*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 58-65*
*www.iosrjournals.org*

# Moving ATM Applications to Smartphones with a Secured Pin-Entry Methods

Kavitha V[1], Dr. G. Umarani Srikanth[2]
[1,2,] *(Department of PG studies, S.A. Engineering College, India)*

***Abstract:*** *A personal identification number (pin) is a widely used numeric password. The 4-digit pin numeric password is being used as authentication in many important applications such as, an ATM. An ATM is a place where the shoulder surfing attack is of great concern. There are some existing methods that provide security to the pin entry. But, those methods use only limited cognitive capabilities of the human adversary. The major disadvantage that exists here is that human adversaries can be more effective at eavesdropping and assumptions by training themselves. The proposed method called improved black white (BW) method can be more secure, as it uses bi-colored keys. Another contribution is the authentication service that uses local databases and a hash function. The hash function is mainly used to send the pin securely to the server through the public channel. An ATM application is created as an android application, where transactions can be performed in smart phones using a virtual money concept.*

***Keywords:*** *personal identification number; improved black white (BW) method; virtual money; hash function; shoulder surfing attack.*

## I. Introduction

When a personal identification number (PIN) is entered by the user in ATM and point of sale (PoS) terminals or any stationary systems including smart phones there is a higher possibility, where a PIN may be attacked by various attacks such as shoulder surfing attack or recording attack. Shoulder surfing is a direct observation based attack and the recording attack is a device based attack where devices such as cameras may be used to record the secret information. A PIN can be authenticated by various settings with different devices including mobile phones and PDA. The PIN entry can be observed by human or device attackers, more effectively in a crowded place. When the user uses a same pin repeatedly for various purposes, there may be a great risk.

To overcome this problem between the user and the system, cryptographic prevention techniques are hardly applicable because human users are limited in their capacity to process information. Instead, there have been alternative approaches considering the asymmetry between the user and the system. Among them, the PIN entry method presented by Roth et al [1] was elegant because of its simplicity and intuitiveness: in each round, a regular numeric keypad is colored at random, half of the keys in one color (black) and the other half in another color (white), which is the BW method.

A user who is the owner knows the correct PIN digit can answer its color by pressing the separate color key below. The basic BW method is aimed to resist a human shoulder surfing attack [1] and uses the perceptual grouping concept but not supported by a recording device attack. The BW method is still considered to be secure against human adversaries due to the limited cognitive capabilities of humans.

The improved BW method is implemented as an advanced method to the basic BW method [2]. To provide security to the PIN entry methods from shoulder surfing attack and recording attack, particularly in the ATM machines, the entire ATM application moved to the smart phones [3]. This can be possible only when the virtual money concept is on practice.

The virtual money is commonly termed as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community". When this concept is implemented the ATM transactions can be performed using the smart phones, where the transactions are made with the virtual money.

## II. Attacks On Pin Entry

### 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 that the distributions of PINs and passwords are not uniform. However, to simplify analysis, we make an idealized assumption that the distribution of PINs is uniform. We also have to take into account that the user (and the attacker) may be allowed to fail several times until s/he inputs the correct PIN. For example, a typical ATM permits three trials. Therefore, we give the following definition for the security of a PIN-entry method against a guessing attack.

### 2. Shoulder Surfing Attack (SSA)

In a shoulder-surfing attack (SSA), the attacker observes the logon procedure by looking over the user's shoulder, and tries to recover that user's PIN. This SSA is most familiar in many of the common places. One best example is shoulder surfing attack during PIN entry at ATMs. The SSA 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.

### 3. Human Shoulder Surfing Attack(HSSA)

The HSSA is one of the types of SSA. A shoulder- surfing attack without any recording device or an electronic device is commonly known as a human shoulder-surfing attack (HSSA) [1].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. In these recent years, the human adversaries had become more powerful to recollect the PIN that was shoulder surfed.

### 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 the remote system. Such type of attacks is of great concern at ATM.

## III. 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 complete security to the PIN entry. But, these methods did not provide the complete security. Some of such existing methods are discussed below.

