



Protection of Confidentiality in Banking Systems

Priyadarshini Bhattacharyya¹, G.K Rajeshwari², Professor Igni Sabasti Prabu³

Department of Information Technology, Sathyabama University, Chennai, India^{1,2}

Professor, Department of Information Technology, Sathyabama University, Chennai, India³

ABSTRACT: PINs or Personal identification numbers are susceptible to shoulder surfing attacks in crowded places and they can be easily traced by various photographic recording tools and equipments like cameras or body cameras. In order to enhance the security of the banking system there is an existing technology called SteganoPIN which enforces pin security[1]. SteganoPIN method includes 2 keypads out of which , one is randomly generated and the other one is a regular keypad. OTPs can be derived by mapping the key locations in a regular keypad into randomly shuffled keypad[1]. The scope of our project is to present a method called ‘Symbol Identifier’ which has comparatively better usage in terms of efficiency. In this method, we use randomly shuffled symbols so that no PIN numbers have to be entered by the users manually. A temporary symbol is selected based on the first digit of the user’s PIN and then this symbol is then used to match the successive numbers of the PIN in order to establish a secured transaction. This application is specially designed for Android Users for Secured PIN Authentication in ATM system.

KEYWORDS: Personal Identification number , PIN ,security, Authentication , ATM , security , ColorPIN , SteganoPin , Human Identification Protocol ,attacker, leakage resilient password system ,password, transaction , mechanism , Symbol Identifier , BinaryPIN.

I.INTRODUCTION

PINs or Personal Identification Numbers, used in various authentication systems have to be remembered by the users. It is extensively based on numeric passwords or encrypted keywords for authenticating the users or for various deciphering purposes. The operation of the PIN numbers is rapidly growing due to the modernized touch screens that helps in the simpler application of the PIN entry methods .This can be applied on various devices like ATMs or Automated Teller machines, different transactional cards, smart phones.

Nowadays, the verification process at ATMs i.e. whether the user is authorized to use the system or not is completely dependent on the PIN number that they enter. The safeness of the ATM authentication gets easily compromised. Hence the users have to be highly conscious while entering their PINs and passwords. Analysis of the various attacks that have taken place in the banking systems have led to the leakage of its confidentiality. This is mainly due to eavesdropping by various attackers and frauds . The difficulty that the users face is that, this system lacks security in it . The eavesdropper or the attacker standing behind can observe the PIN that is being entered by the authenticating person. This leads to shoulder surfing attacks. The assailant may also use body cameras or install recording devices in areas of the ATM terminals to note and store the PIN entries[12]. Typing the passwords or PINs in an indirect method can be used to solve such problems. One such indirect phenomenon has been illustrated by the researchers. This method is called as ‘SteganoPIN’ entry method’ for secure pin authentication system for banking systems using Smart Phones[1].This method is a quite complicated and time consuming method for the users. Also by using camera based equipments from different angles the security of the PINs can be lost.

We propose an improved methodology in order to protect the security of the PIN-entry method using ‘Symbol Identifier Method’. In this method we use randomly generated shuffled symbols so instead of entering PIN numbers the users have to select the symbols corresponding to each digit of their PIN and press ok for each round .The process includes the selection of a temporary symbol in the beginning based on the first digit of the user’s PIN and then this symbol is matched with the consecutive digits of the PIN in order to provide highly secured banking systems. We present that this scheme would be really error free to a greater extent.



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

II. RELATED WORK

The Corroboration in ATM is generally dependent on PIN numbers. The primitive security complication that user faces is that the security of the PIN entered by the users is highly compromised[2]. Users have to strongly make sure that they protect their PIN numbers. The trigger people could be found peeping and watching the PIN that is being entered by the user in the ATM queues. The shoulder-surfing attackers and eavesdroppers may replicate the PIN or passwords and then misuse the PIN[12]. The assailant might also fix up a tiny camcorder on any corner of the ATM center to trace the entries of the client.

Hence, there exists a new arrangement structure which deals with a different PIN entry process known as SteganoPIN which enforces the pin security. SteganoPIN which is composed of two arithmetic keypads, one shielded and the other unclosed, out of which one is randomly generated and the other one is a regular keypad. OTPs can be derived by mapping the key locations in a regular keypad into randomly shuffled keypad. It is designed to physically block shoulder surfing attacks[1].

