International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 3, June 2019, pp. 1879~1886
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i3.pp1879-1886

Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication

Abiodun Esther Omolara[1], Aman Jantan[2], Oludare Isaac Abiodun[3], Humaira Arshad[4], Nachaat AbdElatif Mohamed[5]
[1,2,5]School of Computer Sciences, Universiti Sains Malaysia, Malaysia
[3]Department of Computer Science, Bingham University, Nigeria
[4]Department of Computer Science, The Islamia University of Bahawalpur, Pakistan

Article Info

Article history:

Received May 31, 2018
Revised Nov 27, 2018
Accepted Dec 20, 2018

Keywords:

ATM
Biometric
Eavesdropping
Iris
Password
Shoulder-surfing

ABSTRACT

The tumultuous increase in ATM attacks using eavesdropping, shoulder-surfing, has risen great concerns. Attackers often target the authentication stage where a customer may be entering his login information on the ATM and thus use direct observation techniques by looking over the customer's shoulder to steal his passwords. Existing authentication mechanism employs the traditional password-based authentication system which fails to curb these attacks. This paper addresses this problem using the FingerEye. The FingerEye is a robust system integrated with iris-scan authentication. A customer's profile is created at registration where the pattern in his iris is analyzed and converted into binary codes. The binary codes are then stored in the bank database and are required for verification prior to any transaction. We leverage on the iris because every user has unique eyes which do not change until death and even a blind person with iris can be authenticated too. We implemented and tested the proposed system using CIMB bank, Malaysia as case study. The FingerEye is integrated with the current infrastructure employed by the bank and as such, no extra cost was incurred. Our result demonstrates that ATM attacks become impractical. Moreover, transactions were executed faster from 6.5 seconds to 1.4 seconds..

Corresponding Author:

Aman Jantan,
Security and Forensic Research Group (SFRG) Lab,
School of Computer Sciences,
Universiti Sains Malaysia,
11800 USM Penang, Malaysia.
Email: styleest2011@gmail.com

1. INTRODUCTION

Usability and comfort have made people rely and trust the Automatic Teller Machine (ATM) to conveniently meet their banking needs in Malaysia and worldwide. According to [1], the use of internet banking and also ATMs in Malaysia have catapulted from 2.6 million consumers in 2005 to 23.5 million consumers towards the end of February 2017, an 803.85% growth for the past thirteen (13) years. However, recent occurrence of a geometric increase in ATM fraud in the country and across the globe has caused great concerns. This exponential increase in the use of ATM co-evolves with advanced threats perpetrated daily using ATM platform. Several security threats such as shoulder-surfing: where a fraudster keenly observes a customer entering his pin or password, eavesdropping/man-in-the-middle attack: where a criminal may intercept/record a users verification code, hidden camera attack: where a camera is placed in a hidden area near the ATM to capture and record the customers password or skimming where a device is used to capture a

customer's pin or confidential data using the magnetic strip of the ATM card when the user is entering his details into the ATM [2], [3]. See Figure 1 for illustration of ATM fraudulent activities.

A shoulder-surfing attack often occurs in a crowded place where a customer may not know that a malicious person is observing his fingers as he enters his passwords into the ATM keyboard or touchscreen. Also, in cases where verification code is used as a second security layer (two-factor authentication), an attacker may intercept/eavesdrop on the verification code. As much of this attacks happen at the authentication stage, various authentication schemes have been proposed using biometric of humans. Biometric technologies based on physiological attributes of an individual such as; the hand geometry, retina, iris, fingerprint and those based on behavioural features of an individual such as; signature, lip's movement, blinking, etc have been proposed for identifying a user before authentication is allowed [4]. The recent biometric system proposed by several research centres holds great promise for enhancing the security of authenticating smart systems and smart devices. Biometric system such as Rhythmprint authentication, which combines an advantage of the traditional password-based authentication and a multi-touch innovation based on a touchpad on a computer or a screen of a smartphone [5] provides high security and can mitigate shoulder-surfing. Face recognition system [6], iris detection and recognition [7], ear recognition method [8], electrocardiogram (ECG) signal waveform [9], etc presents recent innovations in biometrics that can be applied to reinforce the biometric security of ATM system. However, most of this technology are in their infancy and have not been applied for the security of ATM machines. Moreover, some of this technology has not been adopted because of low user acceptability, complexity, and failure to work seamlessly in an ATM setting.

