Towards a More Secure Mobile Banking System: The case of Iran

Sepideh Mollajafari

Professor Kamal Bechkoum

DOI: 10.29322/IJSRP.8.7.2018.p7960
http://dx.doi.org/10.29322/IJSRP.8.7.2018.p7960

Abstract- Mobile devices have penetrated most aspects of our daily life activities ranging from the hedonic to utilitarian use. Businesses have invested in benefiting from the opportunities offered by the pervasive nature of mobile technologies to enhance their products and services and therefore improve their customers' satisfaction. The banking sector, in common with other industries, has invested in such mobile solutions to facilitate banking transactions for both themselves and their customers. The growth of mobile banking provides significant benefits in terms of delivery speed and quality of services to customers. However, like other technologies mobile banking faces several challenges, in particular security. This paper addresses the main factors that affect the usage of mobile banking transactions and the related security issues, with a particular emphasis on the case of the Iranian banking system. After a thematic analysis of qualitative data we were able to identify the main factors that affect both mobile banking security and usage, namely: security level, security threats, security policy and standards, transactional risks and awareness. As a result, this study proposes a framework that explains the relations among these factors with a view to enhance the understanding of the current status of such technology.

Index Terms- mobile technology, mobile banking, information security

I. Introduction

Wide-expansion of information technology and telecommunication systems and also collaboration between mobile operators and banks have reshaped traditional banking services and offered new ways for banks to interact with their customers. The pervasiveness of technology and the rapid growth of mobile commerce led to a greater innovation in the banking system. Developments in mobile and telecommunication technologies such as Implementation of new operating systems, availability of wireless network, improved hardware capabilities, user-friendly web browsers have revolutionised the way people use mobile devices in their daily life.

These developments have enabled mobile banking to provide significant benefits in terms of delivery speed and quality of services. However, these advantages come with challenging security threats. The provision of mobile banking requires data to travel over networks, or to be saved on banks' server databases and mobile devices (Narendiran, Rabara & Rajemdran, 2008), which can pose a security risk that needs to be handled properly.

Developing countries, such as Iran, are not immune to this increasingly prevalent use of mobile devices. Flexibility and convenience of use by these devices are an important reason for their attaractiveness. Mobile clients are able to transfer funds between accounts, to make electronic payment, to request and receive information about a personal account by using applications installed on their mobile devices (Elkhodr *et al*., 2012). Mobile banking transactions can be exposed to risks at different levels of the "supply chain". That is because customers, banks, network providers and other parties are all involved in this service (Ghotbi and Nassir Gharechedaghi, 2012).

It is therefore imperative that banks and other service providers ensure an acceptable level of security that protects the customer's sensitive information. This paper looks at security challenges of the private mobile banking system in Iran and provides a framework that improves the understanding of such systems by identifying particular factors and their relations and impact on confidentiality, integrity and availability of the service. For this, and in addition to these introductory notes, section two covers the existing work in relation to mobile banking and security issues. The section deals with mobile banking security challenges and barriers in Iran and developing countries. The Iranian bank structure is explained, before outlining the security challenges and barriers in online banking and mobile banking in Iran. Section three describes research findings and data analysis and explains the result. The proposed mobile banking risk management framework is presented in section four. Finally, we discuss the conclusions and future work in section five.

II. Mobile Banking and Security Issues

Mobile banking service refers to a set of applications that enable people to use their mobile device to manipulate their digital banking service. Nie and Hu (2008) mentioned that mobile banking has two security zones: a mobile security zone and a banking security zone. Different security challenges are associated with each zone, as depicted in figure 1.

Figure 1 Security Zones of Mobile banking (Nie and Hu, 2008)

Khan *et al.,* (2015) state that the security risks associated with mobile devices include:

1. High-level of risk in data loss through losing mobile devices or interruptions by malicious applications

2. Multiple User Logging
3. Weak Authentication
4. Client Side Injections
5. Application-Based Threats (malware, spyware)
6. Network-Based Threats (Operating system, MMS, SMS, WI-FI)
7. Web Based Threats (Browser Exploits, Phishing Scams) Mobile Vulnerabilities (Trojan Horse, worm, botnet, social engineering) Lack of maturity of fraud tools and controls (lack of adequate monitoring, detection or prevention tools)

Mitigating against the above risks requires a multi-facetted endeavour involving creating mobile device security policies, increasing awareness about risks associated with the use of mobile devices, providing authorised access to sensitive data, and continuous monitoring and assessment of the vulnerability risk of all devices.