The major deficiency faced in this technique is that in the process of generating OTP it holds a particular pose or position for guarding purposes. The people who are unable to use the keypad using such positions might experience complication in the procedure. The housing or shielding the keypad is limited to deal with the attackers on the opposite side because of its exposed angle. The upward camera remains a burden, depending on a user posture. The time taken for mapping the digits in the randomized keypad is quite long. The Polaroids found at an angle above the area of the circular touch of the keypad can record the PIN easily and hence the security of the system is bound to get leaked. Duplication of the card can be done once the PIN number is recorded using various attacks. Skimming and cloning devices may be used which may lead to PIN insecurity. The SteganoPIN setup is found to be suitable to immobile setup such as ATMs.

Other previous researches showed the usage of ColorPIN. This method basically comprised of binary colors using a technique called BinaryPIN for entering the password[4]. Usage of ColorPIN is significantly slower since each digit of the PIN has to be authenticated 4 times. Also it becomes inflexible for the users to recall the PINs and also the colors along with it.

We propose a method called 'Symbol Identifier' which is decidedly superguarded and serviceable than the past inventions. In this method, we use randomly shuffled symbols so that no PIN numbers have to be entered by the users manually. A temporary symbol is selected based on the first digit of the user's PIN and then this symbol is used to match the successive numbers of the PIN to establish a secured transaction. This application is specially designed for Android Users for Secured PIN Authentication in ATM. In this method usage of numbers or digits has been replaced with 'Symbols' which is very user-friendly. It takes lesser amount of time compared to the previous techniques and is more accurate. It is simple, robust and less complex.

III. PROPOSED SYSTEM

We propose a system which is known as 'Symbol Identifier Method' which is notably more secure and accessible than the previous proposal. In this method, we use advanced tools to check out the resistance of a personal identification number entry method. At first we build a theoretical groundwork to correctly interpret and guesstimate the safeness. Later, various preliminary methods are conferred to assist the substructure. We further prove with a model stating that this Pin entry scheme is extremely safer and a lot more secure.

'Symbol Identifier Method' is the latest configuration where, we use randomly shuffled set of symbols so that no PIN numbers have to be entered by the users manually. A temporary symbol is selected based on the first digit of the user's PIN and then this symbol is used to match the successive numbers of the PIN to establish a secured transaction.

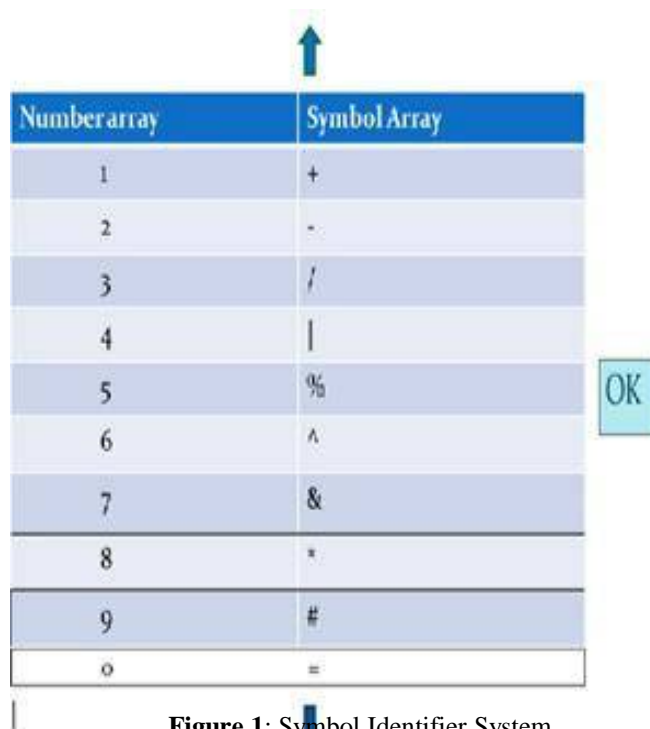
The design of this layout holds various numerical digits and symbols aligned in a vertical manner with two buttons for scrolling purposes. For instance, an ATM PIN number is embraced with four digits. The symbol identification framework is applicative if N is greater than or equal to two digits. It comprises of four different cycles. First is the

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

symbol identifier determination round and the rest of the cycles include the entering of the PIN numbers. During the symbol identifier determination i.e the first round , ten different set of symbols are laid out to the user in accordance to the ten digits ranging from 0 to 9 respectively. Initially, the user selects any one of the symbols that are laid out and position it to the first digit of the user’s password PIN and designates it as a temporary symbol identifier.



