INVESTIGATING THEHUMAN FACTORS AFFECTING ON ONE TIME PASSWORDS TECHNOLOGY ACCEPTANCE: A CASE STUDY IN BANKING ENVIRONMENT

[1]SAJJADSHOKOHUYAR, [2]MAHSAZOMORRODIANBAJI, [3]SAGHARPOUYANSHAD

ShahidBeheshti University, Tehran, Iran
Email: s_shokouhyar@sbu.ac.ir

Abstract: According to fast technology growth, modern banking tries to decrease going to bank and increase customer's consent. One of the problems which banks face is securing customer's password. The banks' solution is one time password creation system. In this researchby adapting from acceptance of technology model theory, assesses factors that are effective on banking in Iran especially in using one time password machine by one of the private banks of Iran's customer. The statistical population is all of this bank's customers who use electronic banking service and one time password technology and the questionnaires were distributed among members of statistical population in 5 selected groups of north, south, center, east and west of Tehran. Findings show that confidential preservation, education, ease of use and advertising and informing has positive relation and distinct hardware and age has negative relation.

Keywords: Security, Electronic Banking, One Time Password, Information Technology.

I. INTRODUCTION

Everyday life depends on computer technologies. From ordinary offices to grocery stores, computers are used to support business processes. Personal life is also relyingon computer and communication technologies. As more and more people do onlinebanking, use e-mails to keep in touch with their friends, read newspapers online, shop online and download music for their MP3 players, authentication for accessingprivileged information is required.Several access control methods have been used. The password-based authentication system is the most commonly used systemfor access control because it is easier to implement and deploy, less costs to manage,and no special device or software is required [1]. However, conventional password-basedauthentication methods are vulnerable to eavesdropping, over-the-shoulder, key-logging,replay, off-line dictionary, and server spoofing attacks. The vulnerability of theseattacks is associated with the permanent characteristic of a password.The one-time password is inherently more robust from these attacks, because thepassword is changed every time and the same password cannot be used at a later time.

One-Time Passwords (OTP) can act to augment existing user IDs and passwords with an extra layer of authentication to enhance security for all authenticated applications. The reason is that if a password is compromised, the OTP would still have to be broken as well to gain access. This kind of authentication is called two-factor authentication, a stronger kind of authentication [2].

In industrial countries, banks' role transforms rapidly and new devices with modern technology were used in banking industry. Thus, presenting modern services and products beside quality preservation and improvement makes this industry's members' fates. Noticing, nowadays international business and banking world is changing rapidly and deeply. We believe that today's banks think about extension and increasing availability among customers strategically. In this circumstance, managers and experts of banking network should align with international modern business. Information and communication technology nowadays is used by different systems especially banks that present new services and products accompanied by continuous assessment and quality improvement as a competitive advantage. This becomes a value-added strategy for customers in different levels.

Today by information technology development and utilization of it more than before in business and financial, lots of economic activities are done in cyber space which becomes more and more. As banking industry and financial institutes use this service more than others, they are attacked by these threats. In electronic banking, by using substitute communication channels, try to reduce going to branches of banks and increase comfort and consent. One of the most important and the most usable of these channels is internet banking which eliminates time and place restrictions with a computer, in all places and all the time, links between customer and bank and present all none-attendance services. Linking between customer's computer and bank's central computer by customer's browser is base of this kind of banking. Today all of the transactions except cash withdrawal are done by internet banking. In addition to these advantages, reducing bank's cost by decreasing paper use, reducing staffs without need to large and fixed place are the main factors that banks approach internet banking. Aside these advantages, there are some threats which the most important one is customers' password break by frauds and having access to their accounts. One of the fundamental reasons for customers' lack of interest to

use internet banking's services is unsecured services and lack of security of it. Thus, banks for increasing customers' confidence to these services, try to increase security of it to attract more customers to this banking. Most of the bank's effort is inclined to avoid breaking or guessing users' password by attackers. To increase internet banking security, a system which is named "one time password creation system" is replaced to existing system.

One time password is used for one log in or one transaction. One time passwords eliminate most of the old passwords' (fixed passwords) faults. One of the most important of these faults is lack of vulnerability in repeated attacks. With this method, a potential annoying person who has access to one time password in some ways can't misuse it, because this password is invalid.

With the explosion of networks and the huge amount of data transmitted along, securing data content is becoming more and more vital. Data encryption is used to ensure security in open networks. Cryptography is the science or study of the techniques of secret writing, especially code and cipher systems, methods, and the like and is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The principle is to encrypt the message in a way so that an eavesdropper would not be able to read it [3].

