International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 4, July – August (2015)

REVIEW ARTICLE

Security and Fraud Issues of E-banking

Emad Abu-Shanab
MIS Dept., IT College, Yarmouk University, Irbid, Jordan,
abushanab@yu.edu.jo

Salam Matalqa
CIS Dept., IT College, Yarmouk University, Irbid, Jordan,
salam.matalqah@yahoo.com

Abstract – E-banking has a lot of benefits that add value to customer's satisfaction in term of better service quality, and at the same time enable banks to gain a competitive advantage over other competitors. However, more attention towards e-banking security is required and needed against fraudulent behavior because the lack of control over security makes e-banking still un-trusted for many till today. This paper presents security issues related to e-banking along with the characteristics and challenges of e-banking fraud. Different types of attacks, some fraud detection strategies, and some prevention methods used by electronic banks, are also presented in this paper. An expert opinion method was used to rank different model and techniques in security. Results indicated that the most effective model is "Transaction Monitoring" and the worst models based on respondent's opinions are "Virtual Keyboards", "Browser Protection", and "Device Identification". The organization of this paper go in the following manner: section 1 will introduce the topic, followed by a literature review in section 2. Section 3 depicts the research methodology adopted and the data analysis process. Finally, conclusions and future work are stated at the end of the paper.

Index Terms – E-banking, Security of E-banking, Attacks, Security Models, Fraud, Expert Opinion, Ranking Models, Jordan.

1. INTRODUCTION

The fast advancement of global information infrastructure during the last decades, including information technology and computer networks (Internet and telecommunications systems) has enabled the development of electronic commerce at a global level, allowing business to effectively interact more with their customers and other corporations inside and outside their industries. E-commerce integrates communications, data management and security services, so that business applications would provide rapid and flexible exchange of information, for the purpose of serving customers and attaining firm's competitive advantage.

The banking industry, like many business sectors, utilized information and communication technology (ICT) to offer its customers value added services and convenience. The electronic banking system facilitated the interaction between customers and banks for the purpose of facilitating many services for bank customers. The previously mentioned system is called "electronic banking", "Virtual banking" or "Online banking". With many labels reported in the literature, they are all denoting the utilization of ICT to conduct banking transactions. E-banking includes the provision of various banking activities conducted virtually from anyplace, at any time outside the physical premises of banks.

However, this changing financial landscape, from traditional banking to electronic banking, has brought with it new challenges. Such challenges are not only related to bank management, but also to national and international regularity and supervisory authorities. The major challenges stem from the increased cross-border transactions, and from the reliance on technology to provide banking services with the necessary security from a remote location through the Internet. These challenges include regularity challenges, legal challenges, operational challenges, reputational challenges, inconvenience challenges and security challenges.

Obtaining safe and secure environment of computer technology is the most important concern for all financial service organizations. Security of online banking transactions is one of the most important challenges to the banking sector. Billions of financial data transactions are conducted online every day, and bank cyber-crimes take place every day by skilled criminal hackers through manipulating the bank's online information system. Threats can come from inside or outside the system, which threatens customers' information and transactions, where bank administrators must ensure that banks have the appropriate practices in place to guarantee the confidentiality of customers' data, as well as the integrity of the e-banking system and the transactions conducted.

In this paper, we present issues concerned with security, fraud and attacks of e-banking. We address the motives and importance of guarding for security, the common types of attacks that e-banking could encounter, and attack detection and prevention. This paper is organized as follows: Section 2 presents the literature review with the following subsections: security of e-banking, characteristics of e-banking fraud, different types of attacks, fraud detection and fraud prevention. In section 3, we present some data analysis for

REVIEW ARTICLE

fraud prevention, and finally section 4 concludes our work and presents some future works.

2. RELATED WORK

E-banking business model started back in the 1980's in New York, where it was offered by major banks in the city such as Citibank and Chase Manhattan. It was not a full transaction banking service, but very basic set of services such as viewing bank statements and paying bills online. However, It paved the way for the more comprehensive and sophisticated e-banking services that we see today [1].

