps on changing and the new password which is intimated through an audio. The user then enters this PIN using the virtual wheel displayed on the mobile screen. The application displays the buttons for selection and screen navigation too. The main drawback of this system is that a motor is attached externally to the device which makes it difficult for the user to carry it along and makes the system to be less portable during the operation.

Kavitha V. and Dr. G. Umarani Srikanth in 2015 [9] proposed a method that uses the PIN entry methods which offers protection against such attacks. The PIN entry methods that are used in the proposed system include 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 incorporated 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 guessing attack (GA), where 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 result in failure even after several attempts until s/he succeeds in inputting the correct PIN. For example, a typical ATM permits a maximum of three trials. Therefore, the following the protocol for the proposed security of a PIN-entry method is said to deter the attacker form succeeding in his/her guessing attack.

Haichang Gao et al. [10] describes about the evolution of the colourlogin graphical password scheme. It proposes the recognition-based graphical password scheme for greater security. The image background colour is used as a safety factor in colourlogin. It provides an authentication method to ensure resistance against shoulder-surfing and intersection attacks. A pass-icon is chosen correctly when the bonafide user clicks on the row which contains the pass-icon. The icons in the row are all replaced with the substituted lock-icon code to deter resist-shoulder surfing attack. It reduces the time consumption through the encryption of the icons.

Abdullah Ali, Ravi Kuber and Adam J. Aviv [11] described the design and evaluation of H4Plock (pronounced "hap-lock"), a novel authentication mechanism to address the threat situation .In order to authenticate, the user enters up to four pre-selected on-screen gestures, informed by tactile prompts. The system has been designed in such a way that the sequence of gestures will vary over each authentication attempt, reducing the capability of a shoulder surfer to recreate entry. 94.1% of participants were able to properly authenticate using H4Plock, with 73.3% of them successfully accessing the system after a gap of 5 days without any rehearsal.

Yoshihiro Kita et al. [12] designed and proposed a new icon-based authentication method that is simple but sufficiently secure even when the authentication sequence is being watched. The proposed method is implemented on a mobile data terminal and is evaluated through experiments and questionnaire surveys.

2. Proposed System

Our proposed system design is based on SteganoPIN method where Stegano means protected. Here, the numeric keys entered by users in plain view of adversaries must be one-time PIN (OTP) keys that conceal a real PIN following instant derivation. We proposed the PIN entry method that is able to achieve both good security and practical user-friendliness**.** The human–machine interface of SteganoPIN consist of two numeric keypads: one shielded/hidden and the other exposed, designed to physically thwart any threat from shoulder-surfing attacks. After locating a long-term PIN in the more typical layout, through the covered permuted keypad, a user generates a one-time PIN that can safely be entered in plain view of attackers. Our proposed system uses two independent systems of PIN entry system:

1. PIN entry system
    a. Standard PIN and
    b. SteganoPIN

The PIN entry time in SteganoPIN (5.4–5.7 s) is longer but acceptable, and the error rate (0–2.1%) was not significantly different from that of the standard PIN.

SteganoPIN affords resilience against camera-based shoulder-surfing attacks over multiple authentication sessions. However, its application remains limited to PIN-based authentication.

2.1 Generation of OTP

We are using android-based mobile phone for the generation of OTP, where the user has to enter the predefined attribute values such as user id, date of birth and ATM PIN number. Mobile's IMSI number and current date and time are automatically retrieved through the inbuilt function of application. By using this parameter, an OTP is generated. Time is one the major factor in this process where it gets changed on regular basis.

We are using SHA1 algorithm to generate the one-time password. SHA1 is basically a secure hash algorithm that works with character input less than 2^64 bits in length. Output generated by SHA1 algorithm has 160 bits in character length. It is more secure than MD5 algorithm. It gives a fixed length of output. In this system, we get 20 bytes of string, i.e. 160 bits. 20 bytes yield 40 characters. It is very onerous task to enter these 40 characters. Therefore, we divide these 20 bytes into four chunks each of five bytes and perform XOR operation on each chunk, which gives us output of five bytes, i.e. ten characters. These ten characters form the final secrete in

generating a password code called the one time password (OTP).

Session key system means that a session key may be derived from a hash value, using the CryptDeriveKey function. This method is called a session-key derivation scheme. Throughout each session, the alternate symbol is placed along with each number. Because much of the security relies upon the brevity of their use in each session, session keys are changed frequently. A different session key can be used for each session.

