An application of DEMATEL for transaction authentication in online banking

Ali Sepehri-Rad[a*], S.J. Sadjadi[a] and Soheil Sadi-Nezhad[b]

[a]Department of Information Technology, Electronic Unit, Islamic Azad University, Tehran, Iran
[b]Department of Statistics and Actuarial Science, University of Waterloo, Waterloo, Canada

CHRONICLE	ABSTRACT
	Business trades among individuals, companies, firms, enterprises, and governments are rapidly expelled from their traditional mode, which were mainly based on paper-based exchange, and are geared towards trading through information-based systems. E-commerce has opened up a new field in terms of speed, efficiency, cost savings, and the exploitation of fleeting opportunities. This paper evaluates different authentication methods for online banking in Parsian Bank, which is one of the biggest private banks in Iran. The study designs a questionnaire and distributes it among some experts to find cause and effect factors based on a multi-criteria decision making technique named Decision Making Trial And Evaluation Laboratory (DEMATEL). The study evaluates 12 criteria and divides them into two groups of cause and effect. "Use of mobile systems in authentication methods", "Authentication with fingerprint and smart card", "Authentication with bank card and password", and "Authentication with digital signatures and passwords" are considered as the causative group, while "Authentication with a bank card", "Biometric authentication and disposable codes" and "Authentication with digital signature" are among the effective group. © 2019 by the authors; licensee Growing Science, Canada.

1. Introduction

Security is one of the main challenges in the use of information technology in banks, which is increasing day by day (Broutsou & Fitsilis, 2012). Security negligence can bring irreparable damage to the country's banking network and poses a serious challenge to this area. One of the security domains that is widely used in e-banking is authentication technology (Blount et al., 2004). Many banking operations, such as financial and monetary transactions, account opening, transaction logging, etc., must be performed by authorized people such as bank account holders or their lawyers, or authorized by authorized users and employees (Chumpitaz Caceres & Paparoidamis, 2007). The identity of the requesting bank operation is one of the most important security issues in the field of electronic banking. Today, the banking system is confronted with the authentication of its Internet users and it is difficult to ensure that the user him/herself has used the internet bank, even the OTPs could not solve this problem because by accessing this device any one can use it without the owner's awareness (Al-Qeisi et al., 2014). In other words, authentication plays an important role for the success of the organizations. Transactions in the digital world are

exponentially growing (Bai et al., 2008). Sending and receiving messages, buying and selling goods, transferring money, buying and renting cars, booking flights and hotels are examples of these transactions (Aren et al., 2013). Today, companies have moved most of their own processes, such as marketing, advertising and customer management to the digital world. To do all of these transactions, we often have to create dozens of usernames and passwords that are very difficult to memorize and maintain (Al-Maghrabi et al., 2011).

However, there is still no need to ensure the security of transactions, and there are dozens of different news streams about scams every day due to caches in browsers, unsafe passwords, fake SMS, and so on. Note that today the tools needed to commit cybercrime are commercialized, and even ordinary people can make heavy blows to security systems by using hacking tools that are abundantly available (Ali & Daly, 2010). One of the most attractive areas for hackers is financial systems. What hackers are looking for is the money users carry under uncertain environment. The methods used by hackers are increasingly evolving (Tang & Wu, 2008). Traditional attacks like the Mount Ice Mountain are a small part of the types of attacks available. Bank customers need to change their banking structures and their perceived risks. Security is one of the main challenges in the use of information technology in banks, which is increasing day by day. Security negligence can bring irreparable damage to the country's banking network and poses a serious challenge to this area. One of the security domains that is widely used in e-banking is authentication technology.

Banking operations, such as financial and monetary transactions, account opening, transaction logging, etc., must be performed by authorized customers such as bank account holders or their lawyers, or authorized by authorized users and employees (Feng et al., 2012). The identity of the requested bank operations is one of the most important security issues in the field of electronic banking (Lee et al., 2013). One of the issues of authentication in the Internet bank is associated with the authentication of its Internet users and it is difficult to ensure that the user him/herself has used the internet bank. Even (OTP) cannot solve this problem, because access to this device can be used without the owner of the device. Today, the dynamics and security of a system are measured by authentication, and in reality, a system where authentication is not available is a system of insecurity. This study aims to evaluate and verify the authentication methods for online banking in Parsian Bank, an Iranian private bank.