Number array	Symbol Array
1	+
2	-
3	/
4	
5	%
6	^
7	&
8	*
9	#
0	=

↑
OK

Figure 1: Symbol Identifier System

To illustrate this, let us suppose that the PIN is 5678 ,the user identifies the symbol “%” as the symbol identifier as it is positioned right beside the first digit of the PIN i.e 5.The rest of the cycles are the entering of PIN numbers where the ith digit is entered in the ith cycle i.e in our example the symbol “%” is aligned with the successive digits of the PIN and after each entry ‘OK’ button is pressed.

So, in all of these cycles, the user is provided with a random collection of ten symbols in an array, and enters the digits of the PIN one after the other by positioning the slot consisting of various symbols. To enable to do so, the application is provided with two extra buttons for traversing throughout the array in an up-down fashion. Similarly, this step is carried for all four cycles and if it is validated, the user successfully performs the banking transactions.

Therefore, this method is superior and is less complicated to use than the previous proposed systems on PIN entry systems and produces more accurate results in shorter duration.

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

IV. ARCHITECTURE

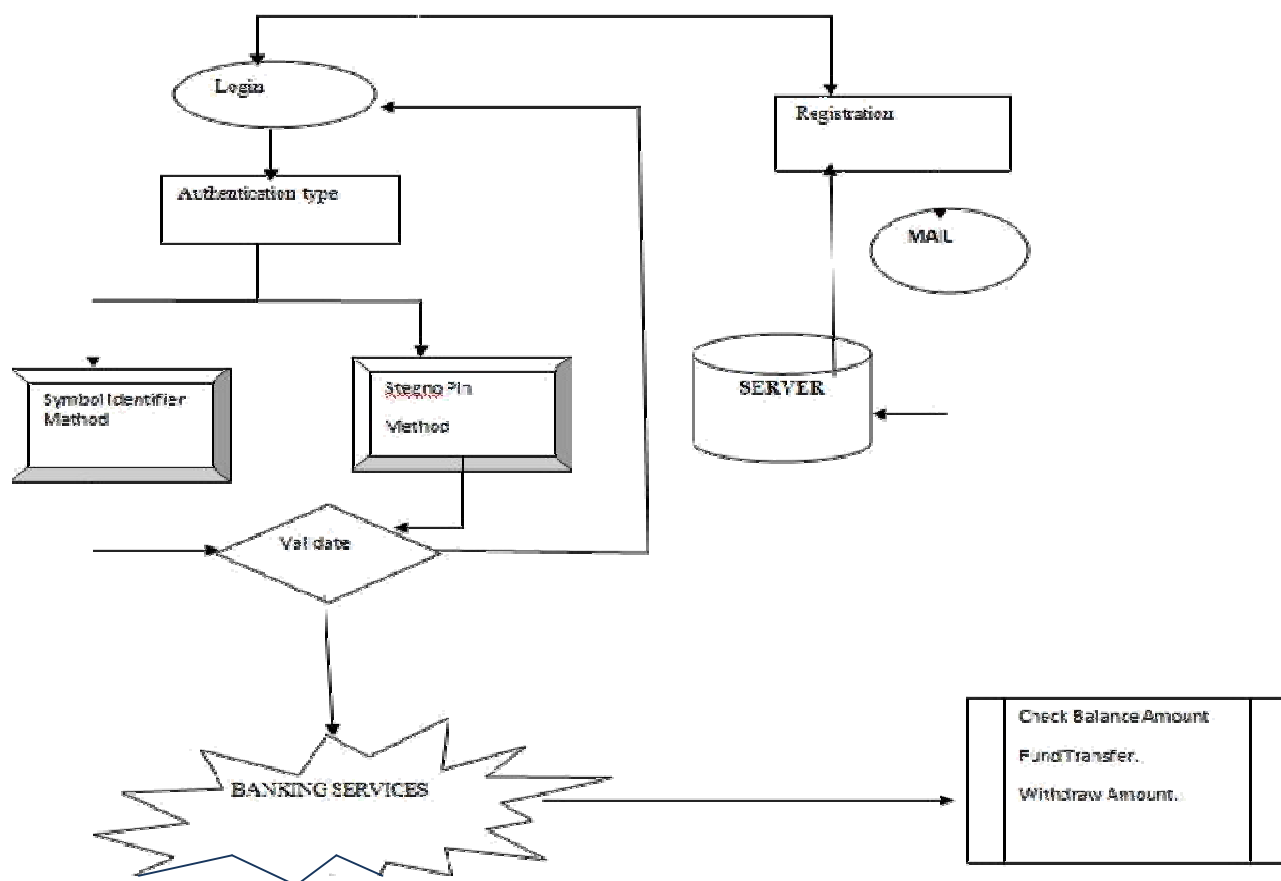


Fig 2. Architecture of banking systems

V. EXPERIMENTAL ANALYSIS

To enter PIN numbers in smart-phones, tablet, and other accessories in public areas is highly insecure. Many cameras, polaroids and other recording gadgets are often found in banking systems which may lead to leakage of confidential information like authentication PIN codes[3].

To elude the ATM deceptions, awareness must be created among the people who use ATM. The main aim of the attacker is the account number and the PIN. This information or the data is gathered during the transaction process performed by the user in the ATM. But, the user is unaware of such things[5].

The shoulder surfing attack and the recording attack are very common in ATMs. To prevent such attacks, the new pin entry method 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 mobile phones or the smart phones containing the android operating system. This application must contain all the possible choices which are existing in an ATM.