Figure shows the alternate symbol for corresponding to each number. The user can enter their PIN via symbol instead of using entry of numbers.

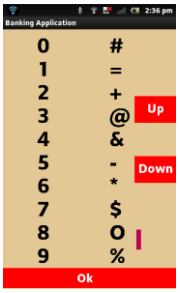

Figure 2.1: Numbers & Corresponding Symbol in Standard PIN

The SteganoPIN system builds on the concept of challenge-response rendered over a user interface [13] and physical hand protection [14] to help achieve the following goals for PIN-based authentication.

(1) User-friendliness.

(2) Strong security: The security of our method is reliable since it is based relied on such a physical hand protection process.

(3) Integration of ATM and android mobile phone for practical enforcement of PIN entry security system.

(4) A versatile, challenge keypad, rendering a randomised challenge for OTP derivation. Once sensing the four sensors in or around the direction, the keys will automatically be rearranged.

Example: The location of PIN 2645 in regular layout can map and derive OTP 7491 on the challenge keypad. Response keypad receives the OTP input, e.g. 7491 as shown by colored numeric indicators in the regular layout. Comparison between performances of standard keypad and after incorporating a challenge keypad.

Figure 2.1.1: Challenge keypad

2.2 SteganoPIN Method

The PIN space of SteganoPIN is 10^4 for a four-digit PIN chosen from the ten-digit alphabet set. With a guess attack, the success probability is $m/10^4$ for m attempts and $1/10^4 - m + 1$ for the m^{th} attempt of guessing, since $1 \leq m \leq 10\,4$. This result is the challenge keypad and the response keypad render a one-to-one mapping in every authentication session [16].

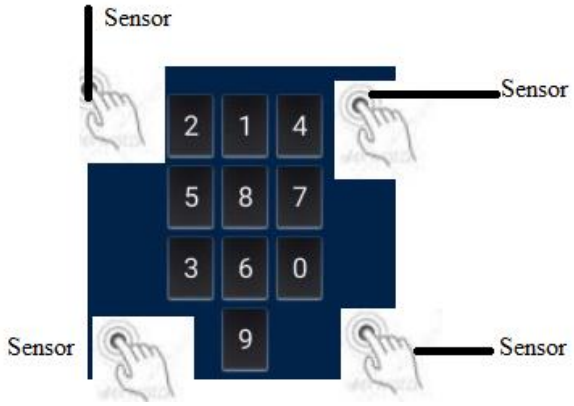

Figure 2.2: Keypad with sensor

We developed a prototype system of SteganoPIN to create a ATM interface with a smart phone to sense both proximity and touch events on the challenge keypad and a tablet to implement the response-key pad performance then reads the challenge keypad. If the user forgets part of the OTP or the PIN length is greater than four digits, the user could repeat the procedure with another random challenge. Furthermore, hand operation using is flexible; for instance, a single hand for both OTP derivation and entry or both hands for OTP derivation work equally well. In practice, it is desirable to implement the circular touch area on both sides for right-handed and left-handed users.

2.3 Algorithm

Step1: Registered users only shall be able to access the ATM application by their unique PIN in mobile phones.

Step 2: Enter the PIN which may be applied to any case with N ≥ 2 digits. We need a total of four rounds.

Step 2.1: The first round is the session-key decision round, which is used for displaying ten randomly arranged objects to the user; the user then recognizes the symbol immediately below the first digit of his/her PIN as the temporary session key and presses "OK."

Step 2.2: 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. In each of these rounds, the user is again provided with a random array of ten objects, and he/she enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit.

Step 3: SteganoPIN simulates a horizontal ATM with a Smartphone and a tablet for OTP derivation.

Step 4: Once the user-entered pattern is manipulated and a PIN is identified, then the user can avail ATM services like cash withdrawal, deposit and fund transfer, which can be done securely using the concept of virtual money.