Electronic banking has been around for quite some time in the form of automatic teller machines (ATMs) and telephone transactions. In recent times, it has facilitated banking transactions for both customers and banks, by using Internet, and has enabled banks to scale borders, change their strategic tactics and open new possibilities. Banking industries in countries all over the world in this 21st century have transformed or changed to better operate in the new complex and competitive environment (the electronic environment or electronic platform), in which the economic climate also has changed. Information technology (IT) is the pivot of these major substantial changes. With the new era of technological revolution, banking and financial industries are now capable for offering financial services, through electronic media to various customers, regardless of their place, time and distance [2].

In the 1990's, the use of Internet evolved when more people owned computers and became connected to the Internet through their dial-up connection from anywhere in their homes. This technological evolution and the spread of home Internet use allowed bank customers to enjoy 24/7 e-banking services. But customers during the 1990's didn't fully trust e-banking enough to make serious and substantial monetary transactions. This triggered a massive effort and investment by banks to develop more security features for their online banking services. Throughout the 2000's, online banking started to grow and become more acceptable by customers. It covered most of banking services range [1].

There are many various types of services that can be provided by e-banking. The popular services include automated teller machines (ATMs), credit cards, debit cards, smart cards, electronic fund transfer (EFT) systems, mobile banking, etc. On the transaction level, e-banking include account access, balance transfer, bill payment, bill presentment, mortgage lending, customer service and administration, cross selling, etc. From the bank's point of view, the use of Internet has significantly reduced the physical costs of banking operations, including the costs of information processing and transmission.

E-banking can be seen as the extension of existing physical banks. It's the use of computers to retrieve and process banking data, and to initiate transactions directly and remotely with a bank via telecommunication networks. It addresses several emerging trends such as customer demand for anytime/anywhere service, product to market imperatives and increasingly complex back-office integration challenges [3]. Scholars classified e-banking under the domain of e-commerce, where e-financing is the other major financial e-service provided. E-banking is more devoted to Internet banking, telephone banking, and other banking channels [4]. While e-banking is the commonly used term in literature, it is used by people interchangeably with virtual banking, on-line banking, cyber-banking, web banking, phone-banking and remote electronic banking [1].

2.1. Security of e-banking

The introduction of e-banking has come with its challenges, ranging from e-banking adoption, to financial limitations of new system [5]. Research concluded to several factors that influence the adoption process of e-banking like its usefulness and ease of use, system security, trust and social influence, the user friendly features of system, accessibility, the cost and time factors embedded in fund transfer [6], [7] and [8]. Security is a factor that is constantly highlighted as a critical success factor (CSF) for the success of e-banking. The inadequacy of security will potentially lead to financial losses, punitive measures by regulators and negative media publicity. Security was rated in some research as the most important issue of online banking services [8].

Jassal and Sehgal [9] aimed to find various types of flaws in the security of online banking that result in loss of money for account holders and financial institutions. They explained the reasons behind security breaches, and the participation of both customers and banks to enable hackers or crackers to access their networks. Bank clients log on to bank websites daily, through a Web-browser installed on client's personal computers, which open opportunities to cybercrimes to take place. The authors pointed to some flaws in security that could result in loss of money, along with leakage of information to unauthorized persons. Flaws could be on banking websites themselves, such as cross site scripting which happens when an attacker injects malicious scripts into a web page, and SQL injection vulnerability in which the hacker enters SQL statements into a field on a web form, in an attempt to get to the website to pass the command to the database [9]. Other Flaws could be in banking security policies, that they publish online in order to help users understand security measures that the bank follows, or could be in users' usability and customer awareness. It is important for clients to educate themselves about risks involved in online banking.

Nigudge and Pathan [10] stated the advantages and various popular services that could be provided by e-banking, but they presented the challenges that e-banking faces in India. One of

REVIEW ARTICLE

these challenges is concerned with the legal and security issues which can be represented by the lack and limitation of legal framework, increased potential of fraud, denial of e-documents in courts, weak security measures, and the lack of strong trust environment. This supports what was presented by Jassal and Sehgal [9] about the importance of security measures and strong business environment.