Existing biometric system often employed in the ATM system is the pin or password-based authentication. The personal identification number (PIN) is the conventional authentication system used in various devices, such as ATMs, mobile devices, etc. Nevertheless, it fails to counter shoulder-surfing attacks. The conventional configuration of numbers on an ATM keypad is familiar to the point that it's feasible for a keen observer to unravel a password or pin after several viewings using surveillance camera. Consequently, several shoulder-surfing resistant strategies have been proposed. Recent studies to mitigate shoulder-surfing by [10] employed IllusionPIN which deploys a hybrid-image keyboard that appears one way to the customer and completely different to an observer at a distance of three feet or more. [11] propose a strategy which is impervious to shoulder-surfing attack by utilizing a false image in the authentication system. Other authentication schemes proposed by [12]-[19] are resistant to shoulder-surfing attacks but some fail to confront man-in-the-middle or eavesdropping attack. Others were not adopted due to usability issues and failure to provide a reasonable security threshold. We discovered from the literature that there is no single proposal that restrains all the attacks as a whole.

We address this problem using FingerEye and iris scan for authentication. A detailed treatment of how FingerEye work can be found in the proposed method section. Our approach is different from other approach found in the literature because it does not mitigate shoulder-surfing but it eradicates the possibility of shoulder-surfing, eavesdropping, and man-in-the-middle attack. The inspiration behind this research relies on the hypothesis that iris identification technology is widely accepted and is gaining ground as the best authentication system as it has high reliability, unique and distinctive (even identical twins do not share the same pattern of iris) [7]. The verification process is swift, the iris texture remains stable (it does not change), it can be captured from a distance without harm to the eye.

Our motivation was not only to propose an approach to curb ATM threats but also to design security solutions keeping in mind not only customers with abilities but also people with disabilities. Thus, it is our conjecture that blind customers can also be served using our proposed approach which other authentication systems are not robust to. This research proposes measures against covert observation so as to deter a customer authentication information from being stolen or intercepted by a malicious observer. Figure 1 shows Techniques and tools for perpetrating ATM frauds

Figure 1. Techniques and tools for perpetrating ATM frauds

2. THREAT MODEL

Our threat model comprises of shoulder-surfing, eavesdropping, man-in-the-middle attack scenarios against Password or Pin-based authentication using ATM. Different scenarios include attacks with a different challenge of alleviating such attacks. Table 1 classifies each attack model with the current authentication.

Table 1. Attack Model on Existing Authentication System

CURRENT AUTHENTICATION SYSTEM	ATTACK MODEL
✦ A single factor authentication where the client enters his password/pin. ✦ The password is checked and compared against the one stored on the bank's database to verify if they match. ✦ Access is granted if there is a match or denied if there is no match.	ATM machines use a keyboard/console where passwords are entered. In some cases, the touchscreen allows direct entry of the passwords. In this regards, we model a shoulder surfer as a malicious person who keenly observes the client's console or screen of the ATM in use. He focuses on the client's shoulder, the motion of his head or the ATM screen. Some banks allow their customers to authenticate using a password-only verification to carry out transactions on the ATM machines. In this case, the attacker needs to shoulder-surf and steal the password only. After which, he masquerades as the customer, authenticates and steal the client's money. Other banks allow password entry after inserting a personalized ATM card. In this scenario, the attacker shoulder-surf and steals the password. Then he may use a bank application on a phone to authenticate and thereafter transfer the money or otherwise use sophisticated chips to withdraw the money directly on the ATM.
✦ To control shoulder-surfing attacks, some banks allow two-factor authentication or multi-factor authentication. ✦ In this setting, the client authentication relies on password and other forms of authentications such as a 4-digit or 6-digit verification code sent to the clients mobile phone or a fingerprint or voice print.	We model an eavesdropper or a man-in-the-middle threat as an attacker that may intercept the verification code and use it for his malicious act. For instance, in a two-factor authentication system, it combines the use of a PIN and a One Time Password (OTP) for the customer's verification. The customer enters his PIN and if the PIN is verified to be correct, then an OTP is generated by the bank and sent to the customer usually on his mobile using a short message service (SMS). If the OTP entered by the customer corresponds to the OTP sent by the bank, then he is authenticated and allowed to carry out his transaction, otherwise, his authentication is rejected. The security of the OTP is highly flawed as SMS is transmitted as plaintext through open channels which are easily wiretapped. Thus, making the OTP susceptible to eavesdropping attack, a man-in-the-middle attack who may intercept, use or modify the OTP. Moreover, in the event that the PIN to an ATM card has been compromised, and the mobile number of the customer is known, the OTP sent via the SMS can be intercepted easily. The attacker can now impersonate the customer and verify into his account using the PIN and OTP without the bank recognising any discrepancy. In the case of a voice print authentication, a criminal may record the voice of the client and use the recording to masquerade as the user to authenticate into the system. The fingerprint can be distorted based on severe manual labour and overtime use and so may not be reliable.