DOI: 10.18535/ijecs/v5i10.62

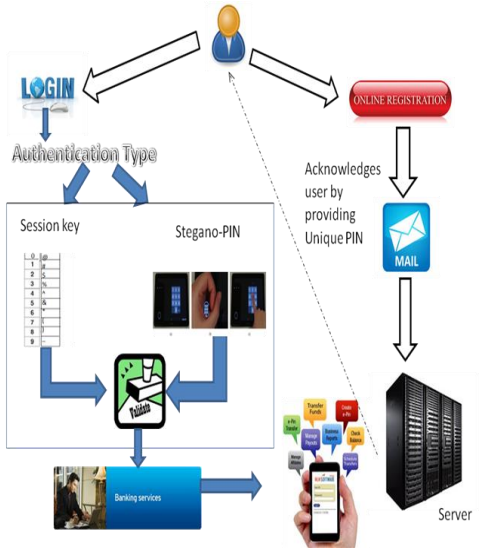

Figure 2.3: Architecture Diagram

2.4 Enhanced Methods in Proposed System

Implementation stage is the major challenging part of this project when the virtual design is modelled into a working system. Thus, it can be considered to be the significant by most-important stage in achieving a novel system and providing giving the user, with the assurance of the security operating the new system that will work efficiently and be useful. The implementation stage involves careful planning, study of the existing system and its restriction on implementation and designing of methods.

- User registration
- Session-key management
- SteganoPIN authentication
- Banking and related services

2.4.1 User Registration

After the user registration is done, the user is entitled to access the ATM application through their mobile phones. Once the user registration is completed, user gets a unique PIN via to their respective e-mail ID. Once the unique PIN is validated, a user can access the required application by entering the username and password.

2.4.2 Session-Key Method

It is a novel PIN-entry method. The basic layout of our method comprises a vertical array of digits from 0 to 9, juxtaposed with another array of ten operators, such as + and /, etc. For the operational ease, we feel that the maximum number of digits in a PIN is four, although the proposed method may be applied to any case with N ≥ 2 digits. We need a total of four rounds.

The initial round is the session-key decision round, and the remaining three rounds are PIN-entry rounds. In the session-key decision round, ten randomly arranged objects are displayed to the user. The user recognizes the symbol directly 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 symbols provided in the session key because it is collocated with the first digit of the PIN, 2.

The remaining rounds are the PIN-entry rounds, in which the ith digit of the PIN is entered in the i^{th} round for i = 2, 3, 4. In each of these rounds, the user is again given a random array of ten operators such as arithmetic and special operators, and s/he enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit. For this operation, the user can use "left and right" Buttons. In this example, the user presses the "right" button twice so that symbols move to the position immediately below 3, and then presses, "OK."

2.4.2.1 SteganoPIN System

A prototype system of SteganoPIN is developed to simulate a horizontal ATM interface with a smart phone (to sense both proximity and touch events on the challenge keypad) and a tablet (to implement the response keypad), for OTP derivation. The challenge keypad does not appear immediately. Only the response keypad appears in its regular layout and size. It shows the challenge keypad only when a user cups a hand on the circle with the grip circularly closed to form a ρ-shape. The challenge keypad then shows up after a small time-lag and disappears immediately when the user releases the cupped hand.

The user interface of SteganoPIN consists of one numeric keypad that is a standard keypad in regular layout and the other is a small independent keypad arranged in a random layout. The random layout keypad is called the challenge keypad because it permutes ten numeric keys as a random challenge. A user must use this challenge keypad to derive a fresh OTP for each session. The user first locates a long-term PIN in regular layout and subsequently maps the key locations onto the challenge keypad for OTP derivation. The user then enters the OTP on a regular layout keypad called the response keypad. The procedure can be repeated over the PIN length.

2.4.2.2Authentication and Services

Once the user-entered pattern is manipulated and a PIN is identified, it will be checked with the local database provided by Android OS using SQL lite. This process is designed to prevent unnecessary server-end process handling playful requests. A one-way hash key is generated for the validated PIN and is sent to the server in public channel so that an active attacker cannot hack the PIN by monitoring the channel. Once a authenticated by the server a quick response to the mobile app will forward the user to the services. The ATM services can be performed in a secure environment by web. This reduces the overhead complexities in the server and will provide the user with an ease of access.

