J. Basic. Appl. Sci. Res., 2(9)9152-9160, 2012
© 2012, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System

Seyyede Samine Hosseini[1], Dr. Shahriar Mohammadi[2]

[1]Tehran University, Iran
[2]Khaje Nasir University, Iran

ABSTRACT

The number of transaction frauds and security breaches in traditional security systems such as passwords are rapidly increasing, and the necessity for a strong authentication method become inevitable. Due to the role of customers in progress of banks, and thus in the economic development of countries, banks should provide convenient and more secured banking services to customers. Banks could not meet this aim via using traditional authentication methods such as identification cards and passwords/PIN, because there are many attacks that could be launched against this authentication system. Biometric technology seems to be a perfect solution to defeat these threats. In this paper we review current biometric applications in banking industry in the world, and then the results of this research are presented. Authentication methods using in Iran's banking system and a suggestion for using a biometric model in this system that could help banks operate more securely is presented.

KEYWORDS: Biometric, Banking system, Authentication, Biometric technologies, Security

INTRODUCTION

Technology is in progress in today's world and we can see the presence of electronic services in all financial marketplaces, such as banks. Bank's features in every society caused development in economic and social sectors; hence, it's obvious that banking industry plays an important role in the development of countries. Keeping money, fund transfer, collection and distribution funds, converting currency, and giving facilities are some of the tasks that a bank can do. With the increased use of the internet, traditional ways of giving service to customers have transformed to the ways which almost use internet services.

Using electronic systems in banks and financial institutions is growing rapidly in the world, and the number of users that benefit from electronic services are increasing. Banking operations, related to customers of traditional banking, are all done manually and there are many factors that impact the operations which are depend on human factors and mistakes. Whereas banking operations for other customers can be done via communication channels, in every hour a day and without the need for the physical presence of them in the bank building. Among the advantages of electronic banking we can point to the reduction of the customer's presence in the bank, reduction of bank's physical development, reduction of customer's activity time, increment in the banking operations and customer's convenience, reduction in human mistakes and so on. Due to these advantages, for reducing costs, accelerating the processes and increasing the quality of customer services in addition to elimination of time and place restrictions and expansion of banking activities, the necessity for transforming traditional banking to electronic banking is obvious. Nevertheless, the most important proposed issue related to electronic banking operations, is providing the security of electronic transactions.

The most important asset in a bank is its customers, so banks should provide a high level of security by securing the transactions, to gain the trust of customers. In other word, security of banking operations impacts the adoption of electronic banking by customers. On the other hand, breaches in traditional security systems and banking frauds are increasing rapidly. To reach the aim of securing operations, one solution is to secure banking transactions using a reliable authentication method, the approach can be biometric that seems to be a perfect security solution. In this research, we studied authentication methods used in different banking operations and discussed about 121 banks in the world that benefit from the biometric authentication method. At last, from the point of authentication we reviewed banking system in Iran and offered a biometric authentication model to service customers in a secured way.

1. Banking

In this section we explain some major tasks in a bank system. Several ways to service customers are as below:

***Corresponding Author:** Seyyede Samine Hosseini, Tehran University, Iran, s.hosseini_84@yahoo.com

- **Branch banking**

In this type of banking, to withdraw cash, fund transfer, cash deposit or other banking operations, a customer should visit the teller/cashier in the bank.

- **ATM banking**

Automatic teller machines are terminals which installs by banks to facilitate cash withdrawal, fund transfer, balance check for customers.

- **POS banking**

A point of sale device usually connects via telephone or wireless communication to the bank server, and allows automatic transfer of the purchased amount from the customer's account to the vendor's account. In other word, a point of sale terminal is an electronic device that is used for verifying and processing credit card transactions.

- **Telephone banking**

Telephone banking is a service which allows customers to perform some banking transactions such as checking the balance in hand or fund transfer over the telephone.

- **Internet banking**

This type of electronic banking allows customers to conduct financial transactions in every hour a day and in any location, through a website.

Identity theft is among the financial transactions threats. Identity theft can be defined as abuse of personal data or documents with the purpose of using somebody else's identity and performing illegal acts, for example, abuse of the person's bank account or other securities. Popular types of bank operations like debit and credit card transactions on automated teller machines (ATM) and POS devices are among the most affected by illegal practices [1].