2. The proposed study

This paper evaluates different authentication methods for online banking in Parsian Bank, which is one of the most private banks in Iran. The study designs a questionnaire and distributes it among some expert to find cause and effect based on a multi-criteria decision making named Decision Making Trial And Evaluation Laboratory (DEMATEL) (Fontela & Gabus, 1976). This technique has been extensively applied in different areas of research (Lu et al., 2013; Dinçer & Yüksel, 2018). Geers (2011), for instance provided some strategic cyber security based on evaluating nation-state cyber attack mitigation strategies with DEMATEL.

In this research, interviews, questionnaires and library method were used to collect data. Accordingly, 2 questionnaires have been used in this research. The questionnaire number 1 was distributed among 8 experts to identify the customer satisfaction and profitability indicators related to the evaluation and selection of transactions authentication for online banking based on Delphi method.

The questionnaire consists of three sections, containing questions about the personal details of respondents, the length of their presence in the banking industry, and the type of service they provide, and the second part is associated with questions related to the subject matter of the research. The third part of the questionnaire is designed in such a way that it is possible to measure the relationship between the indicators of customer satisfaction and various bank profitability with the authentication of transactions for online banking and their impacts on the evaluation and selection of the schemes. This section of the questionnaire was based on Likert's standard in five adjusted options, designed and pre-distributed before

it was distributed to ensure the correct understanding of the questions by the respondents and the elimination of possible doubts. The tool was tested through pre-test.

The second questionnaire is associated with pair comparisons and determines the severity of relationships between customer satisfaction indices and bank profitability related to the evaluation and selection of transaction authentication for online banking. Moreover, the desired satisfaction and profitability indices (the results of the first questionnaire and interviews) were presented to experts in the form of a paired comparison questionnaire (open questionnaire), and they presented the severity of their relationships with each other in a numerical format according to DEMATEL technique. To collect the information on related financial indicators and affecting the evaluation and verification of authentication methods in modern banking, there were approximately 50 managers and experts whose field of activities was in management. Out of the 50 research community, eight experts were selected, two top managers and six senior experts, as a statistical sample of the research. Fig. 1 demonstrates personal characteristics of the participants.
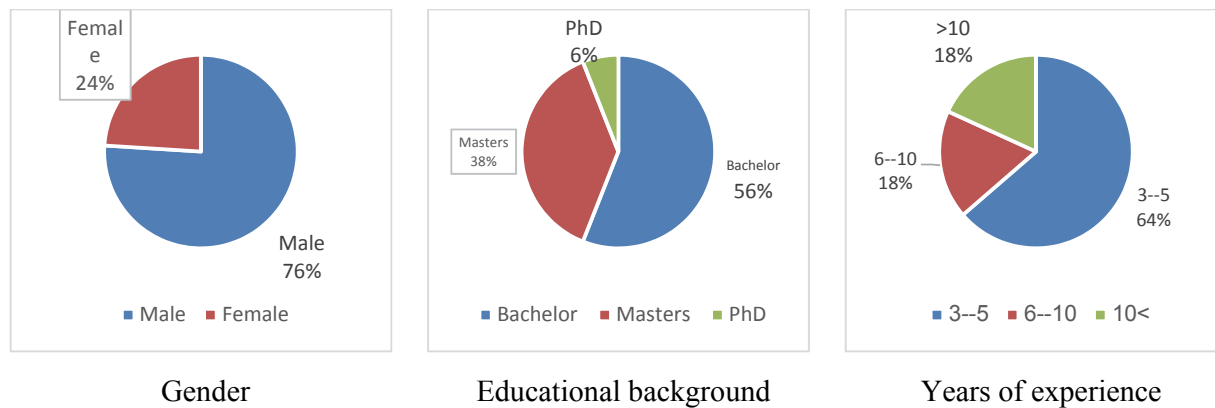

| Gender | Educational background | Years of experience |

Fig. 1. Personal characteristics of the participants

In this survey, Likert scale is used for collecting the measurements where 1 represents "Very low" and 5 denotes "very high". Validity and reliability of the questionnaire were measured based on the experts' feedback and Cronbach Alpha was calculated as 0.86. Table 1 demonstrates the summary of the questions were asked from the experts.