Other security risks emanate from the physical mobile network infrastructure itself. Mobile network weaknesses and transport frequencies have their own security challenges as listed by (Islam, 2014):

1. Wireless carrier infrastructure
2. Weakness of global system for mobile communication (GMS)
3. SMS vulnerabilities (clear text on mobile network)
4. SIM attacks
5. HTTP, WAP, TCP/IP, OTA, USSD, Bluetooth

The above presents only one element of the security component. The other element is related to how the infrastructure is organised within the bank itself. Khan *et al.,* (2015) claimed that the security risks associated with the bank side include:

1. unsecure design and implementation of hardware, software and networks
2. Poor application design and configuration
3. weak telecommunication infrastructure
4. poor e-commerce security system and fraud prevention
5. poor client authentication mechanisms
6. use of unsecure algorithms for data encryption
7. lack of adequate implementation of digital payment security protocols
8. lack of physical security at data centres
9. weak database backup and recovery mechanism in unexpected situations (network failures, radio failures and natural physical disasters)

The above security challenges do not apply specifically to any geographical area. However, they pose a particular difficulty for developing countries trying to set up a secure mobile banking service. The barriers and obstacles facing developing countries in this context are very well documented (e.g: Alafeef *et al.,* 2012; Rumanyika and Mashenene, 2014). We list here some of the main ones:

1. Lack of network and telecommunications Infrastructure
2. Lack of sufficient system security
3. Legal barriers
4. Economic barriers
5. Social-cultural barriers
6. Political barriers
7. Insufficient knowledge of IT and lack of training

In attempting to address these barriers efforts are made to improve the security of financial transactions; for example, the Mediterranean Partner Countries issued a set of Banking Supervision Rules, which identifies the cyber security controls that banks must follow. Each country's Central Bank is responsible for monitoring and ensuring the security of payment systems and related standards (European Investment Bank, 2012). In addition, most developing countries have established security policies and standards for addressing information security risks and maintaining data confidentiality, integrity, authentication and non- repudiation (Jin and Fei-Cheng, 2005).

A. The Mobile Banking System in Iran

In 2003, SHETAB (Interbank Information Transfer Network) was introduced to handle Automated Teller Machine **(**ATM), point of sale purchase (POS) and other card based transactions between all financial organisations and banks all over Iran. Today, most banks are interconnected through the SHETAB system and they have access to some parts of customers' account information. This interconnection has created a path for mobile banking to become the next big phenomenon in the Iranian banking system (Central Bank of Iran, 2016).

The Iranian banking sector includes public banks, private banks and private financial institutions. Central Bank of Iran (CBI) is responsible for the design and implementation of monetary and credit policies, and the supervision of public and private banks and other financial institutions. Private banks provide high quality services and standards at lower cost in order to create a competitive advantage in global banking systems (Peymane, 2014). It is widely believed that they have been more successful than the public banks in service delivery and in the introduction of modern banking systems.

The National informatics Corporation (NIC) has cooperated with the Central Bank of Iran since 1990. NIC is a holding company with several subsidiaries including the Informatics Service Corporation (ISC), Shaparak electronic card Payment Company, Kashef Banking Security Governance Company and Fardis Alborz Info Corporation. All these companies have been established under central bank supervision. The aim of cooperating with these companies is to offer reliable online banking services and implement effective cyber security requirements for protecting data confidentiality, integrity and availability (National Informatics Corporation, 2011).

Informatics Service Corporation (ISC) implemented Information Security Management Systems (ISMS) based on international standard ISO/IEC 27001. The aim is to enhance secure electronic banking services and minimise security breaches (Way2pay, 2014).

In addition, other Iranian banks were awarded the ISO/IEC 27001 security certification in Online Banking and Mobile Banking (Informatics Service Corporation, 2016). As with other parts of the world, Iran faces similar barriers in its quest for implementing an effective and secure mobile banking system. An audit of existing work (e.g. Ghotbi and Nassir Gharechedaghi,

2012; Ghazinoory *et al*., 2016; Charkhandaz, 2014) has identified a number of barriers affecting the implementation of an effective mobile banking system/service in Iran. Such barriers include:

1. Inappropriate technical infrastructure such as telecommunication networks, hardware and software
2. Low speed of communication network
3. Weak internet connection and low bandwidth with high cost
4. Poor mobile phone coverage
5. High cost for upgrading current telecommunication networks and infrastructures
6. Lack of a policy making body
7. Lack of legal regulation with standardised procedures in the field of mobile Banking
8. Political challenge and some limitations to the use of credit cards and international corporation due to sanction

In order to have an appreciation of the risks associated with the varied nature of the challenges inherent to mobile banking in Iran there is a need for a risk assessment framework that enables managers in the banking sector to be in a position to make informed decisions about risk mitigation. The next section explains how the framework was designed.