Banking transactions and operations are compromised, due to the growing number of frauds in the world, and the possibility of using illegal practices by criminals and fraudsters who attempt to access customer's account and steal money and other sensitive information. Hence, banks should provide higher security protection for customers, and this can be provided by using a secure authentication method.

2. Different authentication methods

Methods for authentication can be organized into a three basic categories: something the user knows, something the user possesses, and something the user is [4].

- **Something the user knows**

This method relies on secret information that the person being authenticated knows, something like a word, passphrase, and a personal identification number (PIN).

- **Something the user possesses**

Identification card, passport, swipe Card, proximity card, USB tokens, and keys are the examples of the things that a user possesses and can use them to be authenticated.

- **Something the user is**

This method is based on a physical / behavioral feature that is unique to the person being authenticated. Well-known biometric techniques of authentication are fingerprints, voice, iris scan, hand scan, dynamic signature, and hand geometry.

Passwords effectiveness depends on secrecy and it is hard to keep them secret. There are several attacks against this method, such as sniffing, Trojan horse attack, eavesdropping, and also using social engineering, thus it is relatively easy for attackers to find out the passwords. Even if individuals choose hard-to-guess passwords, a user can forget or mistype a password or be obliged to write them down in order to remember it when needed. A written password is, of course, more vulnerable to theft than a memorized one [3].

O'Gorman [5] listed six attacks that can be launched against authentication systems based on passwords and tokens. These attacks are: Client attack (e.g., Guessing passwords, exhaustive search); Host attack (e.g., Plain-text theft, dictionary attack for passwords, and passcode theft for tokens); Eavesdropping, theft and copying (e.g., "Shoulder surfing" for passwords, and theft or counterfeiting hardware for tokens); Reply attack (e.g., Reply stolen password/passcode response); Trojan horse (e.g., Installation of rogue client or capture device); Denial of service (e.g., Lockout by multiple failed authentications).

Biometric authentication, offers a natural and most reliable solution to the problem of person recognition. Since the biometric identifiers are inherent to an individual, it is more difficult to manipulate, share, or forget these traits. Hence, biometric traits constitute a strong and reasonably permanent link between a person and his identity.[4]

3. Banking on biometrics in the world

Although biometric as a good solution to security problems has developed in many industries, it grows slowly in the banking industry. After searching around the World Wide Web, we just found 121 banks in the world which uses biometric technology in their operations and also the information was available on the internet. We listed these banks with the country's name, the used biometric and the related operation in table 1. In the following sections we represent the results acquired from perusing them.

RESULTS

The results shown in the following sections are bringing forth of 121 banks in the world which use biometrics in their operations.

Proportion of deploying biometric-banking in different continents

In figure 1, we can see that among the world's banks that use biometric technology, 52% are located in Asia. The second continent with the majority of banks is America that includes 32% of all.

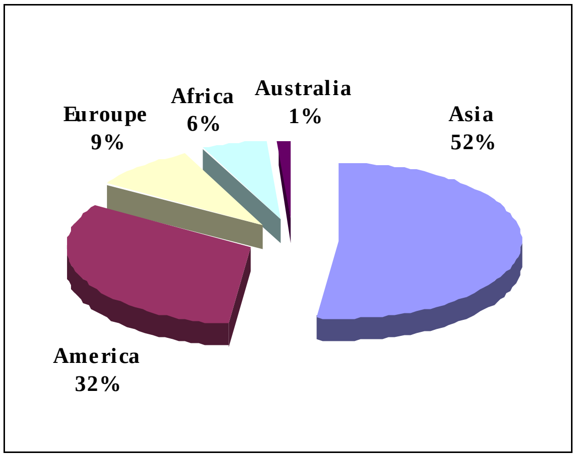


Figure 1- proportion of banking using biometric in different continent (among 121 banks of our survey)

The most used biometric techniques in the world's banks

Figure 2 shows that among the banks in the world that use biometric technology, fingerprint is the most practical biometric techniques. Approximately 48% of the banks of our survey use fingerprint in different operations. The next biometric technologies that used mostly by the banks are finger vein pattern and voice biometric with about 12%. Other biometric technologies with less than 10% are respectively: hand vein, iris, signature, hand geometry, face, keystroke and hand scan.