### 1. Immediate Oracle Choices

Let A be the alphabet of PIN digits. The algorithm of the immediate oracle choice variant starts with a set $Q \leftarrow \mathcal{A}$of probable PIN digits, and executes $n = \lceil \log_2 |\mathcal{A}| \rceil$ rounds. Typically, the alphabet consists of the digits from 0 to 9 and a PIN has l = 4 digits; hence $|\mathcal{A}| = 10$and n = 4. In each round, the algorithm randomly partitions the set of $q = |Q|$remaining probable PIN digits into two sets L and R of sizes $\lceil q/2 \rceil$ and$\lceil q/2 \rceil$. Here, we assume that the PIN pad allows us to change the colour of keys. A round concludes when the oracle chooses one of the sets by pressing a separate black or white button.

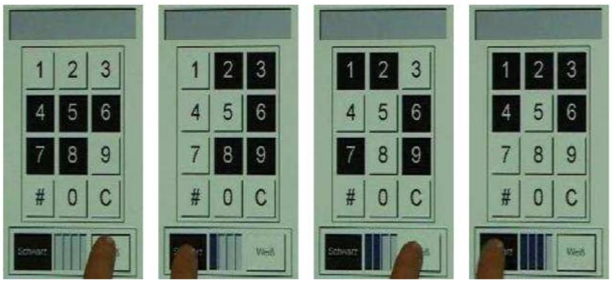


**Figure 1:** The above sequence illustrates the immediate oracle choice variant. The oracle is presented two partitions coloured black and white, and must input in which partition the current PIN digit is. In the example above, the oracle enters the PIN digit '3'.

### 2. Delayed Oracle Choices

If the oracle responds slowly then the partitions are exposed longer to the observer. The longer the exposure is the easier is it for the observer to memorize or manually record a partition (which also uniquely identifies the second partition). As a remedy, we devised another approach which we call "delayed oracle choices." In that 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 colouring that his PIN digit had in these n rounds. Rather than requiring the oracle to input its choice immediately, we delay the input until after exposure of all rounds. On the other hand, the oracle has only a limited period of time to determine the colour of the current PIN digit in each round, and he must memorize the colour sequence. Again, this procedure is repeated until all PIN digits are entered. The delayed oracle choice variant requires that a set of n pairs of random partitions are precompiled such that an input pattern occurs at most once. Otherwise, the input of a PIN digit would be ambiguous.

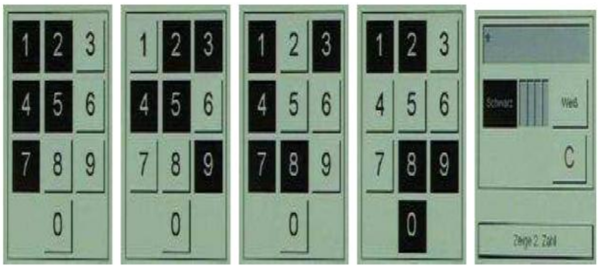


**Figure 2:** The above sequence illustrates the delayed oracle choice variant. Subsequent to the display of the four patterns on the left, the panel to the right appears. The oracle then has to enter the colour sequence of the current PIN digit.

## 3. The basic BW method

The basic BW method partitions a set of ten digits into two random halves, of which one is selected according to the user's key entry in each round. If the selected halves were memorized or written on a paper for m, consecutive rounds and recalled to derive their Grouping Patterns [9], the shoulder surfer could identify a single digit of the PIN.

The grouping pattern is a method of dividing the set of digits 0-9 into two halves, one half with black keys and other with white keys. The user need press the PIN number key directly, instead press the black or white button given below, corresponding to the user PIN. This may take about 16 rounds to completely enter the 4-digit PIN. This method reduced only a part of SSA.

In shoulder surfing attacks, adversaries should move their eye fixations rapidly on the user interface, particularly during preprocessing, to obtain the challenge information, e.g., the layout of the keypad, in an on-time processing phase to catch the key entry information, e.g., a user's key press; and during post processing to filter the acquired information. If the time period allowed for those processes is too short or its memory requirement exceeds the human limit, then shoulder surfing should fail [8].

To extend and effectively use the allowed time period, the existing idea is to employ covert attention. If an adversary suppresses saccadic eye movements during visual perception [9], she can earn more temporal chances for visual information processing within the current visual angle. This is true even while conducting covert attentional shifts to a stimulus inside the visual angle and carrying out parallel motor operations without saccadic eye movements.