III. Designing the Framework

We used a combination of primary and secondary data collection techniques. In addition to an investigation into existing work some qualitative interviews were conducted with six IT bank managers, who were selected by subjective sampling from three different private banks in Iran (two from each bank).

The findings reveal some information about the usage and nature of mobile banking, in addition to a number of security challenges and obstacles that are already present in the mobile banking system in Iran.

A. Research finding

The findings confirm that mobile banking provides a new opportunity in terms of delivery speed and quality of services to customers. However, these advantages come with several security issues that customers are concerned about. With regard to the barriers and security challenges in Iran, CBI and Fardis Alborz Company could address the technical problems by providing more advanced banking IT infrastructure. Moreover, the government's cooperation with internet service providers and network service providers could be useful in improving internet connection speed and coverage and providing an appropriate network and communication infrastructure. Furthermore, the CBI should pay closer attention to bank operations when it comes to applying security policy and standards in online banking and mobile banking, and enforce a greater adherence to policy and standards.

One of the findings of this study is the negative effect that previous Western sanctions had on Iran, which resulted in slowing down development in the information technology sector. It was not permissible to set agreements with some well-known IT companies such as IBM, Oracle, CISCO and HP. Organisations (including banks) were unable to import any advanced equipment or software. This is in addition to difficulties in signing agreements to install security protection software and other related applications such as firewalls and anti-viruses. This research recommends that both Iranian government officials and banking sector officials utilise the recent lifting of sanctions to enter into negotiations with international companies such as those mentioned above, and to import new updated and advanced tools and equipment to enhance the protection of privacy and security within the banking sector in Iran. This will enable customers to have greater trust in the banking service and will therefore lead to greater use of the service, and will in turn benefit both banks and customers in terms of efficiency and effectiveness.

According to the findings, many factors can affect customer's trust for mobile banking such as reliability, cost and ease of use (convenience), technological barriers and security issues.

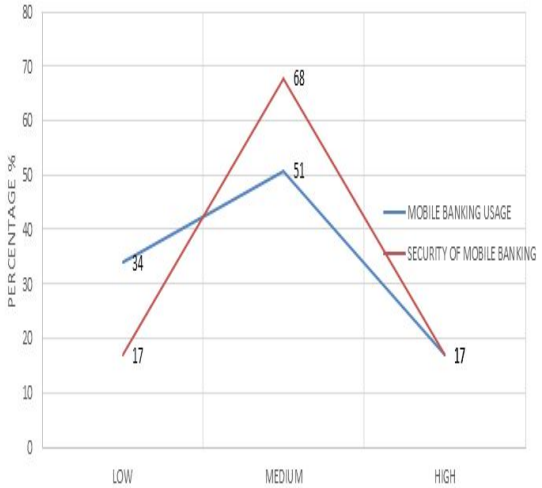

Figure 2 Relationship between the security level and the usage of mobile banking

Figure 2 shows that just over half of all interviewees (51%) mentioned that the usage rate of mobile banking services by bank customers were a medium rate. However, 34% of participants mentioned that they have low level of security to secure this service because some administrative and technical issues. The remaining 17% claimed that the mobile banking services offered by their banks have high adoption rate by their customers. After comparing the usage data to the security level data, it showed that there is a strong relationship between these two factors. When the security level is high the usage rate is high too.

The above confirms that security plays a significant role in the adoption of mobile banking. It should be noted that perception of security influences trust and affects the mobile banking usage. Banks need to develop customer trust by Improving security measures, training employees and making customers aware of security risks.