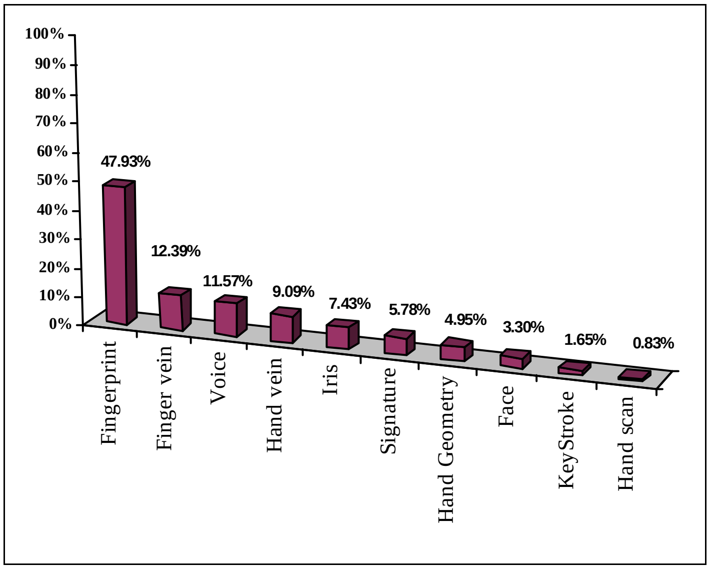


Figure 2- Proportion of used biometric technologies in the world's banks (among 121 banks of our survey)

In the mentioned banks there are different operations performed using biometrics. We categorized these operations into eight groups as it is shown in table 2.