3. Result & Implementation Details

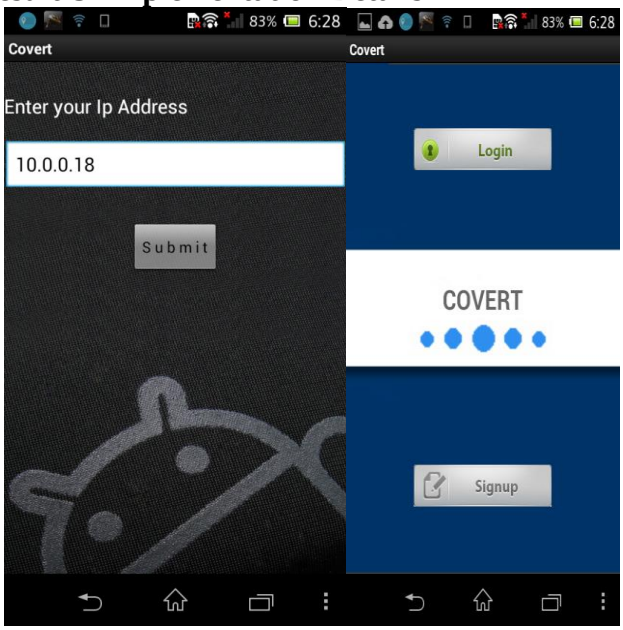

Figure.3.1: Enter IP Address and SignUp

DOI: 10.18535/ijecs/v5i10.62

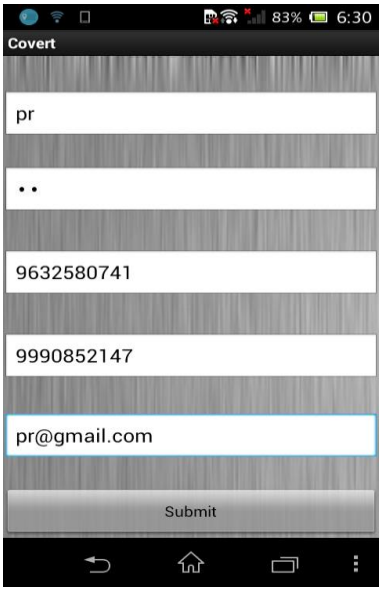

Figure.3.2:.Enter details

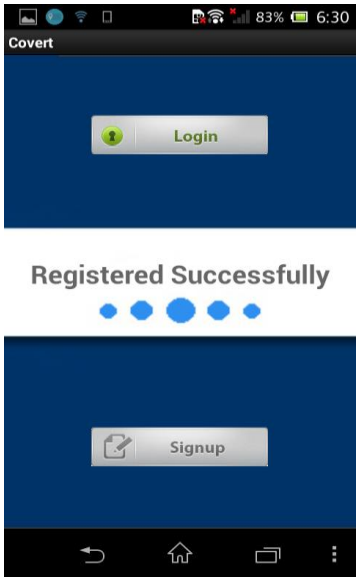

Figure.3.3: User Registered

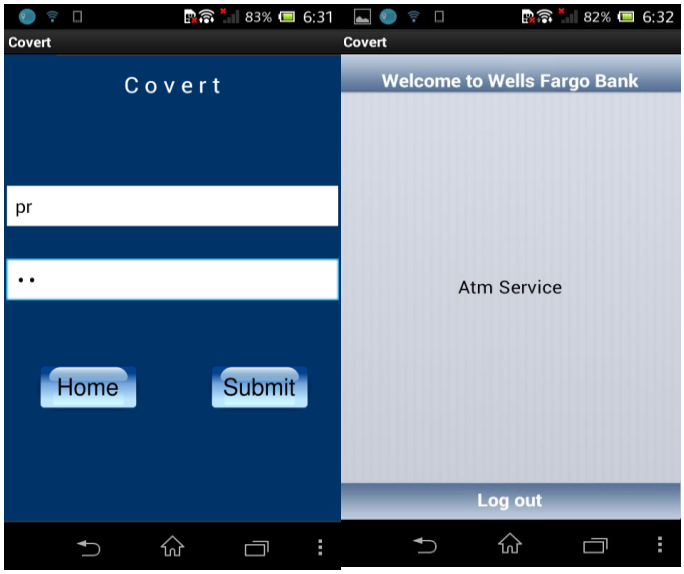

Figure.3.4:. Login and Bank Page

Figure.3.5: Session Key

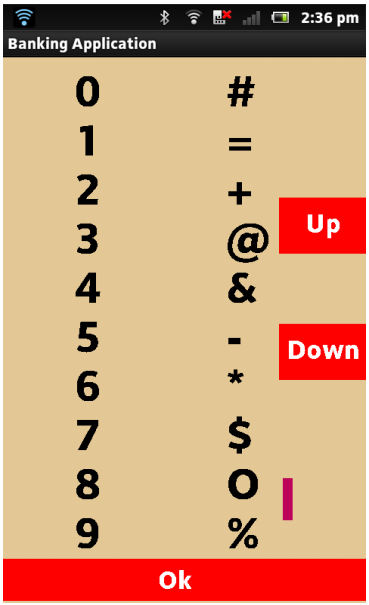

Figure.3.6:. Enter password

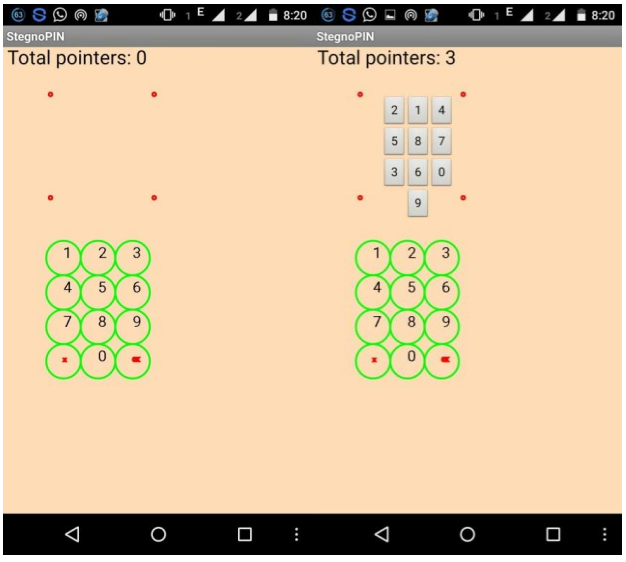

Figure.3.7:. SteganoPIN

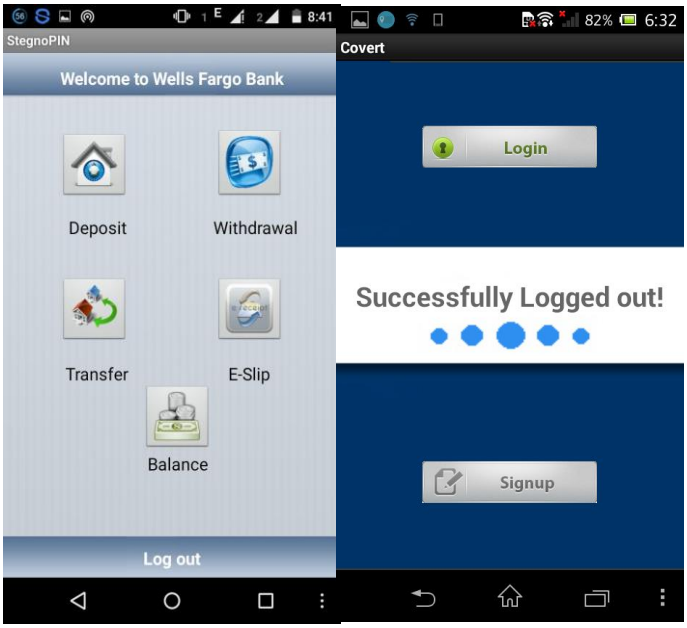

Figure.3.8:. Banking Page and Logout

4. Conclusion and Future Work

The main objective of this project was to implement a multi-touch concept and a voucher code and to provide enhancement through the session key method. SteganoPIN was demonstrated to be secure against camera-based shoulder-surfing and guessing attacks. Specifically, SteganoPIN has proven to be secure against camera-based shoulder-surfing attacks over multiple authentication sessions if a user properly used the system. SteganoPIN was also shown to be user-friendly based on its faster PIN entry time and lower error rates than other advanced-security PIN entry systems. The future work can extend this process for other bank-account transactions and to achieve further reduction in the time consumption.

