Examining Incorporated Biometric Systems in Electronic Infrastructures of Banks (Case Study: Mahabad Mellat Bank)

Anvar Tokmechi and Mehran Molavi

Department of Public Administration, Mahabad Branch, Islamic Azad University, Mahabad, Iran
Corresponding author email: dr_molavi1967@yahoo.com

Abstract: As the goal of the present study was to examine the identification systems (biometric) applicable in banks using infrastructures of electronic banking, one can say that the study is applied in terms of the goal. To collect the data use was made by researcher-developed questionnaire. So, the study is that of descriptive and survey-based. The statistical population comprises of public and private banks' clients chosen using simple random sampling method. 262 questionnaires were analyzed. To study the hypotheses, descriptive statistics, Friedman and binomial test were used. The results showed that none of the physiologic biometrics, behavioral and chemical sets was appropriate for electronic banking. The first five prior methods were reported by participants as pal scanning, fingerprint, DNA, iris print, and retinal imaging. In addition, twenty-sixth to thirtieth prior methods were found to be face mobility, physical form of fist and 3D fingerprint, odor sensing, face mobility, and face form.

Keywords: infrastructures of electronic banking, physiologic biometrics, behavioral biometric, chemical biometrics

Introduction

Humankind has always needed to distinguish enemy from friend in order to keep on living and identity realization has been important area. Nowadays, it is attempted to mechanize the identification systems. These progressions exist because of the community and world demand. Such progression reduces the criminals, increases security and gives rise to the tasks accomplishments. In past, fingerprint and face detection ere used, but they are substituted for mechanism-based system.

Biometric is derived from the Greek term bios meaning measuring and is introduced by bio-. A biometric systems is fundamentally an identifying system which constructs the identification components based on particular characteristics, physiologies or behaviors included in a person. The characteristics components are stored following the extraction from database. A biometric system is of high reliability coefficient. Identification involves the comparison of obtained data in particular format and all users within a database. The confirmation involves only the comparison with particular format, so it is essential that the two issues are considered separately (Tagizade, 2010).

Security is one of the main challenges of using information technology in banks and it is given attention. Despite the accomplished tasks to secure the e-baking, these activities have been done as temporarily, island-based and differentiated due to lack of total planning confirmed by policy-maker and it has a long way to achieve optimum status and compatibility with considered standards. Ignorance or carelessness in security can bring about detrimental repercussions on banking network.

Behavioral biometrics

As the name suggests, these metrics measure some of the human behaviors. The first and most common characteristic is the signature. Today, new methods such as typing and other people's voice are used (Hasanabadi, 2007). It is feasible to consider that signature is one of the first approaches of identification. People should draw a picture or compose some lines of writing so that they are compared with the original forums. It is clear that this approach cannot be used in an expanded way. Unavailability of signature sample and human error are among the problems which restricts the usage of this approach. One digital signature is an asymmetric decoding

Chemical biometrics
DNA

In this method, constant DNA data strips are examined to make the identification which is a rapid and accurate method. Sine this method requires that a long time is spent for each sampling and identification, the use of this method is limited and complex (Hatef, 2007, p.71). The temperature reflection of people is an attribute through the examining of which one can access to regular spectrum. This technology can be used for latent identifications. Ultraviolet sensors are expensive

to purchase which causes that little use is made (Jalali & Rajabi, 2008, p. 18).

E-banking is done in the form of economic transactions through the ATM s or telephone, but the internet itself has provided beneficial changing for banks and clients. Rapid and easy access to internet is possible through the day. In addition, banks are enabled to make their services efficient and provide them with less expenses. As an example in case, a normal financial transaction costs one dollar through banking branches and it costs about 60 cents when it is done in online way. E-banking enables the clients to compare the services and products of different banks. This leads to the increase of competition among the banks and banks can enter new markets along with the fact that the geographical area of their service would be expanded, furthermore, one can regard e-baking as building block of undeveloped countries from financial perspective. Clients living in these countries can have easy access to foreign banks through telecommunication systems. These wireless systems are more rapid than traditional communication systems. The other effect of e-banking is that it is not only sensitive to different risks, particularly from legal, executive and prominence perspective, but also it can worsen the conditions of traditional banking in addition to forming new challenges. Many of the officials have changed their policies to achieve their goals in a response to such a phenomenon. These goals include ensuring the security and health of local banking system, improving market policies, supporting the consumer rights and attracting public trust in relation to banking system. Gradually, the policy-makers are informed of the potential effect of major economic policies on capital transformations (Yavari, 2007, p. 23).