Table 1
The summary of factors authenticating transactions for online banking at Parsian Bank

Row	Description	Symbol
1	Password authentication	A
2	Authentication with digital signature	B
3	Authentication with a bank card	C
4	Authentication using a token (Token)	D
5	Authentication with single-use passwords	E
6	Biometric authentication	F
7	Authentication with 25-pin cards	G
8	Authentication with fingerprint and smart card	H
9	Authentication with bank card and password	I
10	Use of mobile systems in authentication methods	J
11	Authentication with digital signatures and passwords	K
12	Biometric authentication and disposable codes	L

Since there is no choice for the prioritization and, on the other hand, these factors are correlated and their relationships are often nonlinear, therefore, among the methods and techniques of group decision making, DEMATEL technique is the most appropriate method for prioritizing. Fig. 2 and Table 2 show the results of the pairwise comparisons.
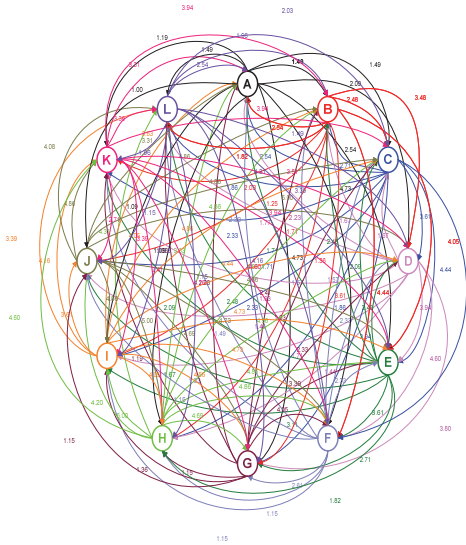

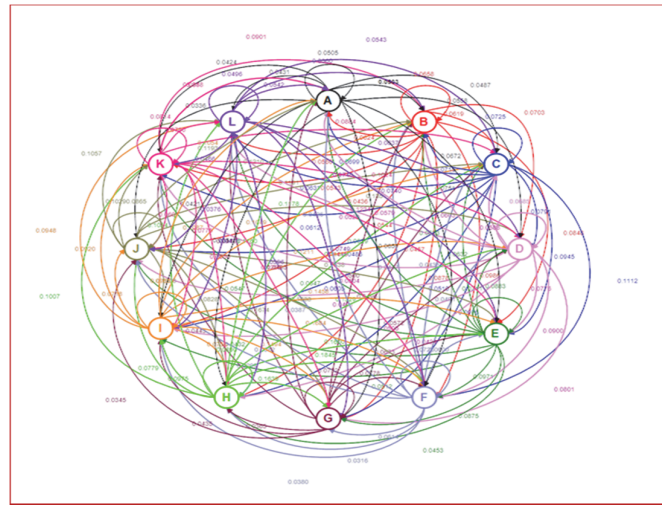**Fig. 2.** The results of pairwise comparison