2.2. Characteristics of e-banking fraud

Fraud is defined as" any behavior by which one person intends to gain a dishonest advantage over another" [11]. Fraud is an act which intends to cause wrongful gain to one person and a loss to the other, either by a way of concealment of facts or otherwise. Based on an empirical analysis performed on real world transaction datasets, Kovach and Ruggiero [12] concluded that a large number of different e-banking accounts were accessed by a single fraudster, which included small value transactions with a total value larger than a single account fraud are common based on the increased number of password failures that open doors for fraudulent behaviors.

Similarly, in investigations made in one of the largest banks in Australia about online banking frauds, results showed that most of them have the following characteristics and challenges [13]: 1) *Highly imbalanced large dataset*: With large number of transactions usually millions in e-banking system and very small number of daily frauds, the task of detecting frauds becomes a tough challenge. 2) *Real time detection*: In some online banking transactions, fraud detection needs to be in real time to prevent instant money loss. 3) *Dynamic fraud behavior:* fraudsters continually advance their techniques to defeat online banking defenses. Defense against an ever-growing set of attacks is beyond the capability of any single fraud detection model. 4) *Weak forensic evidence:* Some external information (forensic evidence) associated with each e-banking transaction is very useful and needed to be known, to help understand the nature of deception of fraud behavior. 5) *Diverse behavior patterns of customers*. Customers of online banking perform various transactions in different ways and for different purposes, this is a challenge as it leads to diversity of genuine customer transactions that would be simulated by fraudsters who change their behavior frequently to compete with advances in fraud detection, thus makes it difficult to characterize fraud behavior from genuine behavior.

2.3. Types of attacks

The objective of an attacker may vary. Attacker may try to exploit vulnerabilities in particular operating systems, or they may try repeatedly to make an unauthorized entry into a website leading to denial of service to customers [14]. Hackers or attackers have many different ways that they can try to break the system through. However, the problems in information systems today are inherit within the setup of communication and the computer itself. Hence, banks and service providers need to guard against various types of online attacks to achieve secure communications over the channels of information systems [3].

Research tried to categorize and classify the various types of attacks against e-banking in different way. Vrincianu and Popa [15] reported that the main threats or attacks to security of e-banking platforms are the following: denial of service, illegitimate use, disclosure of information, and repudiation. Other research presented a classification for the common attacks against online banking systems [16]. Dalton and Colombi [17] proposed a hierarchy of causes that includes three major categories: legitimate access, device control and credentials theft. There model (Attack Tree Model) represents the main efficient attacks and how they relate to each other and how to exploit vulnerabilities inherit in the people (social engineering and phishing attack), and gain control of device (malware), and credential theft of a legitimate user (fake web pages and malware). Such classification is one of the simple and the most commonly used ones for the attacks performed over the online banking system [16].

Omariba et al. [3] also presented a classification of various attacks that e-banking can suffer from to include the following types: Social engineering attacks, port scanners, packet sniffers, password cracking, Trojans, denial of service attacks, server bugs and super user exploits. On the other hand, Brar et al. [14] categorized attacks into three main groups: remote, local and hybrid attacks. Remote Attacks don't modify the victim's machine but try to intercept or redirect the traffic of a session.

The following are some types of remote attacks [14]: 1) *Phishing:* Happens when an attacker sets up a copy of the web site they want to impersonate on a server they control, and this copy includes all the code of the original site. Next, the attacker would send emails that contain convincing message to a large number of email accounts, to trick the recipient to visit the spoofed web site and reveal his/her log on credentials. 2) *Vishing*: Happens when the attacker phones the victim and uses social engineering to trick the victim to reveal some secret information. 3) *Cloned voice-banking systems:* This happens when many vishing attacks clone voice-banking systems so that they sound the same as the official systems. Fake e-mails are used to solicit customers to call a number purporting to be their bank.