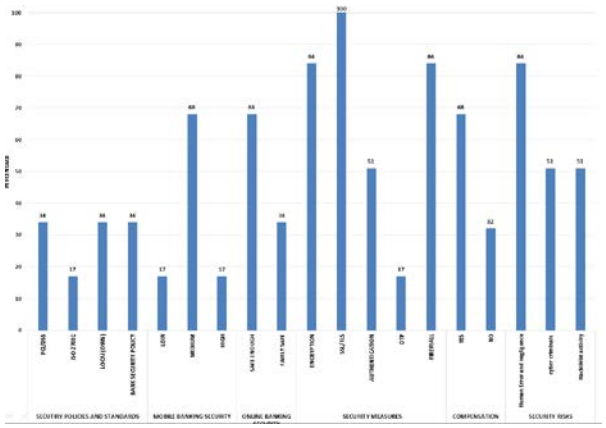

Figure 3 Percentage of mobile banking and online banking security in three private banks in Iran

Figure 3 shows the percentage of security policies and standards, mobile banking security, online banking security, security measures, compensation and security risks in three private banks in Iran. According to the chart, many attacks are possible during mobile banking transactions. Roughly, 68% of participants agreed with medium level of security in mobile banking services and the same percentage given for safe enough transaction in online banking. Another security issue is the absence of unified standards/Protocol or agreed policy to manage and control the mobile banking security among the Iranian banks. There is a difference in using security policies and standards, for example, only 17% of participant mentioned that they followed international security policies and standards such as ISO27001, while 34% of respondents mentioned PCI/DSS. The remaining participants confirmed that they follow CBI and local bank policies and standards.

There is also evidence for some security challenge related to cryptographic mechanisms and authentication methods, which are very important security measures to mitigate the threat of mobile banking. Comparing to banks in developed countries, they use some advanced authentication methods such as fingerprint, passcode generators and one-time-passcode (OTP).
Based on the above findings a framework was put together to help with understanding current security issues and barriers of mobile banking in Iran. The next section gives a brief description of this framework.

IV. Risk Assessment Framework

The framework aims at facilitating and managing the risks of mobile banking services in Iran. The focus is on security objectives such as confidentiality, integrity and availability of mobile banking services in private banks.

The framework also attempts to improve the usage rate of mobile banking by covering aspects such as security policy and standards, perceived security level, security measures, transactional risks and security awareness.

The different elements of the proposed risk assessment framework are shown in figure 4.

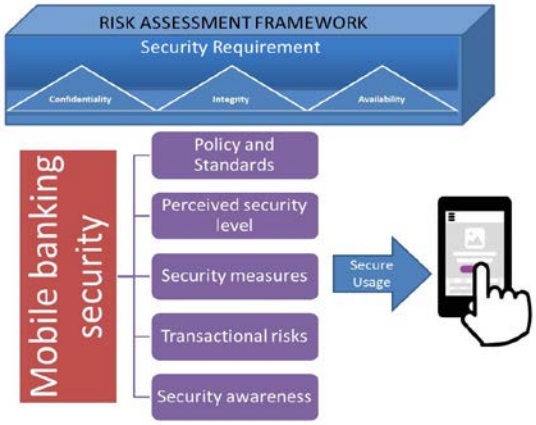

Figure 4 Risk assessment framework

A. Security policy and standards

In order to protect information resources, banks need to implement high-level management instructions and rules to manage and organise banking transactions.

As mentioned above, the CBI established the Kashef Company recently as a policy maker for designing information security standards (Kashef, 2016). However, many banks and financial institutions are using their own standards and policies and they do not follow CBI security policy and standards or even international information security policy and standards. CBI could support banks and financial institutions to evaluate their risks and choose an appropriate level of security measures and technological infrastructure.

In addition, CBI should manage and control all banks' security policy and standards and enforce CBI policy or international standards.

Perceived security level

Customers' perception of security and privacy are factors that affect mobile banking usage. Security is a combination of controls, technologies, standards, methods and measures that are used to secure a particular system and ensure confidentiality, authentication, integrity, authorisation and non-repudiation (Akbari, 2013). There are several non-technical mechanisms such as policies, strategies, and information listed on websites, which represent ways to overcome the security threats facing such services (Law, 2007).

We found that the main concern that participants cited about mobile banking is trusting the security of accessing financial data on a mobile device. 68% of participants claimed the overall rate of mobile banking security for protecting customer's information was at a medium level. In addition, they gave the same percentage for 'safe enough transaction' in online banking, while 34% were not sure of the security of online banking. Therefore, customers' perception of a lack of security is one of the obstacles to mobile banking use in Iran.

Security measures

Security measures should make it easy to implement, manage and operate defensive controls to detect and stop attacks in the banking sector.