Table 1- list of 121 banks in the world that use biometric

	Bank's name	Country	Biometric	Application
1	Jordan Commercial Bank	Jordan	Iris	Branch banking, ATM, Internet banking
2	Cairo Amman Bank	Jordan	Iris	Branch banking, ATM, Internet banking
3	National Bank of Australia	Australia	Voice	Telephone banking
4	Tallinn Business Bank (TBB)	Estonia	Dynamic Signature	Internet banking
5	Bank Hapoalim	Israel	Dynamic Signature	Branch banking
			Voice	Branch banking, Password/PIN reset
6	First Direct Bank	Israel	Voice	Branch banking, Telephone banking, Password/PIN reset
7	Bank Leumi	Israel	Voice	Password/PIN reset
8	Discount Bank	Israel	Voice	Telephone banking
9	FNB Bank	South Africa	Fingerprint	Branch banking
10	The Credit Bank	South Africa	Fingerprint	Access control (Computer system)
11	Absa Bank	South Africa	Fingerprint	Branch banking
12	Standard Bank	South Africa	Fingerprint	ATM
13	Banco Pichincha	Ecuador	Keystroke	Internet banking
14	Deutsche Bank	Germany	Fingerprint	Access control
15	Sparkasse Bank	Germany	Fingerprint	Access control
16	Dubai Bank	UAE	Hand scan	Access control (Safe deposit)
17	Barclays Bank UAE	UAE	Fingerprint	ATM
18	Banco Azeteca	Latin America	Fingerprint	Branch banking
19	Bank of Central Asia	Indonesia	Fingerprint	Branch banking
20	Danamon Bank	Indonesia	Fingerprint	Biometric smart card
21	Bank Negara Indonesia (BNI)	Indonesia	Voice	Password/PIN reset
22	Boundary Waters Bank	USA	Fingerprint	Access control (Computer system)
23	Kroger Bank	USA	Fingerprint	POS
24	InTrust Bank	USA	Voice	Branch banking
25	E*Trade	USA	Fingerprint	Access control
26	American Express	USA	Fingerprint	Access control (Physical)
27	California Commerce Bank	USA	Fingerprint	Access control (Network)
28	Mellon Bank	USA	Fingerprint	Checking the history of individuals
29	Bank of America	USA	Fingerprint	Internet banking
			Face	Branch banking
30	United Banker's Bank	USA	Fingerprint	Internet banking
31	Western Bank	USA	Dynamic Signature	Branch banking
32	First American Bank	USA	Dynamic Signature	Document processing
33	Chase Manhattan Bank	USA	Voice	Branch banking
			Dynamic Signature	Document processing
34	Shearson-Hamill Investment Bank	USA	Hand geometry	Access control(Time and attendance)
35	Chevy Chase bank	USA	Fingerprint	Access control (Physical)
36	First National Bank Group	USA	Fingerprint	Access control
37	Commerce bank of International (IBC)	USA	Fingerprint	Internet banking, Access control (Network)
38	First Tennessee Bank	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
39	Charles Schwab Bank	USA	Dynamic Signature	Branch banking, Document processing
40	Bank of Currituck	USA	Fingerprint	Access control
41	People State Bank	USA	Fingerprint	Checking transaction history
42	Shinkin Bank	USA	Finger vein	Access control (Server room)
43	Bank of Hawaii	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
44	Bank of Utah	USA	Keystroke	Internet banking
45	SunFirst Bank	USA	Hand vein	Access control (Data center)
46	Zions Bank (Zions First National Bank)	USA	Fingerprint & Hand geometry	Access control (Safe deposit)
			Fingerprint	Check Cashing
47	West Texas National Bank	USA	Fingerprint	Check Cashing
48	Texas Bank United	USA	Iris	ATM
49	Somer Trust Bank	USA	Voice	Telephone banking
50	Banco Ambrosiano Veneto	Italy	Iris	ATM
51	Banco Bradesco	Brazil	Voice	Telephone banking, Password/PIN reset
52	Bank Islam Brunei Darussalam (BIBD)	Brunei	Fingerprint	ATM
53	HSBC Bank	UK	Face	Access control (Data center)
54	Lloyds TSB	UK	Voice	Telephone banking
55	United Bank Limited (ULB)	Pakistan	Voice	Branch banking
56	Credicorp Bank	Panama	Fingerprint	Access control (Physical, safe deposit box), Branch banking
57	Western Bank	Puerto Rico	Fingerprint	Branch banking, ATM, Internet banking
58	FirstBank Puerto Rico	Puerto Rico	Hand geometry	Access control (Time&Attendance)
59	Vakifbank	Turkey	Finger vein	ATM
60	Akbank	Turkey	Iris	ATM
61	IsBank	Turkey	Finger vein	ATM, POS
62	Ziraat Bank	Turkey	Hand vein	ATM
63	Mauritius Commercial Bank	Republic of Mauritius	Fingerprint	Access control (Bank building)
64	Industrial&Commercial Bank	China	Dynamic Signature	Workflow automation
65	China Merchant Bank (CMB)	China	Voice	Telephone banking
66	People's Bank of China	China	Face	Access control (Physical, Treasury)
67	Bank of China	China	Fingerprint	Access control (Physical, Time&Attendance)
68	Nanto Bank	Japan	Hand vein	ATM, Branch banking
69	Hiroshima Bank	Japan	Hand vein	ATM, Branch banking
70	Customers Japan Post Bank	Japan	Finger vein	ATM
71	Mizuho Bank	Japan	Finger vein	ATM
72	Bank of Kyoto	Japan	Finger vein	ATM
73	Sumimoto Mitsui	Japan	Finger vein	ATM
74	Resona Bank	Japan	Finger vein	ATM
75	Joyo Bank	Japan	Finger vein	ATM
76	Juroku Bank	Japan	Finger vein	ATM
77	Bank of Fukuoa	Japan	Finger vein	ATM
78	CITI Bank	Japan	Finger vein	ATM
79	Tajima Bank	Japan	Finger vein	ATM
80	Tokyo-Mitsubishi	Japan	Hand vein	ATM