Local attacks happen on the victim's machine, when the opened website is the real bank site, the URL in the address bar is not spoofed, and even the yellow SSL (Secure Sockets Layer) padlock reveals the correct certificate details, but only an overlaid fake password prompt is not part of the original website and of malicious intent. One type of local attacks is shoulder surfing, in which attacker normally associated with

REVIEW ARTICLE

observing the personal identification number (PIN) for a bank card, prior to stealing the physical card either by force by pick pocketing it [14].

Finally, hybrid attacks combine local and remote attacks and are the most powerful. Nothing limits the attacker to only one type of attack. A Trojan would be executed on the infected machine, by checking all saved bookmarks and replacing any valuable online service URL with a fake one. Trojan also needs to modify the browser settings to not display the address bar, or overlay it with a fake pop-up window so that the user can't see the modified URL (local attack). The more sophisticated approach for attackers is that they would rather to use all power they have on the infected machine, alter the host files and redirect certain domains to predefined IP addresses (remote attack) [14].

2.4. Fraud detection

The published work related to fraud detection within the domain of online banking applications is not abundant due to privacy, secrecy and commercial interests concerning this domain. Therefore, the development of new fraud detection methods in banking area is difficult, and most published work is related only to credit card fraud detection [12]. In practice, existing online bank fraud detection systems are rule based, in which the rules are generated according to domain knowledge. Consequently, these systems usually have a high false positive rate, this means that the detection rate of fraud is low [13].

Kovach and Ruggiero [12] proposed a general architecture for fraud detector with the following main issues:

- *Device identification.* The identification of the access devices is made by a component that must be downloaded in client devices, and already used by the actual online banking system. This component generates a fingerprint of the access device (serial numbers, MAC address & some configuration details), and sends it to the bank website as part of each transaction.
- *Global behavior and monitor*. The observation of user's global behavior plays a major role in fraud detection. A large number of different accounts accessed by a single device, or the occurrence of login fail over many accounts using a single trial password are examples of global behavior that infer a fraud. Monitor uses counters to verify transactions which they updated for each transaction.
- *Deferential analysis*. In this approach, the incoming transactions are examined against a set of profiles that characterize the normal use pattern for a legitimate customer. Any significant deviation from this pattern may indicate a fraud. Some of profiles used for differential analysis are payment transaction frequency, password failures and login frequency.
- *Global analysis.* Used for strengthening or weakening the evidence of fraud determined by the differential analysis. This evidence has a probability determined by means of three lists: Black list which contains the fraudulent identities; White list contains the legitimate identities; and the Suspect list which contains the identities that have not yet been classified.
- *Suspect list and the exponentially decaying function*. The assignment of devices to one of three lists and the fraud probability are determined by specific rules. When the device is included in the suspect list, an initial value is assigned to the fraud probability that is calculated by an exponentially decaying function, based on the number of different accounts that were accessed by this suspected device. If a fraud of any of these accounts is reported by a customer, the associated device identity will be moved to the black list.
- *Dempster-Shafer combiner*. This is a mathematical theory of fraud evidence that provides a formal framework for combining sources of evidences, which are estimated by differential and global analysis modules, and computes the overall suspicion score of a transaction.

Wei et al. [13] also investigated fraud detection in e-banking, and reported three main types: Credit card fraud detection, computer intrusion detection and telecommunication fraud detection. In addition, they proposed and implemented an online banking fraud detection system, which takes advantage of domain knowledge, mixed features, multiple data mining methods and multiple layer structure for a systematic solution. Their approach and system were tested in a major bank, and showed that it is particularly effective in detecting fraud in large volume of extremely imbalanced data. Also, it performed better than existing fraud detection methods in both efficiency and accuracy.

2.5. Fraud prevention

Online or e-banking systems require efficient security models that are capable of identifying users and authorizing transactions, and thus mitigating fraud. However, current models are focused on fraud identification more than fraud prevention. This means that actions are taken after the occurrence of a fraud, instead of performing preventive procedures [16].