Fig. 3. The results of the implementation of DE-MATEL technique

Table 2
The results of the case and effect

$\bar{S}_\infty$	A	B	C	D	E	F	G	H	I	J	K	L	Cause
A	0.0505	0.0794	0.0778	0.0966	0.1169	0.1676	0.1576	0.0565	0.0634	0.0531	0.0657	0.0722	1.0573
B	0.1121	0.0658	0.1105	0.1384	0.1639	0.1854	0.1584	0.0724	0.0878	0.0681	0.0940	0.0916	1.3485
C	0.1196	0.1245	0.0725	0.1497	0.1813	0.1882	0.1746	0.0874	0.1061	0.0820	0.1067	0.0996	1.4920
D	0.1034	0.0930	0.0914	0.0685	0.1546	0.1799	0.1543	0.0704	0.0839	0.0682	0.0882	0.0867	1.2425
E	0.0963	0.1119	0.1040	0.1197	0.0883	0.1677	0.1404	0.0809	0.1119	0.0758	0.0956	0.1032	1.2957
F	0.0882	0.0753	0.0742	0.0946	0.1055	0.0723	0.1125	0.0541	0.0605	0.0524	0.0643	0.0678	0.9216
G	0.0940	0.0972	0.0873	0.1028	0.1336	0.1570	0.0732	0.0590	0.0702	0.0570	0.0676	0.0716	1.0704
H	0.1869	0.2130	0.2111	0.2221	0.2551	0.2796	0.2556	0.0890	0.1953	0.1599	0.1907	0.1868	2.4451
I	0.1764	0.1879	0.2000	0.2079	0.2383	0.2609	0.2387	0.1541	0.0965	0.1424	0.1735	0.1611	2.2376
J	0.1841	0.2161	0.2142	0.2329	0.2589	0.2813	0.2591	0.1807	0.1959	0.0865	0.1980	0.1855	2.4930
K	0.1535	0.1671	0.1654	0.1710	0.2003	0.2315	0.2074	0.1123	0.1417	0.1136	0.0814	0.1486	1.8938
L	0.1039	0.0943	0.0940	0.0928	0.1402	0.1698	0.1563	0.0621	0.0702	0.0601	0.0850	0.0496	1.1783
Effect	1.4689	1.5253	1.5024	1.6971	2.0369	2.3414	2.0882	1.0787	1.2834	1.0190	1.3104	1.3242	-----

Table 3 shows the results of ranking of the items using the implementation of DEMATEL technique.

Table 3
The results of the causes

D(A)	D(B)	D(C)	D(D)	D(E)	D(F)	D(G)	D(H)	D(I)	D(J)	D(K)	D(L)
1.0573	1.3485	1.4920	1.2425	1.2957	0.9216	1.0704	2.4451	2.2376	2.4930	1.8938	1.1783

Therefore, we have
D(J) > D(H) > D(I) > D(K) > D(C) > D(B) > D(E) > D(D) > D(L) > D(G) > D(A) > D(F).

Moreover, Table 4 shows the results of the effects,

Table 4
The results of the effects

D(A)	D(B)	D(C)	D(D)	D(E)	D(F)	D(G)	D(H)	D(I)	D(J)	D(K)	D(L)
1.4689	1.5253	1.5024	1.6971	2.0369	2.3414	2.0822	1.0787	1.2834	1.0190	1.3104	1.3242

Therefore, we have

D(F) > D(G) > D(E) > D(D) > D(B) > D(C) > D(A) > D(L) > D(K) > D(I) > D(H) > D(J)

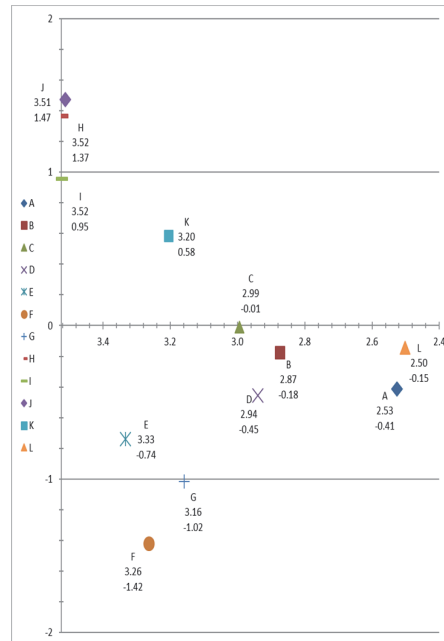Finally, Fig. 4 shows the results of the cause and effects associated with online authentication.

Fig. 4. The summary of the cause and effect

In summary, we determine 4 factors as causes and 8 effective factors summarized in Table 5 as follows,

Table 5
The summary of the cause and effect factors

	Causative factors		Effective factors
J	Use of mobile systems in authentication methods	C	Authentication with a bank card
H	Authentication with fingerprint and smart card	L	Biometric authentication and disposable codes
I	Authentication with bank card and password	B	Authentication with digital signature
K	Authentication with digital signatures and passwords	A	Password authentication
		D	Authentication using a token (Token)
		E	Authentication with single-use passwords
		G	Authentication with cards with 25 pin codes
		F	Biometric authentication

According to the results, we can conclude that the use of mobile systems in authentication methods has the most influence on other factors. After that, fingerprint and smart card authentication, authentication with bank cards and passwords, authentication with digital signatures and passwords are in the next lower priorities.