81	Suruga Bank	Japan	Hand vein	ATM, Branch banking
82	Shinkin Bank	Japan	Hand vein	ATM
83	Ogaki Kyoritsu Bank	Japan	Hand vein	ATM
84	Ikeda Bank	Japan	Hand vein	ATM , Branch banking
85	Norinchukin Bank	Japan	Hand vein	ATM
86	Senshu Bank	Japan	Hand vein	ATM
87	Citi Bank	Singapore	Fingerprint	ATM
88	Pictet&Cie	Swiss	Face	Access control (Building, Time&attendance)
89	Banco Falabella	Chile	Fingerprint	ATM, Branch banking
90	Al Rajhi Bank	Saudi Arabia	Hand geometry	ATM
91	Bank of CostaRica	Costa Rica	Fingerprint	Access control
92	Woori Bank	South Korea	Fingerprint	Internet banking
93	BanCafe	Colombia	Fingerprint	ATM
94	Foreign Trade Bank (FTB)	Cambodia	Fingerprint	ATM
95	BankMed-Lebanon	Lebanon	Iris	Branch banking
96	Podkarpacki Bank Spoldzielczy (PBS)	Poland	Finger vein	ATM
97	Bank Polskiej Spoldzielczy (BPS)	Poland	Finger vein	ATM, Branch banking
98	Reserve Bank	Malaysia	Fingerprint	Biometric card, Online purchase
99	Bank of Cairo	Egypt	Fingerprint	Branch banking
100	Misr Bank	Egypt	Iris	Branch banking
101	Group Financiero Banorte	Mexico	Fingerprint	ATM
102	Banco Azteca	Mexico	Fingerprint	Branch banking
103	Den Norske Bank	Norway	Iris	ATM
104	First Bank	Nigeria	Fingerprint	ATM
105	Royal Microfinance Bank	Nigeria	Fingerprint	POS
106	ABN AMRO	Netherland	Voice	Telephone banking
107	Union Bank of India	India	Fingerprint	ATM
108	ICICI Bank	India	Fingerprint	Access control (Network, Treasury)
109	Indian Bank	India	Fingerprint	ATM
110	Canara Bank	India	Fingerprint	ATM
111	Oriental Bank of Commerce	India	Fingerprint	ATM
112	State Bank of India (SBI)	India	Fingerprint	Access control
113	Central Bank of India	India	Fingerprint	ATM
114	Reserve Bank of India	India	Fingerprint	ATM
115	Punjab National Bank	India	Fingerprint	ATM
116	Dena Bank	India	Fingerprint	ATM
117	Andhra Bank	India	Fingerprint	ATM
118	Syndicate Bank	India	Fingerprint	ATM
119	HDFC	India	Fingerprint	ATM
120	Catholic Syrian Bank	India	Fingerprint	ATM
121	Cooperative&Agricultural Credit Bank	Yemen	Iris	Branch banking, Internet banking, Access control(Time and attendance)

Table 2- Different operations performed using biometrics

	Operation
1	ATM, Biometric Card
2	Branch banking
3	Access Control (Include: Physical access, Building enterance, Deposit, safe and treasure access, Access to network and computer systems, Access to server room and data center, Time and attendance)
4	Internet banking, Online purchase
5	Telephone banking
6	Cashing check service, Reset passwords
7	Checking transaction history of individuals, Document processing, workflow automation
8	POS

Proportion of using biometrics in different operations

As we see in figure 3, about 45% of the banks in the world use biometrics in ATM banking, and approximately 24% of them benefit from this authentication method in their access control systems. Despite the fact that biometric ATMs are the most popular application of biometrics among the world's banks, biometric POS devices have been used only by 2.5% of whole banks of our survey. It is noteworthy that just 10% of the world's banks use biometrics in internet banking.

Using biometrics in the banks of Asia, America, and Europe

Asia:

As we saw in figure 1, Asia with 52%, includes the majority banks using biometrics in the world. Among these Asian banks, the most used biometric technology is fingerprint, since 39% of them use this method. Also, about 19% of the banks use the finger vein pattern to authenticate their users. In addition, the maximum use of biometrics is respectively in ATM banking and branch banking. Approximately 70% of these Asian banks benefit from biometric ATM, about 22% use biometric banking in their branches, and only 8% of them use this authentication method in internet banking.

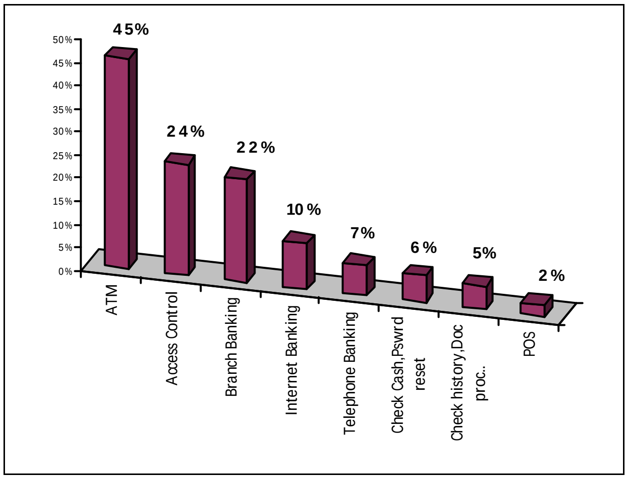


Figure 3- Proportion of using biometrics in different operations

America:

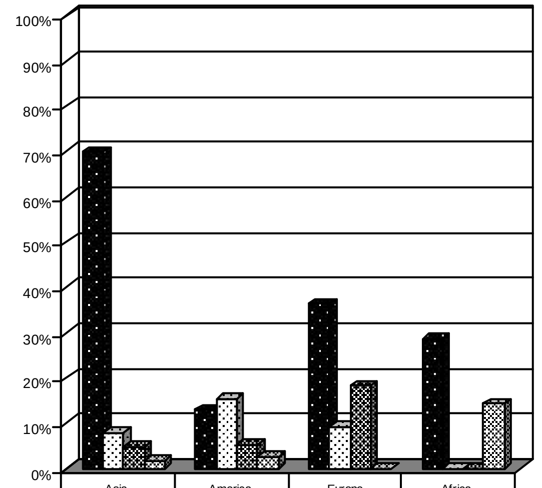
America in the second place includes 32% of the banks deploying biometrics in the world. About 64% of these American banks use fingerprint in their operations. The next biometric technology which used mostly by these banks is hand geometry with about 13%. Among biometric applications in bank environment, access control systems (44%) and branch banking (26%) are the most that American banks use biometrics to perform them. Also 15% of these banks use biometrics in internet banking.

Europe:

Only 9% of the banks in our survey are located in Europe. Each fingerprint, finger vein, iris and face technologies are used by 18% of these European banks for authenticating users. The percentage of using biometric ATMs by the European banks has the highest amount among other biometric operations, where only 9% of them use biometrics in internet banking.

Using biometrics to authenticate customers in major banking operations

Across all the operations that we mentioned before, there are some major banking operations such as: ATM, POS, Telephone banking, and Internet banking, that are electronic banking services, and they can be done without the need of customer’s presence in the bank building. Hence, these electronic transactions may need to be performed more securely, so banks should provide stronger authentication methods in these operations. In figure 4, we see the percentages of biometrics usage in each of these operations in Asia, America, Europe and Africa.



	Asia	America	Europe	Africa
■ ATM	69.84%	12.82%	36.36%	28.57%
□ Internet banking	7.94%	15.38%	9.09%	0.00%
▨ Telephone banking	4.76%	5.13%	18.18%	0.00%
▨ POS	1.59%	2.56%	0.00%	14.28%

Figure 4- Proportion of biometric usage in electronic banking

As it is shown in this figure, we can say that the only development of biometrics in electronic banking is in ATM banking and biometrics in other services like POS, telephone banking and internet banking has not grown yet.

4. Authentication in Iran banks

In this section we describe a banking system in Iran and explain the authentication methods used in this system sectors. To achieve this information we provided a questionnaire and gave it to 21 banks of Iran in Shiraz. In the questionnaire we asked about how they authenticate their customers in different banking operations (Branch banking, ATM, POS, Internet banking, Telephone banking) and also asked about how the employees are authenticated to computer systems, and also time& attendance system. The results in two sections of customers and employees authentication are presented.

Customers' authentication in Iranian banks:

All of these 21 banks use the same authentication methods in different banking operations. How customers are being authenticated in different banking operations is described in this section and is summarized in figure 5.

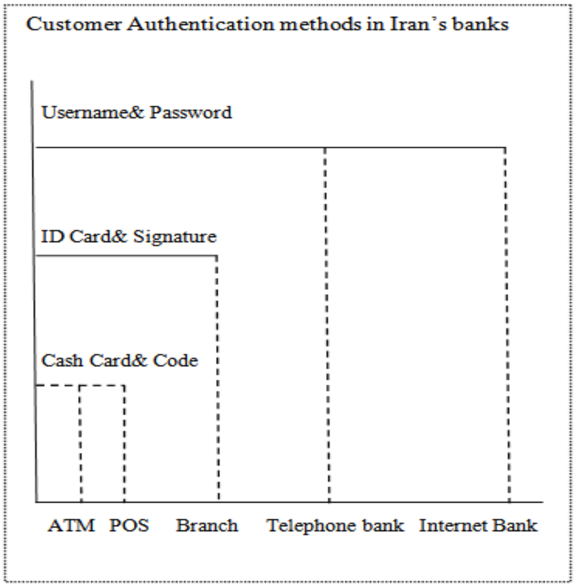


Figure 5- Customer authentication methods in Iran's banks

Branch banking- A customer should visit the bank, communicate with a cashier / teller and fill the bank's form for opening account, payment or withdraw cash, fund transfer, or any other banking operations.