Many one-time passwords authentication mechanisms have been proposed for secure authentication over open network environments. These mechanisms help prevent direct wiretapping attacks, reply attacks, and guessing attacks.

The most important purpose of using one time password is making it hard to have access to private information resources for illegal person. While fixed passwords can be stolen or disclosed by illegal person, one time password can be a good supplement for fixed passwords. One of the most important utilization of one time passwords is internet banking systems and electronic business. As the basis of these systems is confidence to others, we need a powerful identification mechanism.

This research's purpose is to introduce effective factors in acceptance of one time password technology to deeper understanding of effective factors on usage of one time password technology. In this research, we question 385 customers of a bank or financial and credit institute and survey effective factors in acceptance of one time password. The main purpose of this research is to introduce effective factors in acceptance of one time password and the subsidiary purposes are banks' survey, electronic banking, security in electronic banking and recognition of effective factors in electronic banking.

II. LITERATURE REVIEW

Innovations mean change in consumers' lives. In fact, innovation adoption often requires changes in consumers' existing habits and forces them to develop new ones [4].This generates innovation resistance which is a normal cons^{umer} response. Typically, the greater change the innovation entails, greater is the consumers' resistance [5].

The most common method used for authentication is static textual password. They are vulnerable to attacks like shoulder surfing, phishing, key logging, Trojan attacks. The studies have shown that normally users use short passwords that are related to their names or date of birth. But unfortunately these passwords can be easily social engineered. Lengthy password can make system more secure but they are difficult to remember [6].

Since passwordsare commonly used to protect accounts with valuable assets (e.g., Bank or Email accounts), they have increasingly been subjected to several attacks, which mainly exploit users' tendency of choosing simple and poor passcodes (e.g., some dictionary words, names, and personal information). Among our interesting findings are how password characteristics change over time and how earlier password practice is understood in current context: the average password length is 9.46 characters, and most of our passwords have the length between 8 and 11 characters; passwords are still dominated by simple structure, and there is a significant increase of using only numbers as passwords, and easy-to-reach symbols are always the first choice when users added symbols into passwords; users prefer to use meaningful data in passwords [7].

Ultimately, the effectiveness of the password as asecurity tool is dependent on the ability of the user toremember it and any failure to remember a password willincrease the cost to the user of following the securitypolicy. This cost could include the set up costs of creating anew password, the social embarrassment of explaining thepassword has been forgotten and the delay or even failureto complete the task for which the password was required.These costs mean that users need to choose passwords thatbest exploit their memory resources.One of the potential constraint upon the security of passwords is the users' knowledge of security appropriate behavior. Users must be aware of a security procedure before they can use it to inform the construction of passwords [8]. Many investigations tried to mitigate it [9] built an application that increases the security of a chosen password by inserting random characters.One-time password systems provide great strengths over conventional passwordsystems: protection against over-the-shoulder, eavesdropping, replay, etc. One of the most cited papers on passwords is [10]. He defines key issues regarding password security.

If we consider electronic banking as making activities electronic, in most of the countries, banks use computer since the 8th decade and so Iran. But the basic concept of electronic banking which was established in 1991 and by existing computers is

costumers can have transaction in electronic space without going to branches. Electronic tools are Automated Teller Machine (ATM), Point of Sales (POS), internet Bank, Mobile Bank, Phone Bank.

The actions taken by banks to hold consumers liable could have possible negative consequences for internet banking usage in general, which could have a costly impact for banks. These consequences can include impact on perceived risk, loss of trust and demand for better security [11].

The popularity of internet banking has led to an increase of frauds, perpetrated through cyber attacks, phishing scams and malware campaigns, resulting in substantial financial losses [12]. Internet banking fraud is among the most lucrative types of cybercrime in contemporary society [13]. Internet banking frauds are difficult to analyze and detect. Because the fraudulent behavior is dynamic, spread across different customer profiles, and dispersed in large and highly imbalanced datasets. Despite the importance of the problem, the development of new online banking fraud decision support system is made difficult by the limited availability of transactions and fraud datasets, due to privacy concerns [14]. Access to internet, anonymity, high speed of propagation, lack of face-to-face contact, free access to services and invaluable contents, also lack of suitable laws and international agreements are among factors that allow threats to spread and make their prosecution hard [15]. The increased sophistication of attacks has complicated prevention and detection efforts, which in turn has allowed their success to proliferate [11].