3. PROPOSED APPROACH

A user is referred to as a bank customer or client when he has registered his details in the bank and the bank has created a profile for him/her. The content of the profile is usually his personal data along with his authentication details. The authentication details is required to allow access for him/her to carry out any transaction, such as withdrawal, transfer of money etc.

3.1. Registration/enrolment phase

In this phase, the bank collects the client's personal information such as his full names, date of birth and specifically the iris of the client is scanned and recorded using a digital camera. A clear and high-contrast

picture of the client's iris is captured. After capturing the features into the computer system, the computer analyses the pattern in the iris and converts them into binary codes. The binary codes are then stored and are required for verification. Figure 2 outlines the process of enrolment and storage into the bank's database.

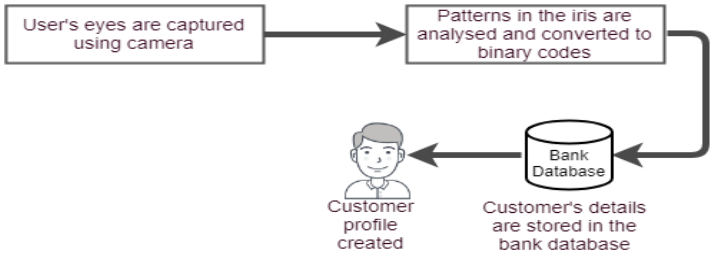

Figure 2. Registration process for creating a customer's profile

3.2. Verification Phase

This phase is where the authentication is actually done. Whenever the client needs to carry out a transaction, he stands in front of the camera and a picture of his iris is taken. It is automatically converted to binary codes and compared with the binary codes of the previous image captured at the enrollment phase (which is stored in the bank's database). If the two codes matches, then the client is authorized to carry out his/her transactions otherwise, he is denied entry into the application. Figure 3 outlines the process of verification of a customer's credentials.

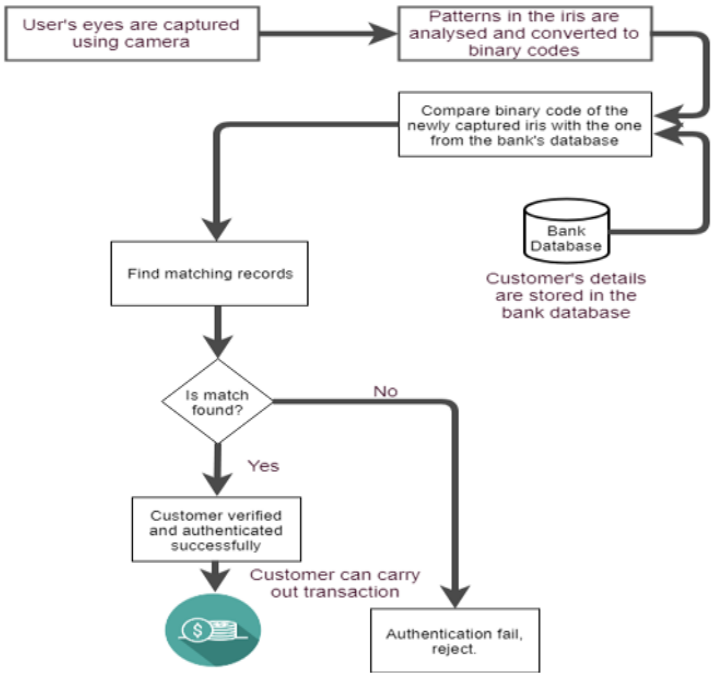

Figure 3. Verification process for enabling entry/denial into the ATM transaction interface

3.3. FingerEye

We decided to leverage on iris scanning technology because it provides a fast, stable and accurate result during authentication. Iris scanning is an eye-based identification which implies that they depend on unique physiological features of the eye to identify an individual.

The human iris is a flat, ring-shaped tissue behind the cornea of the eye. It contains muscles that constantly adjust the size of the pupil and control the amount of light that gets into one's eye. Iris recognition

uses video camera technology with near infrared illumination (NIR) to capture images of the structures of the iris. The images are turned into binary codes which represent an individual's identity.