Fraud prevention describes security measures to avoid unauthorized individuals from initiating transactions on an account, for which they are not authorized [18]. Peotta et al. [16] presented many current security models adopted by online banking systems based on several security layers which

REVIEW ARTICLE

aim to protect banking applications and users data. They implemented analysis of security devices in ten large banks in Brazil, and explored the models adopted by each bank along with most and least model used. There results indicated the models depicted in Table 1. Similar to these fraud prevention methods listed in Table 1, Brar et al. [14] also presented some solution options for preventing fraud, which have some commonality with the methods presented by Peotta et al. [16]. They recommended that security of online bank services should not be solely based on the security on the end point (User's PC). The discussed methods are listed in Table 2.

Online banks have invested heavy efforts in securing the financial information of customers. A five-step approach has been implemented to protect online customer information against external threats, by which we can create much secured banking environment. These steps are conducted as follows: First, the user enters an access number (ID) provided by the bank on the bank's website. Second, he/she must enter a password to complete the access process to his/her account. The third and fourth steps ask the user to answer first and second personalized questions, to add more security measures. Finally, the fifth step identifies an image that would be marked previously by the user. After completing the five steps, users are granted access to the banking system [19].

In addition to fraud prevention methods used in e-banking domain, many national regulators have already amended their regulations to ensure safety and soundness of the domestic banking systems, protect customer rights, and achieve public trust among them. Licensing, verifying an individual's identity, capacity planning, adaptation, legalization, harmonization and integration are all policies that can be used to achieve and enhance safety and security of e-banking [20].

3. METHODOLOGY AND DATA ANALYSIS

This study adopted the work of Peotta et al. [16] and their classification of security models as depicted in Table 1 previously. The authors tried to summarize the models and tabulated them in a style similar to that of Table 1. In the following step, a group of information technology specialists (25 master students in Information Technology College in a public university in Jordan) were probed for their opinions regarding the effectiveness of such models in the context of Internet banking. The respondents needed to understand the models, their descriptions and their limitations (as proposed in this paper). Then each expert was given adequate time to rank the models according to their effectiveness in e-banking context.

Twenty one valid responses were received after 1 week, where respondents ranked the models. The ranking takes value from 1-12. The value "one" represents the most effective model among all models listed in Table 1, and the rank of "twelve" represents the worst among all. The 21 responses are summarized and depicted in Table 3 below.

To compare the models, the means and standard deviations of all responses were estimated. Then results were ranked according to the means and standard deviations, where perceptions of respondents are further summarized. Table 4 shows the results, where the rows of the table represent the methods, arranged in a similar format to that used in Table 1. To better represent the results, radar diagrams were plotted for the 4 methods disputed. Diagrams are shown in Figure 1, representing these results.

4. CONCLUSION AND FUTURE WORK

The exponential growth of Internet has offered tremendous market potential for today's businesses including e-banking industry. E-banking revolution changed the business of banking fundamentally by providing many benefits for customers and new business opportunities for banks. However, it imposes traditional banking risks and many challenges especially in terms of security issues. Security aspects should be taken in consideration at all levels of financial organizations, to protect themselves against various types of fraud and attacks.

Research indicated that many factors influence the adoption of e-banking, where factors like usefulness, ease of use, trust, and social influence were major influencers to the intention of using e-banking [6] [7] [8] [21]. Research also concluded that the well-rooted trust in paper-based transactions and change-avoidance culture still need more time to enable e-banking services to be used on a wider range. Furthermore, based on the work of Shannak [1] and discussions with local experts and through reading local regulations, it is shown that e-banking regularity coverage in Jordan has been overshadowed by the poor reputation of e-commerce regularity issues.