Acknowledgments: The authors wish to express their thanks to M.E. Santhanagopalan who helped to language edit the contents of this manuscript which resulted in the improvement of the presentation.

References

[1] T.Kwon,S.Shin,andS.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.

[2] Ming Lei, Yang Xiao, Susan V. Vrbsky, Chung-Chih Li*, and Li Liu" A Virtual Password Scheme to Protect Passwords "DOI: 10.1109/ICC.2008.297 Conference: Communications, 2008. ICC '08. IEEE".

[3] Arash Habibi Lashkari , Dr. OMar Bin Zakaria, Samaneh Farmand, DR. Rosli Saleh" Shoulder Surfing attack in graphical password Authentication" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 2, 2009

[4] Ms.K.Devika Rani Dhivya, S.Pavithra" Review On Color Password To Resist Shoulder Surfing Attack" International Journal of Computer Science and Mobile Computing, Vol.4 Issue.10, October-2015, pg. 20-26

[5] Peipei Shi, Bo Zhu and Amr Youssef "A Rotary PIN Entry Scheme Resilient to Shoulder-Surfing" Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc

[6] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider" A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication" World Applied Sciences Journal 19 (4): 439-444, 2012 ISSN 1818-4952;© IDOSI Publications, 2012 DOI: 10.5829/idosi.wasj.2012.19.04.1837

[7] Alexander De Luca, Bernhard Frauendienst, Sebastian Boring, Heinrich Hussmann "My Phone is my Keypad: Privacy-Enhanced PIN-Entry on Public Terminals" OZCHI 2009, November 23-27, 2009, Melbourne, Australia.