We design and implement a simple application called the FingerEye to run on the existing windows computer used in the bank so as not to incur the cost of additional hardware/infrastructure. We build the interface and integrated it with the bank digital camera to collect the details of customers during enrolment and subsequently allow authentication.

Our application, FingerEye is designed using a cross-platform Python framework, Kivy. The role of the FingerEye is to act as a medium of connecting the bank, the surveillance system and the user. Figure 4 presents a screenshot of the FingerEye software.

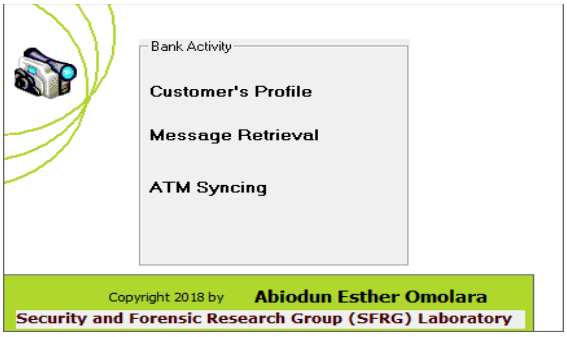

Figure 4. A Screen-shot of FingerEye software

We proposed two methods for carrying out transactions.
In the first method, a bank customer who has a customer profile with the bank and wants to withdraw one thousand (1,000) dollars will follow the outlined process as shown in Figure 5.

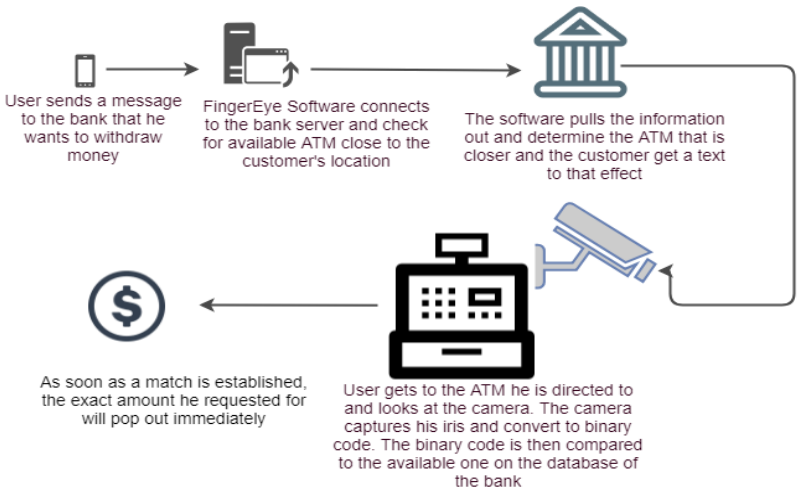

Figure 5. A simple process to withdraw a sum of $1000

We discovered that this method was very good especially where the customer wants to withdraw a large sum of money. However, a limitation with this is that the ATM pops out the original sum the customer requested and logs off. What if the customer has a change of mind and wants to reduce or withdraw more money? He will have to place another request and cancel the first request or withdraw the initial request he made and make another request. This may be cumbersome for the customer. With this in mind, we propose the second method where the customer only informs his bank that he needs to carry out a transaction and he is authenticated as soon as he gets to the ATM and given full control of the ATM.
In the second method,

1. The customer sends a message to the bank that he wants to carry out a transaction. Note that the FingerEye can be configured such that the customer just send a unique code. The unique code signifies (not for verification) that he/she wants to carry out a transaction in the ATM.
2. FingerEye checks for the closest ATM near the customer's location and sends a message to the customer to use the ATM. The software is configured to send up to five (5) ATM's that are close and the software will be on the lookout for the one the customer visits.
3. Once the customer gets to any of the suggested ATMs, he looks at the camera and his iris is captured and compared with the ones in the database, when a match is found, he is authenticated and can withdraw, transfer and carry out other activities on his account.

We thought of a third method where a customer does not need to send a message. He just goes to the ATM machine and he authenticates by directly looking at the ATM machine. This appears to be the fastest and easiest method as the customer need not send any message. This system also worked well when we tried it as we did not have to install any new infrastructure. We only had to configure the FingerEye software to be in automatic-mode to capture any customer using the iris for authentication and subsequently, work in sync with the camera to record the transaction details. In all the three methods proposed, the third method was the fastest. However, we prefer the first and second method because it gives us a level of control of the customer's activities. In all the three methods, a user is automatically logged out in 5 seconds as soon as no further activity is detected by the FingerEye software.