E-banking relies on network and internet-based environment. As a public network, the internet encounters top confidential and security information. Its nature leads to prominence of threats and various deceits, and development of the dark and ambiguous side of network [15].

Electronic banking causes eliminating cash, reducing traffic, increasing productivity. Government, banks and costumers are the beneficiaries of this technology. But acceptance of every new technology faces resistance of consumers which can be controlled by several factors. Banks encourage costumers to use electronic banking; because electronic banking lead to reducing costs and increasing competitive power and finally electronic banking develops by costumers and businesses acceptance. Modern technologies like mobile technology become inclusive by providing tools for organizations to achieve prominent advantages in productivity, efficiency and other business performance indexes[16].

Surveys were done in 1998 till 2005 used qualitative and exploratory methods to determine causes for lack of electronic banking acceptance by costumers. But in 2005 till 2010 were done by statistical confirmation methods. Because of electronic banking growth, increasing costumers and inclination to use electronic services in recent years, researchers in different countries investigate about effective factors on acceptance improvement and modern technology diffusion. But there is no survey about effective factors on one time password technology acceptance, yet.

There are several researches about electronic banking and acceptance factors but according to searches, there is neither specific research about affective factors of one time password acceptance in Iran nor paper directly.

III. CONCEPTUAL MODEL

In this research, we derived some variables like gender, age, education and … from different basic theories that was accepted and used before. UTAUT model was formulated by Venktash and stands for Unified Theory of Acceptance and Use of Technology. DOI model was developed by Everett Rogers and stands for Diffusion of Innovation. It seeks to explain how, why, and at what rate new ideas and technology spread. Edwin B. Holt developed the SCM theory which stands for Supply Chain Management. The MM theory is a theorem on capital structure, arguably forming the basis for modern thinking on capital structure. The basic theorem states that in the absence of taxes, bankruptcy costs, agency costs, and asymmetric information, and in an efficient market, the value of a firm is unaffected by how that firm is financed.In psychology, the theory of planned behavior (abbreviated TPB) is a theory that links beliefs and behavior and the concept was proposed by IcekAjzen.The Technology Acceptance Model (TAM) is an information systems theory that models how users come to accept and use a technology. It was developed by Fred Davis and Richard Bagozzi.Conceptual model's variables which were used in basic models are:

Table1. Research's variables

No	variable	Model	Author
1	Age	UTAUT	Venkatesh (2003)
2	Education	DOI	Everett Rogers (1962)
3	Risk insensitivity (privacy)	SCT,MM	Edwin B. Holt (1931), Miller and Modigliani (1958)
4	Ease of utilization	DTPB,TAM,SCT,TAM2, MPCU	IcekAjzen (1991), Fred Davis and Richard Bagozzi (1982), Edwin B. Holt (1931)
5	Simplifying conditions	DTPB,MPCU	IcekAjzen (1991), Thompson (1991)

This conceptual model examine variable such as age, education, gender, ease of utilization, privacy and simplifying conditions. In this research, we surveyed factors that have prominent impact on one time password technology. As we discussed, several researches were done on tools and electronic banking services acceptance factors but there is no research about effective factors in acceptance of one time password technology.

- Privacy vs. acceptance of one time password:

Many companies keep sensitive personal information about customers or employees in their files or on their network. Having a sound security plan in place to collect only what you need, keep it safe, and dispose of it securely can help you meet your legal obligations to protect that sensitive data. So we there should be a relation between privacy and acceptance of this technology.

> H1: There is negative relation between increasing privacy and information confidential and costumers' sight to use one time password.

For surveying this question and according to achieved data from Kolmogorov Smirnov test, data is not normal. So we use Spearman correlation coefficient. Achieved correlation coefficient was 0.798 that shows there is a positive and strong correlation between these variables and means the more privacy, the more one time password technology acceptance. Thus, H0 will be rejected and H1 will be accepted. Our findings are accommodated by others' findings that each one believe one reason for using electronic banking services and one time password is increasing trust and security.

- Age vs. acceptance of one time password

The advances in technology for consumers aren't necessarily aimed at young people, but they tend to be the ones who embrace them first. If it's something new and better (and affordable) they want it.

For them, the whole of technology can seem like a giant playground, with its devices like toys to be explored and enjoyed. They're enthusiastic about technology, even if they don't realise it. It's why they want the new video game with great graphics, the latest console – even if they already have others.

> H2: There is a negative relation between age and one time password acceptance.