In these activities, customer's identification card and customer's signature will be checked to authenticate him/her.

ATM banking- A customer should first apply for the ATM card, and bank will issue an ATM card with a PIN, for him/her. Then the customer can use ATM terminals, which are installed in different locations, to withdraw cash, fund transfer, pay bills, or purchase phone charge cards.

A customer for authenticating him/herself to the ATM should carry the ATM-card and remember the PIN.

POS- The authentication method in POS devices is the same as in ATM banking.

Internet banking- Customers who request for ATM cards can make online purchases through the internet. Along with ATM card's PIN, bank will give them a second code which they can use it for online purchasing. But to use bank's website for doing banking operations such as fund transfer, pay bills, or print the account reports, customers must first apply for this service. Then the bank will give them a customer number(username) and password, for accessing their accounts via internet.

In an online purchase, a customer will be authenticated with the bank card number, second code, CVV2 code which is engraved on the card and the expiration date of his/her bank card. As we mentioned before in internet banking through the bank's website, a customer will be authenticated via a customer number (username) and password.

Telephone banking- To use the telephone bank, a customer should first request to the bank for using this service, and then the bank will give the customer a PIN. Customers can do some banking operations like checking account balance, fund transfer, pay bills and some other operations via telephone.

In this service, a customer will be authenticated through entering card/account number and the PIN.

Employees' authentication:

All these 21 Iranians banks deploy the traditional method of username and password for authenticating their employees when using computer systems. As it is shown in figure 6, among the 21 banks of our survey 62% of them use fingerprint biometric and other 38% use token for time& attendance of the employees.

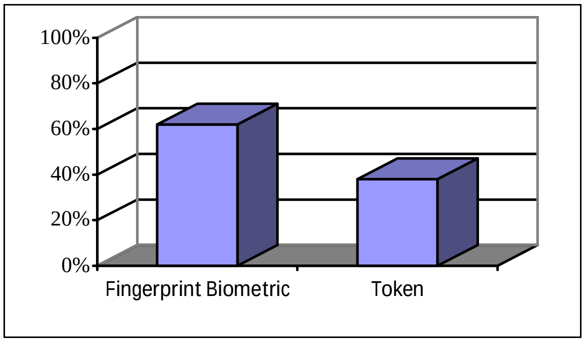


Figure 6- Authentication methods in time& attendance of employees

5. Solutions for improvement of authentication in Iran's Banking System

According to banking on biometrics in the world's banks we discuss about how we can use an authentication biometric model in Iran banking system.

First of all, at the point of opening account, the bank teller should collect customers' biometric traits through a biometric reader. The biometric traits could be fingerprint, finger vein, face, iris, dynamic signature or any other biometric traits that required for doing banking operations. These traits will be stored in the bank's database for later comparisons to authenticate customers.

Branch banking using biometrics- Banks should install biometric scanners in their branches. When customers visit the bank, they go to the counter and authenticate themselves through scanning their biometric traits. If acquired biometric traits through the scanner, match with the customer's template in bank database, customer will be allowed doing banking operations. Fingerprint technology could be a good solution to apply in branch banking, because it is user friendly, high in accuracy, easy to use and its scanners are low-cost [6,7]. Although its security is not too high, but due to the fact that the teller of the bank could check the authentication process, there is no need to use technologies with higher security.

ATM banking using biometrics- Banks should equip their ATMs with biometric scanners. There are two approaches for customer authentication in ATMs: 1) Without the need for carrying bank cards, a customer only is authenticated using biometrics; 2) Along with biometric authentication, customer is authenticated via bank card and PIN. In the second approach, biometric traits of customers should be embedded in their bank cards. Finger vein pattern is a very good biometric solution for ATM banking. Unlike fingerprints, the vein does not leave any trace or information that can be used to duplicate the biometric data and it is completely hidden and unexposed during the authentication process; also it has other advantages such as flexibility, compactness, and extremely high accuracy [8, 9]. So, using finger vein pattern is a good solution to apply in ATM banking in Iran. This method can also be implemented in POS devices.