4. EVALUATION

In this section, we evaluate our proposed system. We carried out our experiment using ten (10) computer science students from our laboratory as the participants. Our intention was to experiment and evaluate the proposed system for accuracy in curbing attacks, usability, and speed with which each transaction takes place. Unfortunately, we were not able to test the system for visually impaired people. In our future work, we shall be testing the system on the visually-impaired person and also adding some features for the deaf, dumb and other functions for people with disabilities.

All ten (10) participants were enroled into the bank system. This includes collecting their details and capturing their eyes individually to extract the features of the iris and convert to binary codes which were stored in the bank's database.

4.1. Shoulder-surfing

To evaluate if shoulder-surfing was mitigated, we mobilized the 10 participants to the bank, and each participant was authenticated using the camera while the nine remaining participants watched from behind. It was observed that shoulder-surfing is completely impractical as the participant is authenticated with his iris. Shoulder-surfing is possible only in an environment where the attacker can observe the movement of the user's body/finger as he enters his password/pin. Our system defeated any form of shoulder-surfing.

4.2. Eavesdropping attack/Man-in-the-middle attack

Eavesdropping/man-in-the-middle attack is possible in an authentication system that employs verification code. In our proposed approach, verification is done using the iris scanner which works with the FingerEye to verify the user and as such eavesdropping or man-in-the-middle attack is impracticable with our system.

4.3. Speed

To evaluate the speed, we decided to create a pin for each participant. We intended to determine how fast a user is authenticated using the pin-based method and the proposed iris scanning method. We show the time in seconds within which each participant took to authenticate to ATM using existing and proposed method in Table 2. in (1) for calculating the average to determine the method with the higher speed of authenticating is

$$A = \frac{1}{n}\sum_{i=1}^{n} a_i = \frac{a_1+a_2+a_3+\ldots+a_n}{n} \quad (1)$$

Where,
A = Average
n = Number of observations (participants)

a_i = the value of each participant's time to authenticate

Table 2. Time taken by each participant to authenticate to ATM using the existing and proposed method

Participant	Pin-based Authentication Time (seconds)	Proposed FingerEye Authentication Time (seconds)
1	7	2
2	6	1
3	8	1
4	4	1
5	7	1
6	6	2
7	9	2
8	8	1
9	4	1
10	6	2
Total	65	14

The average time for existing pin-based authentication method was $\frac{7+6+8+4+7+6+9+8+4+6}{10} = 6.5$ Seconds

The average time for the proposed FingerEye method was $\frac{2+1+1+1+1+2+2+1+1+2}{10} = 1.4$ Seconds

From our investigations, we deduced that shoulder-surfing assault, man-in-the-middle attack, and eavesdropping attack is not just mitigated but entirely dismissed in the proposed approach. We also observed that the efficiency of the system is improved as the average time to authenticate in the proposed system is 1.4 seconds which is faster than the pin or password-based system that takes about 6.5 seconds. The increased speed of authentication means that transactions can be carried out faster in the proposed method. Unlike retina or other body-biometric systems that may affect the eyes/body part, the iris scan authentication does not affect the eyes. All these features improve the security and usability of the proposed system.

We were unable to test the proposed system for a visually impaired person, but we surmise that authentication will also be secured and faster. Each of our participants used 1 or 2 seconds to authenticate to our proposed system; we can safely conclude that a visually impaired person will use between the same range. Moreover, our proposed approach creates a secure authentication means for the visually impaired customer as he/she may not detect a hidden camera installed to eavesdrop on him/her or even measure the presence of a nearby shoulder-surfer during authentication.

5. CONCLUSION AND FUTURE WORK

Majority of ATM attacks are perpetrated during the authentication stage when a bank client wants to enter his/her password or personal details to carry out bank transactions. In this paper, a proactive approach of confronting ATM threats that occur during the authentication stage was proposed. Threats such as shoulder-surfing, eavesdropping, and man-in-the-middle attack are completely eliminated in this approach. We used CIMB Bank, Malaysia as a case study and we also created an attack model of the current authentication system in use and how they can be defeated during the authentication stage. Our approach employs iris-scan authentication and FingerEye software to allow seamless authentication.

From the experiment conducted while testing our system, we can safely conclude that attacks perpetrated through eavesdropping and man-in-the-middle attack become infeasible. Also, impersonating a user and also shoulder-surfing becomes impractical. Finally, the speed of authenticating a customer increased considerably from the existing pin-based method which is 6.5 seconds to 1.4 seconds. This improvement increases the speed of transaction and subsequently the efficiency of the system.