Benefits of e-banking

One can consider the e-banking benefits from clients and financial institute's perspectives. One can mention economizing the expenses, economizing the time and access to diverse channels for doing the banking operations from clients' perspective. Characteristics such as establishing and increasing the fame of banks in providing innovation, preserving the clients despite place-base transportations, establishing opportunity to look for clients in considered geographical scope, and providing conditions for complete competition are among the benefits from financial institutes'' perspective. The most important advantages of e-banking are as follows: focusing on new distributing elements, offering modified services to clients and using electronic business strategies. E-banking benefits are considerable from short-term mid-term and long-term viewpoints. Equal completion, preserving and attracting client are among short-term benefits of e-banking. Integrating different components, managing information, expanding the clients' diversity, leading clients to appropriate components with optimum attributes as well as reduction in expenses, recuing transactions process, offering services to clients aiming to form income are among long-term benefits (Amirahmadi, 2010, p. 36).

Security challenge approach in e-banking

The most important challenge of e-banking systems is proving and providing secutiy for transactions. Considering three security elements is important in e-paying system listed as follows:
Identifying security issues of clients
Security of virtual sale in transferring the data from browsers to browsers and leading to banks
Appropriate design of websites and certain encoding
Regarding the fact that security should be run in technical organizational infrastructure and that its implementation is guaranteed in line with paying electronically, one can say that complementing security protocols in different layers is done in a response to three major problems in secure financial context:
Defraud: how one guarantees that the password of client's credit card is not stolen when the client enters the website to do the transaction?
Eavesdropping: how is it possible to guarantee that the information of clients account is not accessible to offenders when the client performs account actions in website?
Changing of information: how one can guarantee that the personal information of client are not changeable by offenders (Kosari Langari et al., 2011).

Research hypotheses

Using behavioral biometrics in banks is more appropriate when accompanied by electronic infrastructure
Using chemical biometrics in banks is more appropriate when accompanied by electronic infrastructure

Study design

The design of the study is that of survey-based. The statistical population comprises of Mahabad banks. 300 questionnaires were distributed randomly among the clients of banks and 262 questionnaires were collected to make analysis. To collect the data, the scale of questionnaire was developed based on types of biometric method known so far. The questionnaire involved 30 items developed on Likert-five item scale.
Using Kolmogorov-Smirnov test, the data can be examined. This test was done on all data and variables individually. This test is done at 95% level of confidence. In other words, the level of significance is $\alpha = 0.05$. Two hypotheses are at work in the study:

H0: data follow normal distribution
H1: data do not follow normal distribution

In case the p value is greater than 0.05, then data are normally distributed; otherwise, the data are said to follow non-normal distribution.

Table 1. The results of normality test related to variables

result	probability	k-s-z	variable
Not normal	0.001	0.077	Using biometric in e-banking
Not normal	0.000	0.103	Using physiologic in e-banking
Not normal	0.000	0.096	Using behavioral in e-banking
Not normal	0.000	0.114	Using chemical in e-banking
Not normal	0.000	0.185	Using other biometrics in e-banking

The results of K-S test shows that variables are not distributed normally, so non-parametric test of hypotheses is used.

Testing the hypotheses
Secondary hypothesis 1

Using physiologic biometrics in banks is appropriate through employing electronic infrastructures

The results obtained from binomial test indicate that iris imaging, retinal printing, finger printing, and palm as well as body vein scanning are appropriate as physiologic methods of identification from clients' perspective while the other methods are not considered appropriate, in addition, the priorities done by Friedman test regarding types of physiologic biometrics show that palm scanning, finger printing, iris scanning, and retinal imaging are ranked as the first four priorities accompanied by lip scanning which is the last priority.