To reduce the memory requirement, our idea is to employ perceptual grouping. If an adversary extracts significant visual relations from lower-level features, e.g., color of squares by ignoring the individual digits, and groups them into higher-level structures, e.g., a larger polygon in the same color, based on the Gestalt principles, she can reduce the number of visual objects stored in the short-term memory. So in Covert attentional shoulder surfing, three main operations such as covert attention, perceptual grouping, and parallel motor operation, are combined together for deriving a PIN digit. In each round, attended objects are lined for easier understanding of covert attention. Covert attentional shoulder surfing [4] can break the BW method through the modeling-based analysis.

The major disadvantages of this method are that it uses the perceptual grouping concept which the hackers can easily trace out the PIN number of the user [6]. Only two colors are used which makes the way easier to find the user PIN number [9]. this method even takes more number of iterations which makes the PIN entry method of the user complex.

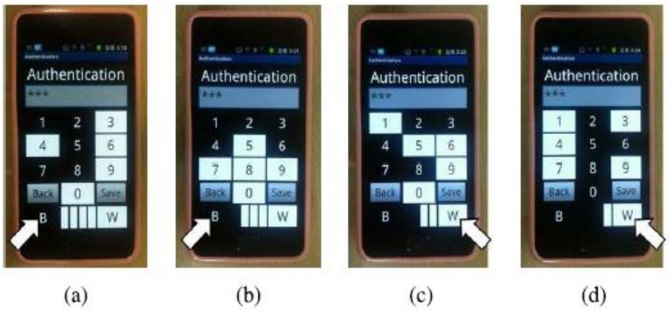


**Figure 3:** An example round to input 1 in IOC, where the user enters "Black," "Black," "White," and "White" in sequence. (a) Stage 1. (b) Stage 2. (c) Stage 3. (d) Stage 4.

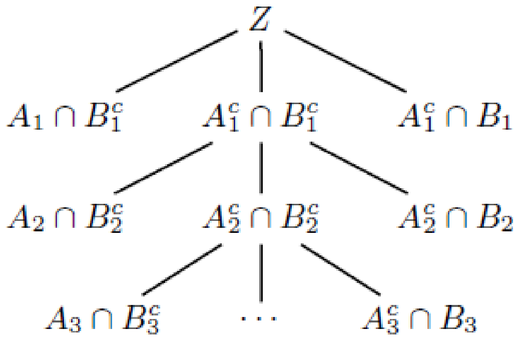
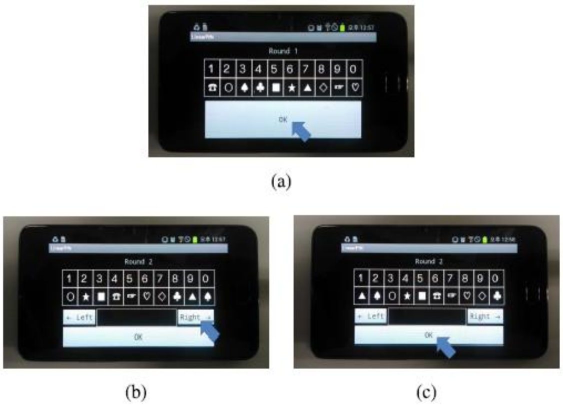


**Figure 4:** The decision tree to compute the probability of successful impersonation of a BW method by an adversary.

### 4. Session key method

The basic layout of our method comprises a horizontal array of digits from 0 to 9, juxtaposed with another array of ten familiar objects such as ○ and △, as shown in Figure 3. For simplicity, we assume that the number of digits in a PIN is four, although the proposed method may be applied to any case with N ≥ 2 digits.

It is a new 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 familiar objects such as + and / etc. For simplicity, we assume that the 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 first 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 immediately 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 symbol as the session key because it is collocated with the first digit of the PIN, 2. The remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in the ith round for i = 2, 3, 4. In each of these rounds, the user is again given a random array of ten objects, and s/he enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit. For this task, the user can use two additional buttons (“Left” and “Right”). In the example round, shown in Figure. 3(b) and (c), the user presses the “Right” button twice so that symbols moves to the position immediately below 3, and then presses “OK.”.This method is also known as the linear key board method and it is considered to be one of the weakest methods as it can be easily hacked using GA and RA.