Contrasting one time password acceptance in different age groups, considering that data was not normal, we use Kruskal Wallis test. As confidence interval was less than 0.05, there is a prominent difference between age groups in one time password acceptance. In the other word, one time password acceptance is different in different age groups. Considering Kruskal Wallis test, for making homogeneous groups, we use Mann Withney test. According to the result of test, we divided customers into 4 groups:

First group: customers who are 20-25 years old that according to average of ranks is the first one in one time password technology acceptance.

Second group: customers who are 26-30 years old that according to average of ranks is the second one in one time password technology acceptance.

Third group: customers who are 31-35 years old that according to average of ranks is the third one in one time password technology acceptance.

Fourth group: customers who are more than 35 years old that according to average of ranks is the fourth one in one time password technology acceptance.

According to Mann Withney test and average of ranks, customers who are 20-25 years old accepted one time password technology the best. Acceptance of one time password by customers who are 26-30 years old is the second, customers who are 31-35 years old are the third and customers who are more than 35 years old are the fourth. As it is obvious, increasing in age results in decreasing acceptance of one time password technology. In the other word, there is a negative relation between age and acceptance of one time password technology. Thus, the second hypothesis will be accepted. Only this research shows that there is a relation between age and acceptance of one time password technology and none of the others' findings consider age or effective impact of it.

> H3: There is positive relation between customers' education and acceptance of one time password technology.

Contrasting one time password acceptance in different educational groups, considering that data was not normal, we use Kruskal Wallis test. Finding shows that there is difference between different educational groups in acceptance of one time password technology. For making homogeneous groups, we use Mann Withney test. According to the result of test, we divided customers into 4 groups:

First group: customers who are MS graduated that according to average of ranks is the first group in acceptance of one time password acceptance.

Second group: customers who are BS graduated that according to average of ranks is the second group in acceptance of one time password acceptance.

Third group: customers who are undergraduate that according to average of ranks is the third group in acceptance of one time password acceptance.

Fourth group: customers who are less than diploma that according to average of ranks is the fourth group in acceptance of one time password acceptance.

According to Mann Withney test and average of ranks, customers who are MS graduated are the first in acceptance of one time password acceptance, customers who are BS graduated are the second, customers who are undergraduate the third and customers who are less than diploma are the fourth. As it is obvious, increasing in education degree results in increasing of one time password technology acceptance. So, the third hypothesis will be accepted.

None of the previous researches show that there is a positive relation between education and acceptance of one time password.

- Ease of utilization including having separated device vs. acceptance of one time password

The technology acceptance model (TAM) is an information systems theory that models how users come to accept and use a technology. The model suggests that when users are presented with a new technology, a number of factors influence their decision about how and when they will use it, notably:

- Perceived usefulness (PU) – This was defined by Fred Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance".
- Perceived ease-of-use (PEOU) – Davis defined this as "the degree to which a person believes that using a particular system would be free from effort" [17].

H4: There is negative relation between ease of utilization and peoples' sight to use one time password.

To test this hypothesis, considering that data was nonparametric, we use Spearman correlation coefficient. According to correlation coefficient (0.759), we conclude that this correlation is strong and positive and means that the more ease of use, the more acceptance of one time password technology by customers. So, H0 will be rejected. This research's findings are accommodated with others' findings that show there is no relation between ease of use and acceptance of one time password technology.

H5: There is negative relation between existing separated hardware and acceptance of one time password.

To test this hypothesis, considering that data was nonparametric, we use Spearman correlation coefficient. According to correlation coefficient (-0.297), we conclude that this correlation is opposite and negative and means that the more separated hardware, the less acceptance of one time password technology by customers. So, H0 will be rejected. Findings of this hypothesis that show there is a negative relation between existing of separated hardware and acceptance of one time password, is not confirmed by previous researches, so, none of them assess the impact and relation of these two variables.

H6: There is positive relation between advertisement andacceptance of one time password.

To survey relation between advertising and acceptance of one time password, considering results of Kolmogorov Smirnov test and abnormal data, we use Spearman correlation coefficient. Results show that there is a relation between advertising and acceptance of one time password. Because of the correlation coefficient (0.740) in 95% confidential interval, relation is strong and positive. Thus, researcher's hypothesis is confirmed and H0 is rejected. None of the previous researches show this relation.

Modern banking paves the way for using costumers' confidential information and even causes different frauds. Solving this problem and increasing security of internet banking, there is a system called "one time password system" as a substitution system. The purpose of this research is determining effective factors on one time password technology acceptance by costumers.