Different methods for fraud detection and prevention have been introduced and proposed by many researches, in which some were effective in improving the accuracy of fraud detection and prevention. However, there is no any single strategy or method that covers all different dangers or attacks threatening e-Banking platforms. Researchers proposed diverse techniques for authentication also, where multi method is recommended when utilizing biometric techniques in security [22]. More potent issues are faced when dealing with new environments like cloud computing [23]. The future of e-banking seems to be secure as stated by Saranya and Gunasri [24], due to the ever increasing adoption and arrival of new technologies to address the existing limitations of e-banking. Also, mobile phones will have a significant and major role in the area of e-banking and security provision [25], still we need to watch for their negative side and its influence on Health [26]. E-banking raises many complicated issues for banks and regulators alike, and thus much work is

REVIEW ARTICLE

needed at national and international levels. Furthermore, e-banking will be a system where users are able to interact with their banks "worry free", as stated by Omariba et al. [3], and that banks will be operated under one common standard.

This study collected an expert evaluation of a set of 12 security models based on the work of Peotta et al. [16]. Experts ranked the security models and yielded the results in Table 4. Results in Table 4 include 4 columns, where the values of the last two columns represent the rank related to the most effective model for respondents compared to other models in the list (according to the means and then according to standard deviations). Results show that the most effective model is "Transaction Monitoring" followed by "Short Message Service (SMS)" and "One-Time Password Tokens". And the worst models based on respondent's opinions are "Virtual Keyboards", "Browser Protection", and "Device Identification".

By looking at the standard deviations, which mean dispersion in responses, we see dispute on the rank. The smaller values of standard deviation mean more consensuses on the rank, and the opposite means a dispute between responses. Based on high agreement between respondents, the model with the least standard deviation is "Virtual Keyboards" model. Similarly, the "Browser Protection" model is the 3rd in dispersion, which again means a consensus to be the least effective model. On the other hand, the analysis also indicates that the highest standard deviation is associated with "Digital certificates" model, which is ranked in the middle. Finally, a surprising result is the dispute associated with "Short Message Service (SMS)" model, which indicates a dispute among respondents regarding its effectiveness. Finally, the radar diagrams indicate that the "Transaction Monitoring" model is the superior model, and the "Virtual Keyboards" model is the least effective among all. The remaining results are disputable.

Model	Description	Frq.*
Virtual Keyboards	Capture information typed into the device based on Java and software-based cryptography, to thwart the efficient use of key loggers.	7
One-Time Password Cards	Provides a second authentication factor; less expensive for generating dynamic passwords.	5
Browser Protection	Protects the user and his/her browser against known malware by monitoring the memory area allocated by the browser.	5
Digital certificates	Used to authenticate both users and the banking system itself using Public Key Infrastructure (PKI) and a Certificate Authority (CA).	4
One-Time Password Tokens	Devices that commonly used as a second authentication factor by dynamically changing passwords.	3
Device Identification	Applied together with device registering but also used as a standalone solution. It is based on physical characteristics of users' devices.	3
Positive Identification	Requires the user to input some information that is only known to him/her to identify him/her self.	2
Pass-Phrase	Technique based on information held by the user which used in money movement transactions.	2
Device Registering	Restricts access to banking systems to previously known and registered devices.	2
CAPTCHA	(Completely Automated Public Turing test to tell Computers and Humans Apart) Renders automatic attacks against ineffective authenticated sessions.	1
Short Message Service (SMS)	Notifies users about transactions that require their authorization.	1
Transaction Monitoring	Includes many approaches such as Artificial Intelligence, transaction history analysis and other methods for identifying fraud patterns.	0

**Frequencies based on the Brazilian data*

Table 1: Internet Banking Security Models commonly used (Source: Peotta et al. [16])