(a)

(b)

(c)

**Figure 5:** 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.

## IV. The Proposed Method

The advanced method of the basic BW method, which is the improved BW method, is proposed by extending BW method. In this, the proposed algorithm uses randomly generated four digits in which each digit block, is combined with the combination of two, to prevent the attentional shoulder surfing attack by extracting the PIN digit after all the user iterations got completed.

To resist covert attentional shoulder surfing, it would be effective to interrupt the adversary during perceptual grouping without changing the user task significantly. One possibility is to keep the BW method, but randomize the ordering of the digits in each round so that perceptual grouping cannot be done in the way we proposed. In this case, however, the user task requires the added saccadic eye movement while searching for the location of the target digit in every round can lead to longer PIN entry time. Another possibility is to keep the numeric keypad in the regular layout, but produce more perceptual groups so that the adversary is frustrated. Toward similarity in the task of perceptual grouping, we make color groups look similar (neither the same nor opposite) in their shape because color must be distinguishable by the user.

Toward complexity, the color groups are made to look overlapping (not separate), so that adversaries experience severe difficulties not only in holding the groups in VSTM but also in separating them. The fundamental idea for combining similarity and complexity is to split visually every numeric key into two halves, so as to be filled with two distinct colors simultaneously whereas each color fills half of the available keys, i.e., five out of ten keys[4]. So there exist four color groups on the numeric keypad and two colors for every numeric key. The adversary who launches covert attentional shoulder surfing may need to perceive four color groups and attend to one of them for the next round, while the user only needs to answer either of the two colors that fill his/her PIN digit key in each round. Authentication Services are also provided by this method.

### 1. Creating an ATM application using android

The ATM is considered as the highly defected area according to this paper. Hence, the ATM application is been moved to the smart phones for the purpose of privacy and security[5]. Now-a-days, smart phones are used by many people and it being converted as one of the basic needs. A survey says that, one of every five people in the world own a smart phone.

When such an application is moved to the smart phones, a large list of measures has to be considered. It is a good thought to create this process as an android application. An ATM application is created as a android application which may be downloaded and installed easily in every android mobile from the play store.

This application is created to particularly focus on the secure PIN entry. In such case, it is better to provide choices to the user of the application to provide the PIN number securely. As there is no detailed study about the existing PIN entry methods, those methods are also included in this application for making the detailed analysis.

When such ATM applications are created and implemented, the transactions can be made within the smart phones and even there will be no need to use the ATM cards [5]. The user will possess the ATM cards but once registered in this application the transactions can be processed using smart phones.

The application diagram shows the model or the workflow of the application that is been created. First, the user registers into the application where the user is asked to the basic details such as name, password, email id, etc. Once that form is submitted, a unique PIN is send to the respective mail id of the user. When the user id verified, registration phase will be made successfully. Then the user will login into the application with the user name and the password. Once the user is validated, the services are provided to the user [7].

The user is given three options for the PIN entry. Any one method may be selected for entering the PIN to the application. When the user’s PIN is validated, the ATM transactions may be performed by the user by using the application.

The virtual money is commonly termed as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community". When this concept is implemented the ATM transactions can be performed using the smart phones, where the transactions are made with the virtual money.

This method mainly uses the concept of virtual money where the money is represented with a tokens or an image with unique id. so which the entire ATM applications can be moved to the smart phones . All transactions can take place through this application which is developed for the devices using android. This application may help the user to make all the transactions more simple and easy.

## V. The Architecture Diagram

The application diagram shows the model or the workflow of the application that is been created. First, the user must register into the application where the user is asked to the basic details such as name, password, email id, etc. Once that form is submitted, a unique PIN is send to the respective mail id of the user. When the user id verified, registration phase will be completed successfully. Then the user will login into the application with the user name and the password. Once the user is validated, the user gets the access rights of the service.

The user is given three options for the PIN entry such as BW method, IBW method and session key method. Any one method may be selected for entering the PIN to the application. When the user’s PIN is validated, the ATM transactions may be performed by the user by using the application.