The existing SteganoPIN entry system uses proximity sensors, a randomly generated keypad and a regular keypad. The regular keypad is always shown to the user whereas the randomly generated keypad is shown to the user only when he/she uses the cupped hand position and keeps his/her fingers on any of the three points out of the four points. Once the user does that the randomized keypad gets generated. The user starts mapping the actual PIN number locations from the regular keypad into the randomized one. In this way the OTP gets generated. This OTP is then entered by the user on the regular or normal keypad. Hence, the users enter the OTP instead of the actual PIN in this process which keeps the antagonists and other attackers perplexed and confused. In this system

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

,each and every time a new set of random numbers is generated and the mapping procedure is carried out which ensures PIN entry to be quite secured[1].

There are few drawbacks under the existing scenario such as entering in the randomly generated keypad and remembering the digits , hence we go for a further new implementation method called “Symbol Identifier” mechanism. The initial cycle is the symbol identification decision round and the rest of the cycle deals with PIN entry. At first few random symbols are initially shown to the user . If we analyse a bit deeper into this, the user exclusively selects a symbol and aligns it beside the very first digit of the ATM PIN. Now, all the symbols get shuffled in a randomized manner. Next , the user aligns the selected object or symbol to the next digit of the PIN by using the up and down buttons and finally presses the “OK” button . If the user enters the PIN number correctly, he is allowed to perform the banking transactions further.

This mechanism is very good when compared to the complicated existing method and would be able to fetch better results than the previous one.