REVIEW ARTICLE

Method	Description
SMS Challenge Code	Used to ensure secure log on to a valid user's mobile phones, by receiving an activation code by which users identify themselves to the bank with their account names. The bank generates a random temporary password, and sends it in a short text message (SMS) to user's mobile phone number, which he/she enters in the browser to prove that he/she is accessing the current mobile phone.
Image Verification	This method is based on a shared secret between the bank and the user, which consists of an image and a verification phrase. When the user logs on to the bank system with his username, device ID is sent along with this username and realized through an encrypted cookie that is stored on user's computer/mobile. The system then determines if the device ID and username match the ones stored, and opens the login page to the user with the secret image verification phrase that would be embedded in it.
Dynamic Security Skins-DSS	User chooses an image which will be overlaid on web forms and contains sensitive information prompts, along with a virtual hash (a unique graphical pattern) tied to the secured SSL session. This makes it infeasible for attackers to spoof a pop-up that is identical to password prompts.
PKI based Software Solution	The use of Public Key Infrastructure (PKI) would make it possible to authenticate not only the server to the user, but also vice versa. This mutual authentication would eliminate MITM (Man in the Middle) attack.
PKI based Hardware Token	This method uses tamper resistant key storage to ensure high security against Trojans, which can steal private keys and PIN codes for a PKI based software token. Key pairs and certificates will be Pre-generated and stored on a tamper proof smartcard, and by using a PIN code on the external device's keypad, this will unlock the key vault in the smartcard and prevent key logger form intercepting it.

Table 2: Fraud Prevention methods (Source: Brar, et al, [14])

	Security Model											
Expert	1	2	3	4	5	6	7	8	9	10	11	12
1	12	6	4	3	2	3	4	5	5	2	1	2
2	5	3	9	11	7	11	10	9	11	4	8	11
3	7	2	6	9	3	12	8	10	11	5	4	1
4	8	7	10	11	6	2	5	4	9	3	1	6
5	11	12	10	6	7	8	9	5	4	2	3	1
6	8	2	10	7	1	11	4	5	12	9	3	6
7	8	10	12	11	3	9	4	7	2	5	6	1
8	12	4	6	8	3	10	11	5	9	7	1	2
9	12	4	7	10	5	6	2	11	8	9	1	3
10	3	7	4	10	12	6	1	11	8	9	5	2
11	8	10	12	3	9	7	6	4	11	2	1	5
12	11	8	7	9	6	4	3	10	2	12	5	1
13	9	7	5	4	6	10	11	1	2	12	8	3
14	8	3	7	1	6	10	12	11	5	4	9	2
15	10	1	9	5	2	4	7	11	3	6	12	8
16	11	7	12	10	3	9	4	6	4	8	1	2
17	6	12	5	1	10	3	2	7	4	11	9	8
18	10	2	1	4	11	7	5	9	6	8	12	3
19	9	11	8	2	7	6	12	3	1	5	10	4
20	7	2	5	1	3	10	7	11	6	12	4	8
21	9	10	11	12	8	2	7	3	1	5	4	6

Table 3: The ranking of respondents

REVIEW ARTICLE

#	Model Name	Mean	Std. Dev.	Mean Rank	Std. Dev. Rank
12	Transaction Monitoring	4.05	2.906	1	2
11	Short Message Service (SMS)	5.14	3.745	2	11
5	One-Time Password Tokens	5.71	3.117	3	4
9	Device Registering	5.9	3.59	4	9
2	One-Time Password Cards	6.19	3.655	5	10
7	Positive Identification	6.38	3.427	6	8
4	Digital certificates	6.57	3.828	7	12
10	CAPTCHA	6.67	3.381	8	7
8	Pass-Phrase	7.05	3.232	9	6
6	Device Identification	7.14	3.198	10	5
3	Browser Protection	7.62	3.057	11	3
1	Virtual Keyboards	8.76	2.385	12	1

Table 4: The means and standard deviations of security models and their ranks.