In order to protect customer information and address security challenges and fraud management in the banking industry, researchers recommend a few security measures, including: (Akbari, 2013; Luvanda, 2014; Cognizant, 2014)

1. Implement Intrusion Detection Systems (IDS)
2. Implement physical security measures such as firewalls
3. Implement malware and virus detection and protection methods, system auditing controls, patch management, back up servers
4. Monitor and evaluate security controls
5. Track mobile banking transactions
6. Control physical access to databases and servers
7. Upgrade management software and system security
8. Apply real time detection services
9. Check Operating System security periodically
10. Carry out data validation to verify uncorrupted transmission

Transactional risks

Banks and financial institutions use different types of technology such as Short Messaging Service (SMS), Unstructured Supplementary Service Data (USSD), Wireless Application Protocol (WAP), Near Field Communication (NFC) and mobile applications to offer mobile transactions.

Some Iranian banks offered simple services via SMS, which can pose security problems during data transmission. Furthermore, USSD is another method for providing mobile banking transactions in some private banks in Iran. This is not necessarily a safe technology, because communication could be interrupted while the data is travelling between the USSD gateway and the information server. Fortunately, CBI has managed and minimised this risk by limiting the value of transactions that can be performed over USSD. They should, perhaps, focus on mobile banking applications, which provide a more secure type of transactions.

In any technology-based transaction, the possibility always exists that the transaction does not take place as expected or in a timely manner, which can represent a transactional risk that a bank needs to protect itself from. For instance, any delay in a transaction can make customers nervous about security and affect their perception of mobile transactions. The risks associated with this service includes network risks (Man-in-the-middle attack, network snooping, Bluetooth, Wi-Fi, automatic backup of sensitive data to a cloud), observation risks (information or passwords being observed while a device is being used), device risks (theft, loss, malware, hacking, access by unauthorised person, storage of sensitive data without encryption) and remote service risks (Web site) (Trewin *et al*., 2016).

Banks and financial institutions should identify the security risks and promote secure requirements to mitigate against transactional risks in mobile banking services. Some of this could be done through training and awareness as explained in the next section.

Security awareness

The human factor is hugely important in the security chain. This research found that lack of technical education and general awareness amongst banks' employees, as well as lack of security awareness amongst customers were key barriers to the Iranian banking system. Whilst the creation and maintenance of secure information systems is crucial for banks' credibility, they also need to be aware of mistakes or oversights by their employees and other users of their systems (PCI Security Standards Council, 2014). Therefore, it is important that banks and financial institutions have a security awareness and continuous training programme in place, aimed at both employees and users of the services.

CBI, banks and financial institutions need to establish security awareness teams for creating and maintaining security awareness programmes based on three levels: in-depth security awareness; intermediate security awareness for specialised roles and some managers, also general security awareness for customers and banks' employees who are customer-facing by formal training, computer-based training, e-mails, web sites, text and posters (PCI Security Standards Council, 2014). According to Trewin *et al*. (2016), customers who are well informed about the risks of mobile banking, and have a perception that these risks are easy to detect and control, are more willing to trust transactions to mobile systems.

V. Conclusion

The purpose of this study was to examine the security challenges of the private mobile banking in Iran. An attempt is made to provide a better understanding of the current status of security in mobile banking in Iran and identify the main factors that affect the level of security of mobile banking transaction, which then led to the development of a new framework. The Risk Assessment Framework aims to alleviate the existing security challenges with a view to achieve the security objectives of confidentiality, integrity and availability. The research focused on mobile banking technologies, security measures and security standards and policies.

It is hoped that the risk assessment framework will help manage the risks of mobile banking services and enhances the security that impacts on mobile banking usage. There is still more work to evaluate the framework involving the key stakeholders within the Iranian banking sector.

References

[1] Narendiran, C., Rabara, S. A. and Rajendran, N. (2008) 'Performance evaluation on end-to-end security architecture for mobile banking system', 2008 1st IFIP Wireless Days: IEEE, pp. 1-5.

[2] Elkhodr, M., Shahrestani, S. and Kourouche, K. (2012) 'A proposal to improve the security of mobile banking applications', ICT and Knowledge Engineering International Conference on: IEEE, pp. 260-265.

[3] Ghotbi, A. Nassir Gharechedaghi, N. (2012) 'Mobile Banking, Challenges and Strategies in the Banking System of Iran', Journal of Basic and Applied Scientific Research, pp. 5583-5594.

[4] Nie , J .Hu, X. (2008) 'Mobile Banking Information Security and Protection Methods', pp. 587 – 590. doi: 10.1109/CSSE.2008.1422.

[5] Khan, J., Abbas, H. and Al-Muhtadi, J. (2015) 'Survey on Mobile User's Data Privacy Threats and Defense Mechanisms', Procedia Computer Science, 56, pp. 376-383. doi: 10.1016/j.procs.2015.07.223

[6] Islam, M.S. (2014) 'Systematic Literature Review: Security Challenges of Mobile Banking and Payments System', International Journal of u-and e-Service, Science and Technology, 7(6), pp.107-116.