IV. DATA ANALYZE

The purpose of this research is determining effective factors on one time password technology acceptance by costumers. Achieving this goal, we use quantitative approach and descriptive and survey method. Statistical population is costumer who uses electronic services and is familiar with one time password and statistical sample contains 5 selected groups in north, south, center, east and west of "EghtesadNovin" bank. "EghtesadNovin"bank presents banking and financial services by using multi tasked and adapted personnel.

It is bounded to do this in Islamic banking framework and absorb costumers' satisfaction and play an effective role in developing Iran's economic growth. In this research we use accidental method in branches. This research is sectional study and was done in period of time. Thus, time is not considered as a factor. Information is collected by questionnaire that contains effective factors of one time password acceptance by costumers. Measuring each variable, there are indexes which are defined as a question in questionnaire. To make variables quantitative, we use 5 points Likert scale. Measuring variables' stability, we use Cronbach alpha and to analyze data we use SPSS.

Table2. People redundancy who answer questions by age

Age	redundancy	Percentage of redundancy	Cumulative Percentage
20-25	45	11.72	11.72
26-30	174	45.31	57.03
31-35	92	23.96	80.99
>35	73	19.01	100

Table3. People redundancy who answer questions by education

Education	redundancy	Redundancy percentage	Cumulative redundancy
Less than diploma	65	16.93	16.93
Undergraduate	85	22.14	39.06
BS	186	48.44	87.5
MS	48	12.5	100

Model evaluation:

In this research, we show demographic information of people and variables by tables. And for investigating on hypothesis and concluding, we use different statistical methods and tests by SPSS 22. Kolmogorov Smirnov test is for surveying about normal data and we use Spearman correlation test, Kruskal Wallis test, Mann Withney test to examine our hypothesis.

Analyzing data is a multistep process that we gather information by some tools, summarize, categorize and finally processing them that we can use them to examine our hypothesis.

In the table below, we describe the spread of variables in 3 different important indexes: central index (mean), dispersion indexes (variance, standard deviation), spread indexes (kurtosis, skewness).

Table4.Analyse of central, dispersion, spread indexes

variable	mean	Standard deviation	variance	skewness	kurtosis	sample
Acceptance of OTP	3.01	0.857	0.735	0.848	0.681	384
privacy	2.98	0.837	0.701	0.479	0.953	384
Ease of utilization	3.2	0.813	0.661	0.378	0.035	384
Existing of separated hardware	2.66	0.749	0.561	0.759	-0.110	384
advertisement	3.14	0.854	0.729	0.21	-0.240	384

According to table4 we analyze different indexes like this:

1. Mean of acceptance of one time password is 3.01, its standard deviation is 0.875, skewness is 0.848 and kurtosis 0.681. Positive skewness shows that tail of distribution function is long. On the other hand, positive kurtosis shows that shape of variable is higher than normal distribution.
2. Mean of privacy is 2.98, its standard deviation is 0.837, skewness is 0.479 and kurtosis 0.953. Positive skewness shows that tail of distribution function is long. On the other hand, positive kurtosis shows that shape of variable is higher than normal distribution.
3. Mean of ease of utilization is 3.20, its standard deviation is 0.813, skewness is 0.378 and kurtosis 0.035. Positive skewness shows that tail of distribution function is long. On the other hand, positive kurtosis shows that shape of variable is higher than normal distribution.
4. Mean of existing of separated hardware is 2.66, its standard deviation is 0.749, skewness is 0.759 and kurtosis -0.11. Positive skewness shows that tail of distribution function is long. On the other hand, negative kurtosis shows that shape of variable is shorter than normal distribution.
5. Mean of advertisement is 3.14, its standard deviation is 0.854, skewness is 0.21 and kurtosis -0.24. Positive skewness shows that tail of distribution function is long. On the other hand, negative kurtosis shows that shape of variable is shorter than normal distribution.