Internet banking using biometrics- Using majority of biometric technologies in internet banking, requires that customers' computers be equipped with biometric scanners. Since many computers and laptops have webcams and microphones, there is no need to install additional equipments for using voice and face biometrics in online banking. On the other hand, keystroke biometric can be better solution due to the fact that there is no need to even webcams or microphones. Keystroke dynamics is one of several innovative technologies used to automate the process of authenticating an individual based upon a unique, personal behavior, their typing patterns. Using keystroke dynamic in authentication software delivers a solution that is fast, accurate, scalable to millions of users, requires no change in user behavior and is immediately deployable across the Internet without the need for expensive specialized hardware [10]. Hence, keystroke dynamic biometric is a good solution for authenticating customers of internet banking in Iran, and it also can be performed along with the former method of authentication (username and password).

Telephone banking using biometrics- Transactions in this type of banking could be performed through a voice authentication system. Voice capture is not intrusive and Voiceprint is an acceptable biometric in almost all societies. In addition, due to presence of a microphone in phones, there is no need to embed additional hardware into telephones. Whenever a customer wants to do a transaction through telephone banking, his/her voice pattern will be authenticated via a voice recognition system.

6. Conclusion

Since current authentication methods in banking systems, such as passwords and tokens, are not perfect solutions and they don't offer a high level of security, the necessity for a stronger authentication method such as biometric is clear. Although several banks in the world use biometric authentication to represent convenient, fast, and more secured services to their customers, banking using biometrics has not grown yet. Due to this research, only few banks in the world use biometric in their operations. It was shown that most of these banks were located in Asia (with 52%), the most biometric technology that was used by all of these banks in the world was fingerprint and more than other banking operations ATM-banking used biometrics for authenticating customers. Also there was no bank in Iran that deploys biometric technology to authenticate its customers, while implementation of such a biometric model in Iran's banking system will secure bank transactions, provide fast and convenient services for customers, and so the banks could gain the trust of customers. It's obvious that Iranians banks' progress will cause in the economic development of the country.

Recommendation

- All of the banks in Iran should implement biometric authentication systems for all of their banking operations, such as branch banking, internet banking, telephone banking, ATM and POS. Such a system could prevent fraud in banking, and with the increased in security, banks will gain the trust of customers.
- The problems that will be faced during implementation of a biometric system should also be considered. These problems could be the privacy of customers, the costs for implementation of such systems, and system's inability to deal with customers with disabilities.
- Using multi-biometric systems for authenticating can provide operations more secure, instead deploying a single-biometric system. For example the biometric system can check both hand scans and fingerprints of the customers.
- In addition of banks in Iran, the airports of the country can also benefit from biometric technology for authenticating passengers.

REFERENCES

[1] Parusheva, S., 2009. Identity Theft and Internet Banking Protection. Economic Alternatives, issue 1, pp: 44-55.

[2] Thigpen, S. ,2005. Authentication Methods Used for Banking. East Carolina University.

[3] Smith, R.E. ,2002. Authentication: from passwords to public keys. London: Addison-Wesley.

[4] Jain, A., Arun A. Ross, A. and Karthik N. ,2011. Introduction to Biometrics. New York: Springer.

[5] O'Gorman, L. ,2003. Comparing Passwords, Tokens, and Biometrics for User authentication. In the proceeding of IEEE, Vol. 91, No. 12, pp: 2021-2040.

[6] Jain, A., Bolle, R., and Pankanti, S.,1999. Biometrics: Personal identification in networked society. Wellington, New Zealand: Springer.

[7]Srivastva, A., Singh, V. ,2011. Biometrics based identification techniques (BIT). Journal of Global Research in Computer Science, Vol. 2, No. 11, pp:11-15

[8]Himaga, M., Kou, K. ,2008. Finger vein authentication technology and financial applications. In:, Advances in biometrics sensors, algorithms and systems(Eds Ratha,N.K., Govindaraju,V). pp: 89-105. New York: Springer-Verlag.

[9]Edgington, B. ,2007. Introducing Hitachi's Finger Vein Technology: A White paper. <www.hitachi.com>.

Accessed: June 2012, Available at:

http://www.hitachi.eu/veinid/documents/veinidwhitepaper.pdf

[10]BioPassword. ,2006. Authentication Solutions through Keystroke Dynamics. <www.biopassword.com>.

Accessed: June 2012, Available at:

http://www.infosecurityproductsguide.com/technology/2007/BioPassword_Authentication_Solutions_Whitepaper_FINAL.pdf