[7] Alafeef, M., Singh, D. and Ahmad, K. (2012) 'The influence of demographic factors and user interface on mobile banking adoption: a

review', Journal of applied sciences, 12(20), p. 2082. doi: 10.3923/jas.2012.2082.2095, Vol: 12.

[8] Rumanyika, J. D. and Mashenene, R. G. (2014) 'Impediments of e-commerce adoption among small and medium enterprises in Tanzania: A review', International Journal of Information Technology and Business Management, pp. 45-55.

[9] European Investment Bank. (2012) Mobile financial services in Mediterranean Partner Countries. Available at:

[10] http://www.eib.org/attachments/country/femip_study_mobile_financial_services_en.pdf (Accessed: 09 August 2016).

[11] Jin, N., Fei-Cheng, M.A. (2005) 'Network security risks in online banking', In Proceedings 2005 International Conference on Wireless Communications, Networking and Mobile Computing, 2005, Vol. 2, pp. 1229-1234.

[12] Central Bank of Iran. (2016) Payment & Clearance Systems. Available at:

[13] https://www.cbi.ir/page/15746.aspx (Accessed: 09 May 2018).

[14] Peymane, F. (2014) The Effectiveness of Private Banking on the Banking System in Iran. Available at: http://brisjast.com/wp-content/uploads/2015/06/July-55-2014.pdf (Accessed: 22 August 2016).

[15] National Informatics Corporation. (2011) Company's Profile. Available at: http://www.nicholding.net/indexltr.html (Accessed: 12 September 2016).

[16] Way2pay. (2014) Informatics Service Corporation awarded ISO/IEC 27001certification. Available at: http://way2pay.ir/30190 (Accessed: 10 August 2016).

[17] Informatics Service Corporation. (2016) Strategies and Objectives. Available at: http://en.isc.co.ir/Portal/home/?67358/Strategies-and-Objectives (Accessed: 11 September 2016).

[18] Ghazinoory, S., Dastranj, N., Saghafi, F., Kulshreshtha, A. and Hasanzadeh, A. (2016) 'Technology roadmapping architecture based on technological learning: Case study of social banking in Iran', Technological Forecasting and Social Change.

[19] Charkhandaz, G.H. (2014) Development of the electronic banking in Iran (Identifying barriers and guide-lines). Available at:

[20] http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwj49_mM69_QAhULJ8AKHUioBM0QFggaMAA&url=http%3A%2F%2Fpharmascope.org%2Fijrls%2Findex.php%2Fannounce%2Fdownload%2F148&usg=AFQjCNEkf0JAAGrjGjeC2EsHt1wEdvBLJQ (Accessed: 05 May 2016).

[21] Kashef. (2016) Kashef Banking Security Governance Company. Available at:

[22] http://www.kashef.ir/Portal/Home/Default.aspx?CategoryID=3d889a01-dae8-4f21-9f80-1b6110885cb2 (Accessed: 10 September 2016)

[23] Akbari, P. (2013) 'A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry (Case Study: Kermanshah Melli Bank)', International Journal of Management and Business Research, 2(2), pp.123-135.

[24] Law, K. (2007). Impact of perceived security on consumer trust in online banking. Available at:

[25] http://aut.researchgateway.ac.nz/bitstream/handle/10292/491/LawK.pdf?sequence=4 (Accessed: 16 November 2016).

[26] Luvanda, A. (2014) 'Proposed Framework for Securing Mobile Banking Applications from Man in the Middle Attacks', Journal of Information Engineering and Applications.

[27] Cognizant (2014) Mobile Banking Security: Challenges, Solutions. Available at:

[28] https://www.cognizant.com/InsightsWhitepapers/Mobile-Banking-Security-Challenges-Solutions-codex898.pdf (Accessed: 20 November 2016).

[29] S. Trewin, C. Swart, L. Koved and K. Singh. (2016) "Perceptions of Risk in Mobile Transaction", IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 2016, pp. 214-223. doi:10.1109/SPW.2016.37.

[30] PCI Security Standards Council (2014) Information Supplement: Best Practices for Implementing a Security Awareness Program. Available at:

[31] https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (Accessed: 25 November 2016).

AUTHORS

First Author – Sepideh Mollajafari, Professor Kamal Bechkoum Sepiedeh2000@gmail.com, KBechkoum@glos.ac.uk