Table 2. The results of binomial testing related to physiologic biometrics

result	Percent of negative responses	Percent of positive responses	The number of negative responses	The number of positive responses	sig	Expected value	components
appropriate	0.33	0.67	86	176	0.000		iris scanning
appropriate	0.36	0.64	94	168	0.000		retinal imaging
appropriate	0.20	0.80	52	210	0.000		fingerprint
inappropriate	0.56	0.44	148	114	0.041		video imaging
inappropriate	0.53	0.47	140	122	0.294		thermal imaging
appropriate	0.12	0.88	32	230	0.000		Palm scanning
appropriate	0.41	0.59	108	154	0.005		Body veins (fingers, wrist, pal, back of hand)
inappropriate	0.98	0.02	258	4	0.000		Lip sign
inappropriate	0.99	0.01	260	2	0.000	50%	Lip mobility
inappropriate	0.98	0.02	258	4	0.000		Lip form
inappropriate	0.98	0.02	256	6	0.000		Skin wrinkles
inappropriate	0.96	0.04	252	10	0.000		Skin thermal property
inappropriate	0.98	0.02	256	6	0.000		Style of smiling
inappropriate	0.96	0.04	252	10	0.000		Skin electromagnetic spectrum (absorption and reflection of photon)
inappropriate	0.90	0.10	236	26	0.000		Sub-nail fibers
inappropriate	0.97	0.03	254	8	0.000		Ear form
inappropriate	0.83	0.17	218	44	0.000		Echo of output sound derived from ear

Table 3. Friedman test related to types of physiological biometrics usable in e-banking

Level of significance	df	Chi-square	number	rank	Mean rank	index components
0.000	16	2495.949	262	1	14.48	(6) palm scanning
				2	14.10	(3) fingerprint
				3	13.38	(1) iris scanning
				4	13.16	(2) retinal imaging
				5	12.43	(7)
				6	11.73	(5)
				7	11.55	(4)
				8	9.11	(17)
				9	7.92	(14)
				10	7.84	(12)
				11	7.00	(15)
				12	6.16	(11)
				13	5.94	(16)
				14	4.90	(7)
				15	4.83	(5)
				16	4.26	(4)
				17	4.20	(17)
				1	14.48	(14)
				2	14.10	(12)
				3	13.38	(15)
				4	13.16	(11)
				5	12.43	(16)
				6	11.73	(7)
				7	11.55	(5)
				8	9.11	(4)
				9	7.92	(17)
				10	7.84	(8) lip sign
				11	7.00	(13) style of smiling
				12	6.16	(9) the quality of lip movement
				13	5.94	(10) form of lip

Secondary hypothesis 2

Using physiologic biometrics in banks is appropriate through employing electronic infrastructures

The results obtained from binomial test indicates that clients prefer signature method as the behavioral method in identification process and are not agree with the other methods. So, one cannot claim that the behavioral methods are appropriate for identification in e-banking. Friedman test results prove this claim. From the clients'' perspective, the signature method is the first rank and the typing method is the last rank of behavioral biometrics.

Table 4. The findings of binomial test regarding the behavioral biometrics

result	Percent of negative responses	Percent of positive responses	The number of negative responses	The number of positive responses	sig	Expected value	components
inappropriate	0.97	0.03	254	8	0.000		Quality of typing
inappropriate	0.91	0.09	238	24	0.000		handwriting
inappropriate	0.67	0.33	176	86	0.000	50%	Voice properties
inappropriate	0.83	0.17	218	44	0.000		Manner of walking
appropriate	0.40	0.60	104	158	0.001		signature

Table 5. Friedman test related to types of behavioral biometrics usable in e-banking

Level of significance	df	Chi-square	number	rank	Mean rank	index components
0.000	4	414.265	262	1	4.19	(22) Signature
				2	3.69	(20)Voice properties
				3	2.58	(19) Handwriting
				4	2.28	(21) Manner of walking
				5	2.25	(18) Manner of typing

References

Amirahmadi, D. (2010). Electronic banking and incoming challenges. Payam Bank, 499, 34-37.

Azad, M; Sepahvand, R; Rahmatinejad, A; Momeni, A. (2011). Examining the fingerprint identification system. Shahid Ashrafi Isfahan University.

Hasanabadi, M. (2007). Identity confirmation technologies. Computer Journal, 167.

Hatef, M. (2007). Biometric, an approach to provide the safety. Journal of Police Human Development, 4(120), 57-81.

Jalali, A; Rajabi Nasab, M. (2008). Biometric, instrument of citizen's security, Karagah, 2(4), 6-31.

Kosari Langari, R; Vahdat, D; Mogadam Cherkeri, N. (2011). Security challenges of electronic system banking.

Tagizade, H; Soltani Fasagondis, Gh; Mehdilo, R. (2010). Investigating the amount of using knowledge management process in service-providing organization. Farasoie Modiriat, 3(12), 33-48.

Yavari, M (2007). Challenges of e-banking revolutions. Journal of Economy, 53, 95-103.