In the future, we plan to further extend our work by testing and building an ATM system with complete features for serving every kind of disabled persons such as the blind, the deaf and the dumb.

REFERENCES

[1] Tan SF, Samsudin A., "Enhanced Security of Internet Banking Authentication with EXtended Honey Encryption (XHE) Scheme," *In Innovative Computing, Optimization and Its Applications, Springer, Cham,* pp. 201-216, 2018.

[2] Sankhwar S., Pandey D., "A Safeguard against ATM Fraud," In *Advanced Computing (IACC), 2016 IEEE 6th International Conference,* pp. 701-705, Feb 2016.

[3] Shriram S., Shetty SB., Hegde VP., Nisha KC., Dharmambal V., "Smart ATM surveillance system," In *Circuit, Power and Computing Technologies* (ICCPCT), *2016 International Conference*, pp. 1-6, Mar 2016.

[4] Siddiqui AT., "Biometrics to control ATM scams: A study," In *Circuit, Power and Computing Technologies (ICCPCT), 2014 International Conference*, pp. 1598-1602, Mar 2014.
[5] Wongnarukane N., Kuacharoen P., "The Security Challenges of The Rhythmprint Authentication," *International Journal of Electrical & Computer Engineering (IJECE)*, vol. 8(3), pp.2088-8708, Jun 2018.
[6] Rassem TH., Makbol NM., Yee SY., "Face recognition using completed local ternary pattern (CLTP) texture descriptor," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7(3), pp. 1594, Jun 2017.
[7] Biswas R., Uddin J., Hasan MJ., "A New Approach of Iris Detection and Recognition," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 7(5), pp. 2530-6, Oct 2017.
[8] Hourali F., Gharravi S., "An Ear Recognition Method Based on Rotation Invariant Transformed DCT," *International Journal of Electrical and Computer Engineering (IJECE)*, 7(5), pp. 2895-901, Oct 2017.
[9] Shdefat AY., Joo MI., Choi SH., Kim HC., "Utilizing ECG Waveform Features as New Biometric Authentication Method," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 8(2), pp. 658-65, Apr 2018.
[10] Papadopoulos A., Nguyen T., Durmus E., Memon N., "Illusionpin: Shoulder-surfing resistant authentication using hybrid images," *IEEE Transactions on Information Forensics and Security*, vol. 12(12), pp. 2875-89, Dec 2017.
[11] Yeung AL., Wai BL., Fung CH., Mughal F., Iranmanesh V., "Graphical password: Shoulder-surfing resistant using falsification," In *Software Engineering Conference (MySEC), 2015 9th Malaysian*, pp. 145-148, Dec 2015.
[12] Lee MK., "Security notions and advanced method for human shoulder-surfing resistant PIN-entry," *IEEE Transactions on Information Forensics and Security*, vol. 9(4), pp. 695-708, Apr 2014.
[13] Sun HM., Chen ST., Yeh JH., Cheng CY., "A shoulder-surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, Mar 2016.
[14] Wang L., Chang X., Ren Z., Gao H., Liu X., Aickelin U., "Against spyware using CAPTCHA in graphical password scheme," In *Advanced Information Networking and Applications (AINA*), *2010 24th IEEE International Conference*, pp. 760-767, Apr 2010.
[15] Wakabayashi N., Kuriyama M., Kanai A., "Personal authentication method against shoulder-surfing attacks for smartphone," In *Consumer Electronics (ICCE), 2017 IEEE International Conference*, pp. 153-155, Jan 2017.
[16] Jang JJ., Jung IY., "An access control resistant to shoulder-surfing," In *Intelligence and Security Informatics (ISI)*, 2015 IEEE International Conference, pp. 196-196, May 2015.
[17] Omolara AE., Jantan A., Abiodun OI., Singh MM., Anbar M., Dada KV., "State-of-The-Art in Big Data Application Techniques to Financial Crime: A Survey," *International Journal of Computer Science and Network Security*, vol. 18(7), pp. 6-16, Jul. 2018
[18] Bianchi A., Oakley I., Kostakos V., Kwon DS., "The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices," In *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*, pp. 197-200. Jan 2011.
[19] Bianchi A., Oakley I., Kwon DS., "The secure haptic keypad: a tactile password system," In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 1089-1092, Apr 2010.