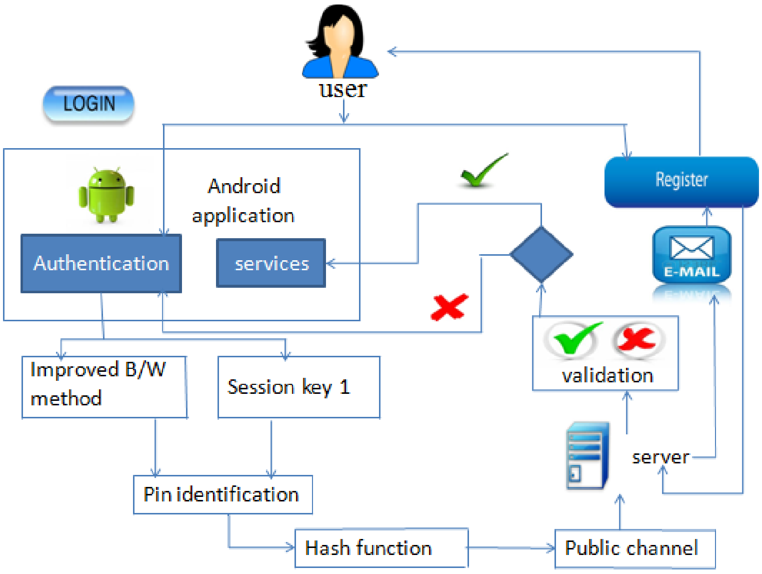


**Figure 6:** The Architecture Diagram

The ATM transactions include the deposit, withdrawal and balance checking [7]. All actions can be performed in the android ATM application where the money will be in the form of tokens or images by using the virtual money concept. All online transactions can be done with those token and it can also be exchanged into money at the exchange centers specially developed for this purpose. Many public threats such as theft may also be avoided.

### The Improved Bw Method

The improved method BW method consists of two colors on the single key. A single key is divided into two halves, each half containing different colors. The user is given an option to choose an upper half color or the lower half color. Even if the shoulder surfing attack is been done during the PIN entry in this method, those human adversaries will not be able to guess the right PIN. This method also prevents the recording attacks.

A well-trained perceptual grouper could not track the PIN digit entered by the User in a conventional way. The This method is implemented with a new Strategy that will completely reduce Shoulder Surfing attacks and even perceptual grouping concept used in the BW method is made more complex and hence the adversaries would find it difficult to shoulder surf or record the information of the user.

When the layout of the IBW method is represented with the sets then the colors and the digits should be put in separate sets. Let P denote a set of four colors and/or patterns customizable [4]. Let P = {black, blue, white, yellow} or P = {black, white, dotted, diagonal stripes}, for a color blind person. The system displays a set of ten digits, A = {0, ???, 9}, on the regular numeric keypad with two split colors, which may be chosen from P, in each numeric key; and there exists the four color keys below.

A color is chosen at random from P and fills in the splits of distinct keys; each split could be either upper or lower one. A single color would be filled in five half spaces. The remaining colors fill five splits, respectively, in the same way. The user attends to the PIN digit and enters either of its color through the color key. The user and the system repeat this procedure for m rounds that the PIN digit is identified by intersection, and until the entire PIN digits are identified.

The improved BW method is implemented as an advanced method to the basic BW method. To provide security to the PIN entry methods from shoulder surfing attack and recording attack, particularly in the ATM machines, the entire ATM application moved to the smart phones. This can be possible only when the virtual money concept is on practice.

The structure layout of the Improved Black White method is shown below.  There is also a digit indication which will help the user to know that which digit they are entering currently.

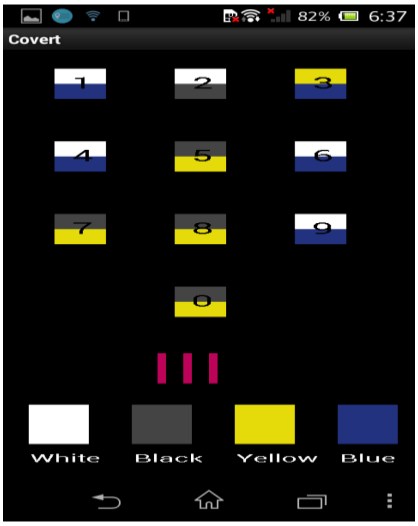


**Figure 7:** The Structure of Improved BW method

## VI. Conclusion

The proposed method uses an android ATM application which can be installed in the android smartphones, along with the improved black white method, which increases the security level of the password or the PIN number. This approach gives the user a secure PIN entry method which mainly protects the user's PIN from various attacks such as shoulder surfing attack, guessing attack and the recording attack.