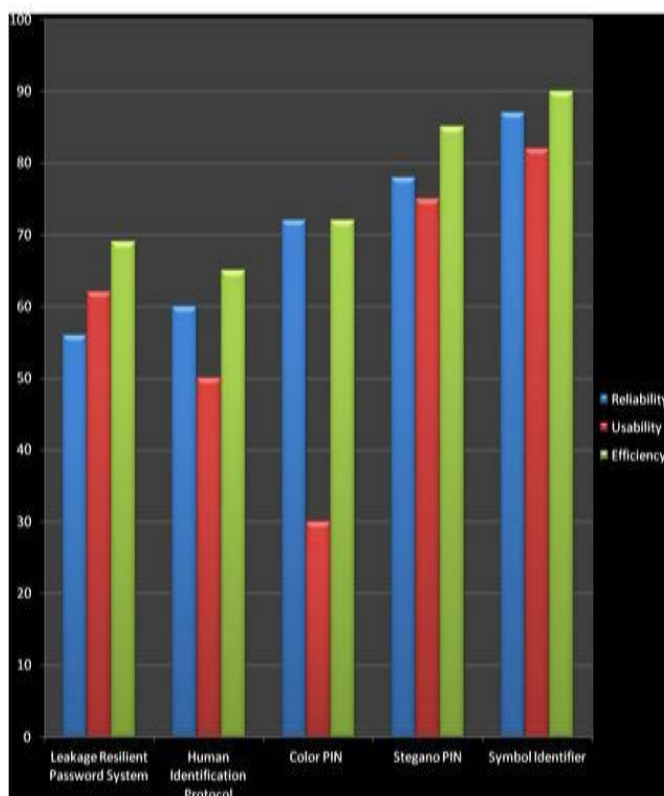


Figure 3: Graphical Representation of the Existing papers and the Proposed paper based on Reliability, Usability, Efficiency factors.

VI . CONCLUSION AND FUTURE WORKS

In this project, a secure PIN authentication protocol for ATM transactions has been used. A user can access the ATM services more securely using their personal android mobile devices. The security of the entire ATM systems is enhanced. In our proposed systems we use multi-touch keypads in mobile applications.

This system avoids the usage of numbers , is simpler and is more robust than the previously proposed systems for indirect PIN authentication. Compared to other systems it produces more accurate and time-bound results.

The future system would be kit based so that it is enhanced by single touch for authentication.



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 6, Special Issue 3, November 2017

REFERENCES

- 1.StegnoPIN : Two - Faced Human - Machine Interface for Practical Enforcement of PIN Entry Security(Android).-by Taekyoung Kwon and Sarang Na, IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 46, NO. 1, FEBRUARY 2016 ,USA.
- 2.On limitations of designing leakage-resilient password systems: Attacks, principles and usability,"- Q. Yan, J.Han, Y. Li, and R. H. Deng in Proc. 19th Internet Soc. Netw. Distrib. Syst. Security Symp., 2012, pp. 1–16.
- 3.Cryptanalysis of the Convex Hull Click Human Identification Protocol-Hassan Jameel Asghar, Shujun Li,Josef Pieprzyk, and Huaxiong Wang ,May 2010.
- 4.ColorPIN – Securing PIN Entry through Indirect Input -Alexander De Luca, Katja Hertzschuch, Heinrich Hussmann, CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
- 5.Kwon, Taekyoung, and Sarang Na. "SteganoPIN: Two-Faced Human–Machine Interface for Practical Enforcement of PIN Entry Security" , IEEE Transactions on Human-Machine Systems, 2015.
- 6.Lee, Mun-Kyu. "Security Notions and Advanced Method for Human ShoulderSurfing ResistantPIN-Entry" , IEEE Transactions on Information Forensics and Security, 2014.
7. Neenu N A, . "On screen randomized blank keyboard" , 2015 National Conference on Recent Advances in Electronics & Computer Engineering (RAECE), 2015.
- 8.Chang Soon Kim. "Secure and user friendly PIN entry method" , 2010 Digest of Technical Papers International Conference on Consumer Electronics (ICCE), 01/2010.
- 9.De Luca, Alexander, Katja Hertzschuch, and Heinrich Hussmann. "ColorPIN : securing PIN entry through indirect input" , Proceedings of the 28th international conference on Human factors in computing systems - CHI 10 CHI 10, 2010.
- 10.Khan, Rasib, Ragib Hasan, and Jinfang Xu. "SEPIA: Secure- PIN-Authentication-as-aService for ATM Using Mobile and Wearable Devices" , 2015 3rd IEEE International Conference on Mobile Cloud Computing Services and Engineering, 2015.
- 11.Kwon, Taekyoung, Sooyeon Shin, and Sarang Na. "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected" , IEEE Transactions on Systems Man and Cybernetics Systems, 2014.
- 12.Hindusree, M., and R. Sasikumar. "Preventing shoulder surfing in secure transactions" , 2015 International Conference on Computing and Communications Technologies (ICCT), 2015.