4. Conclusion

In this paper, we have presented an empirical investigation to determine the cause and effect factors in online banking system. The survey has designed some questionnaires in Likert scale and distributed among experts who were enrolled in management levels of a private Iranian bank. The results have been

analyzed using DEMATEL technique and determined four causative factors including "Use of mobile systems in authentication methods", "Authentication with fingerprint and smart card", "Authentication with bank card and password" and "Authentication with digital signatures and passwords". The study has also determined eight effective factors influenced on online banking such as "Authentication with a bank card", "Biometric authentication and disposable codes", "Authentication with digital signature" and "Password authentication". Considering the location of the research area and its statistical community, it is noted that the results are related to the Parsian Bank's credit department and may be different in other banks and credit institutions of the country as well as internationally. Therefore, the results of this study could be cautiously considered for other banks. Moreover, the authentication technique is growing rapidly and new methods and techniques will be introduced in future. Therefore, this study needs to be updated in future.

References

Ali, A., & Daly, K. (2010). Macroeconomic determinants of credit risk: Recent evidence from a cross country study. *International Review of Financial Analysis*, *19*(3), 165-171.

Al-Maghrabi, T., Dennis, C., Halliday, S. V., & BinAli, A. (2011). Determinants of customer continuance intention of online shopping. *International Journal of Business Science & Applied Management*, *6*(1).

Al-Qeisi, K., Dennis, C., Alamanos, E., & Jayawardhena, C. (2014). Website design quality and usage behavior: Unified Theory of Acceptance and Use of Technology. *Journal of Business Research*, *67*(11), 2282-2290.

Aren, S., Güzel, M., Kabadayı, E., & Alpkan, L. (2013). Factors affecting repurchase intention to shop at the same website. *Procedia-Social and Behavioral Sciences*, *99*, 536-544.

Bai, B., Law, R., & Wen, I. (2008). The impact of website quality on customer satisfaction and purchase intentions: Evidence from Chinese online visitors. *International Journal of Hospitality Management*, *27*(3), 391-402.

Blount, Y., Castleman, T., & Swatman, P. (2004). Employee development strategies in the B2C banking environment: two Australian case studies. *ECIS 2004 Proceedings*, 3.

Broutsou, A., & Fitsilis, P. (2012). Online trust: the influence of perceived company's reputation on consumers' trust and the effects of trust on intention for online transactions. *Journal of Service Science and Management*, *5*(04), 365.

Chumpitaz Caceres, R., & Paparoidamis, N. G. (2007). Service quality, relationship satisfaction, trust, commitment and business-to-business loyalty. *European Journal of Marketing*, *41*(7/8), 836-867.

Dinçer, H., & Yüksel, S. (2018). Financial Sector-Based Analysis of the G20 Economies Using the Integrated Decision-Making Approach with DEMATEL and TOPSIS. In *Emerging Trends in Banking and Finance* (pp. 210-223). Springer, Cham.

Feng, T., Liu, Z., Kwon, K. A., Shi, W., Carbunar, B., Jiang, Y., & Nguyen, N. (2012, November). Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*(pp. 451-456). IEEE.

Fontela, E., & Gabus, A. (1976). The DEMATEL observer.

Geers, K. (2011). *Strategic Cyber Security: Evaluating Nation-state Cyber Attack Mitigation Strategies with DEMATEL*. Tallinn University of Technology.

Lee, H., Zhang, Y., & Chen, K. L. (2013). An investigation of features and security in mobile banking strategy. *Journal of International Technology and Information Management*, *22*(4), 2.

Lu, M. T., Lin, S. W., & Tzeng, G. H. (2013). Improving RFID adoption in Taiwan's healthcare industry based on a DEMATEL technique with a hybrid MCDM model. *Decision Support Systems*, *56*, 259-269.

Tang, C., & Wu, D. O. (2008). An efficient mobile authentication scheme for wireless networks. *IEEE Transactions on Wireless Communications*, *7*(4), 1408-1416.