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. It comes with a more secure and a colourful keypad. As this method uses more than two colours (i.e.  Four colours), the PIN entry method is made protectable and entertain able for the users.

This requires an inference with better optimization techniques, which can for example; reduce entry time taken by the user that may further improve the classification accuracy. The covert attentional shoulder surfing proposed in this paper is to our knowledge the first sophisticated counter-attack of humans against the system, previously evaluated to be secure.

In addition to this, the methods which are explained in the existing system (such as black white method and session key method) is also implemented in order to find a better statistics to show that the proposed method is the more secure and the safety method. The experimental results of the existing BW method and the proposed IBW method are shown in the form of graph.

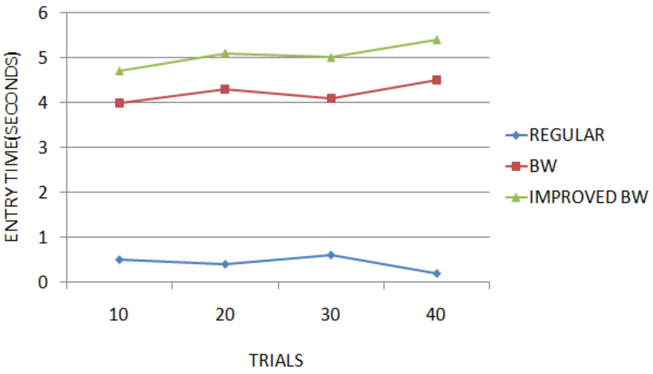


**Figure 8:** The graph for the comparison of PIN- entry methods

## VII. Future Enhancement

Some of the future enhancements that can be done to this system are that it is possible to upgrade the method and can be adaptable to desired environment. This is done based on the optimization methods where the number of rounds taken for the PIN entry method can be minimized. It is also based on the object- oriented design hence any further changes can be easily adaptable. Based on the future security issues, security can be improved using emerging technologies. It also includes the adjustment of the selection bias in the future PIN entry model training process. This method also implements the virtual money concept and moves the ATM application to the smart phones.

## References

[1]. V. Roth, K. Richter, And R. Freidinger, "A Pin-Entry Method Resilient Against Shoulder Surfing," In Proc. Acm Conf. Comput. Commun Security, 2004, Pp. 236– 245.

[2]. A. D. Luca, K. Hertzschuch, And H. Hussmann, "Colorpin: Securing Pin Entry Through Indirect Input," In Proc. Chi, 2010, Pp. 1103–1106.

[3]. A. Bianchi, I. Oakley, V. Kostakos, And D.-S. Kwon, "The Phone Lock: Audio And Haptic Shoulder-Surfing Resistant Pin Entry Methods For Mobile Devices," In Proc. Tei, 2011, Pp. 197–200.

[4]. W. S. Geisler And B. J. Super, "Perceptual Organization Of Two-Dimensional Patterns," Psychol. Rev., Vol.107, No. 4, Pp. 677–708, 2000.

[5]. X. Bai, W. Gu, S. Chellappan, X. Wang, D. Xuan, And B. Ma," Pas: Predicate Based Authentication Services Against Powerful Passive Adversaries," In Proc. Ieee Annu. Comput. Security Appl. Conf., Dec. 2008, Pp. 433–442.

[6]. T. Kwon, S. Shin, And S. Na, "Covert Attentional Shoulder Surfing: Human Adversaries Are More Powerful Than Expected," Ieee Trans. Syst., Man, Cybern, Syst., Pp. 1–12, To Be Published.

[7]. 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 (Ndss) Symp.2012.

[8]. Banking—Personal Identification Number (Pin) Management And Security—Part 1: Basic Principles And Requirements For Online Pin Handling In Atm And Pos Systems, Clause 5.4 Packaging Considerations, Iso 9564-1:2002, 2002.

[9]. W. Moncur And G. Leplâtre, "Pictures At The Atm: Exploring The Usability Of Multiple Graphical Passwords," In Proc. Chi, 2007, Pp. 887–894.