[8] M.R.Divya, A.P.Janani "Defending Shoulder Surfing Attacks in Secure Transactions Using Session Key Method"International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Special Issue 6, May2015

[9] Kavitha V, Dr.G.Umarani Srikanth "An Android Application For ATM With A Secured Pin-Entry Methods" International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 7 No.4 Apr 2015

[10] M Sreelatha , M Shashi , M Anirudh , Md Sultan Ahamer , V Manoj Kumar "Authentication Schemes for Session Passwords using Color and Images International Journal of Network Security & Its App lications (IJNSA), Vol.3, No.3, May 2011 DOI : 10.5121/ijnsa.2011.3308

[11] Abdullah Ali, Ravi Kuber and Adam J. Aviv "Developing and Evaluating a Gestural and Tactile Mobile Interface to Support User Authentication " iConference 2016

[12] Yoshihiro Kita, Fumio Sugai, MiRang Park,Naonobu Okazaki" Proposal and its Evaluation of a Shoulder-Surfing Attack Resistant Authentication Method:Secret Tap with Double Shift" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(1): 48-55/

[13] Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing esistant graphical password scheme," in Proc. ACM Int. Working Conf. Adv. Visual Interfaces , 2006, pp. 177–184.

[14] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. W. Nicholson, J. Nicholson,and P. Olivier, "Multi-touch authentication on tabletops," in Proc. ACM SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1093–110

[15] Taekyoung Kwon and Sarang Na "SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security "IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 46, NO. 1, FEBRUARY 2016

[16] Teddy Seyed, Xing-Dong Yang, Anthony Tang,, Saul Greenberg,Jiawei Gu, Bin Zhu, and Xiang Cao "CipherCard: A Token-based Approach against Camera-based Shoulder Surfing Attacks on Common Touch screen Devices "In Proceedings of the 15th IFIP TC.13 International Conference on Human-Computer Interaction - Interact'2015. (Bamberg, Germany), Springer, 18 pages, September 14-18.

Author Profile

Ms.K.Kiruthika received the B.Tech (IT) degree in Engineering and M.Tech (IT) with distinction in Engineering in 2011 from Sathyabama University, Chennai having an experience of 10 years. Currently working as an Assistant Professor/Computer science and engineering in Panimalar Engineering College Chennai. Her area of interest includes Data Base, Data Structure, and Operating system, Compiler Design and Computer Graphics.

Ms. D. Jennifer is currently working as Assistant Professor in the Department of Computer science & Engineering in Panimalar Engineering College, Chennai having an experience of 7.5 years. This college has been affiliated to Anna University, Tamil Nadu, and India. B.E with department first rank and M.E Degree is awarded to her by the St Peter's

University during December 2012. Area of interest includes Data Mining, Theoretical Computer Science, Digital Signal Processing.

Ms.K.Sangeetha completed B.E with department first rank and M.E (CCE) degree in Engineering in 2012. Currently working as an Assistant Professor/Computer science and engineering in Panimalar Engineering College, Chennai having an experience of 3 years. Area of interest includes Data Mining, Software Engineering, and Cryptography and network security.

Ms.Jackulin.C is a Member of **ISTE** from 2009 , Member Id number is LM-64803. She completed B.Tech Information Technology (2008) and M.E Computer Science and Engineering (2013) in Anna University Chennai, Tamilnadu , India. Currently working as an Assistant Professor, Computer Science and Engineering Department, Panimalar Engineering College, Chennai and having total experience of 6.5 years. Her research interests are in the area of Networks, Analysis of Algorithm, Data Structures, and Compiler Design.

Ms.R.Shalini completed M.Tech Computer Science and Engineering (2012) in Sathyabama University Chennai, Tamilnadu , India. Currently working as an Assistant Professor, Computer Science and Engineering Department, Panimalar Engineering College, Chennai and having total experience of 8 years. Her research interests are in the area of Microprocessor, Analysis of Algorithm, Data Structures and Computer Graphics.