CONCLUSION

Today banks play a prominent role in different countries' industry and business. So that companies and enterprises' economic activities and commerce are done by banks. Thus traditional banking which causes go to banks and waste time and energy has changed and replaced by electronic banking that costumer can do economic activities by least of time and cost.Modern banking makes dome misuse of private costumers' information which even causes frauds. To solve this problem and increase security, there is a system named "one time password system" to replace these systems. The purpose of this research is to determine factors adoption affecting one time password (OTP) technology by customers. To do this we use quantitative approach and select costumers from 5 different branch of "EghtesadNovin" bank. According to findings, as banks advertise in the way that focus on privacy and advantages of device utilization, can effect customers and encourage them to accept and use one time password device and costumers recognize that one time password covers lots of the old passwords' defects and by using them, make it difficult for illegal person to private information. As findings show there is a positive and significant relation between ease of use and one time password acceptance, so we recommend processes and orders of internet transactions become easier and simpler than before. Also it shows there is a positive

and significant relation between advertisement and announcing and utilization of one time password, so we recommend that appropriate policy should be done for advertising, announcing and creating culture of it. There are two applicable results.As findings show there is a positive relation between ease of utilization and acceptance of it. So, we recommend simplify internet transactions' processes more than before. And the other one, there is a positive relation between advertisement and utilization of one time password. Thus, banks should make decision to advertise for public and inform them.For future studies and researches we recommend that asurvey should be done to compare acceptance of one time password in 2 different banks. By this, we can investigate about banks' growth in technology and customers' inclination to use modern technology. And to survey popularization of these findings to all consumers of Iran's banks, this research should be done in other cities of Iran. Because different cultures causes different behavior and it needs separate investigations. Also this research can be done in different non-profit, governmental banks or creditinstitutes.

REFERENCES

[1] Seung S. Yang, Hongsik Choi (2010). Vulnerability analysis and the practical implications of a server-challenge-based one-time password system, Information Management & Computer Security Vol. 18 No. 2, pp. 86-100.

[2] Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai (2013). A new One-time Password Method, IERI Procedia 4 : 32 – 37.

[3] Geoffrey B. Duggan, Hilary Hohnson, BeateGrawemeyer (2012). Rational Security: Modeling every day password use. International Journal of Human-Computer studies; 70: 415- 431.

[4] Nilsson M, Adams A, Herd S. (2005) Building security and trust in online banking. In: Extended abstracts on human factors in computing systems (CHI '05). New York, NY: ACM Press; pp. 1701–04.

[5] HosseinMohammadi (2015). A study of mobile banking loyalty in Iran. Computers in human behavior; 44: 35-47.

[6] D. Mahto and D. K. Yadav (2015). Enhancing Security of One-Time-Password using Elliptic Curve Cryptography with Biometrics for E-commerce Application. Third International Conference on computer, cpmmunication, control and information (C3IT). P. 1-6.

[7] Chao Shen, Tianwen Yu, Haodi Xu, Gengshan Yang, and Xiaohong Guan (2016). User Practice in Password Security:An Empirical Study of Real-Life Passwords in the Wild.

[8] Geoffrey B. Duggan, Hilary Johnson, BeateGrawemeyer (2012). Rational security: Modelling everyday password use, Int. J. Human-Computer Studies 70: 415–431.

[9] Hiltgen A, Kramp T, Weigold T (2006). Secure internet banking authentication. IEEE Security and Privacy: 21–9.

[10] S. Paul, T. K. Das, P. Saha, R. Hussain and U. Barauh (2015). Comparative Analysis of Two Different System's Framework for Text Dependent Speaker Verification. International Conference on Circuit, Power and computing technologies.

[11] Nicole S. van der Meulen (2013). You've been warned: Consumer liability in Internet banking fraud, computer law & security review 29 : 713-718.

[12] Conor T. MLennan, Philip Manning, Samantha E. Tuft (2017). An evaluation of the game changer password system: A new approach to password security. International Journal of Human-computer studies; 100: 1-17.

[13] Chao Shen, Tianwen Yu, Haodi Xu, Gengshan Yang, Xiaohong Guan (2016). User practice in password security: an empirical stidy of real-life passwords in the wild. Computers and security.

[14] Michele Carminati, Roberto Caron, Federico Maggi, IlenaEpifani, Stefano Zanero (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. Journal of computers and security: 1-12.

[15] Gholam Ali Montazer, Sara ArabYarmohammadi (2015). Detection of phishing attacks in Iranian e-banking using a fuzzy-rough hybrid system. Applied soft computing.

[16] S. Maria UelestinVigila, K Muneeswaran (2012). Key generation based on curve over finite prime field, Int. J. Electronic Security and DigitalForemics, Vol. 4, No. 1.

[17] Agarwal R., Rastogi S., Mehrotra A., (2009). Customers' perspectives regarding e-banking in an emerging economy. Journal of Retailing and Consumer Services; 16: 340–351.

★★★