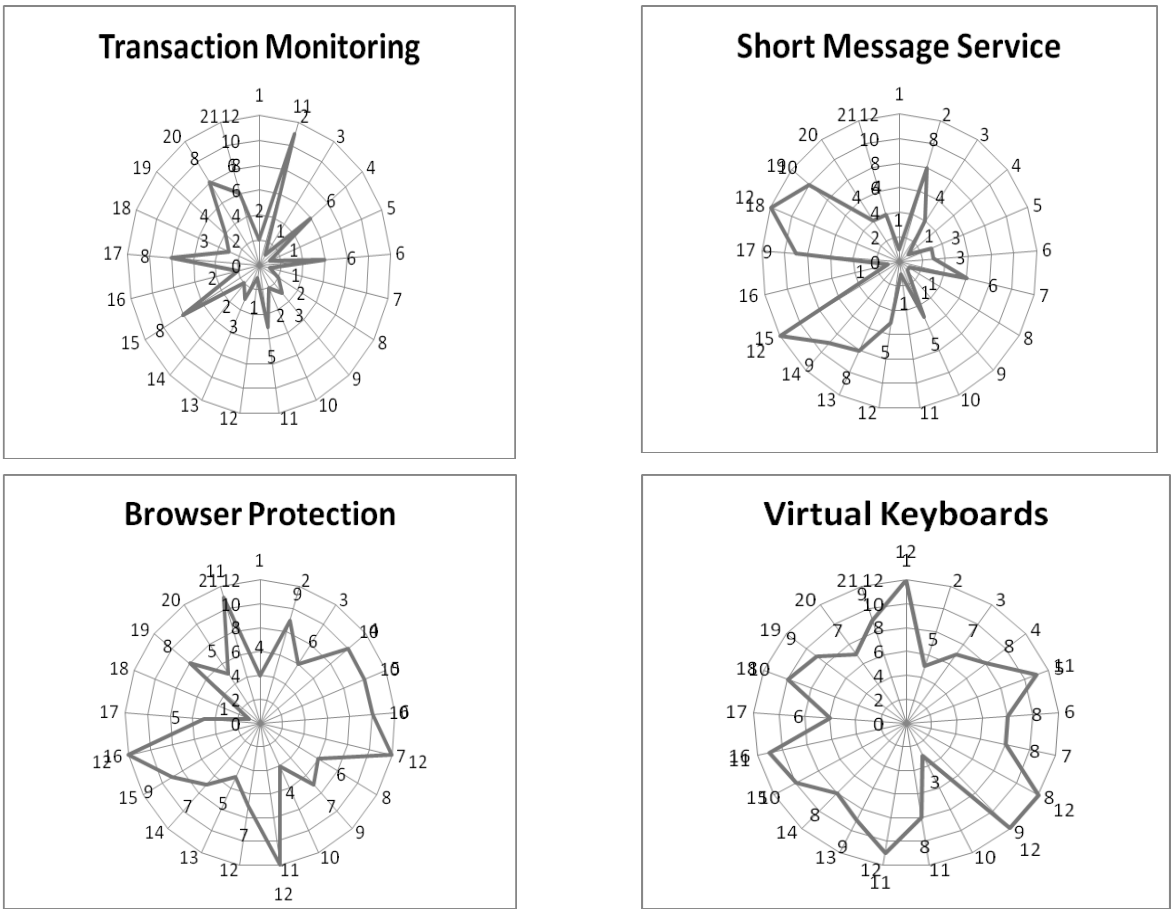

Figure 1: Radar diagrams representing four security models

REFERENCES

[1] Shannak, R. (2013). Key Issues in E-Banking Strengths and Weaknesses: The Case of Two Jordanian Banks. European Scientific Journal, 9(7), 239 – 263.

[2] Tunmibi, S. & Falayi, E. (2013). IT Security and E-Banking in Nigeria. Greener Journal of Internet, Information & Communication System, 1(3), 61 – 65.

[3] Omariba, Z., Masese, N. & Wanyembi, G. (2012). Security and Privacy of Electronic Banking. IJCSI International Journal of Computer Science Issues, 9(3), 432 – 446.

[4] Chavan, J. (2013). Internet Banking - Benefits and Challenges in an Emerging Economy. International Journal of Research in Business Management (IJRBM), 1(1), 19 -26.

REVIEW ARTICLE

[5] Usman, A. & Shah, M. (2013). Critical Success Factors for Preventing e-Banking Fraud. Journal of Internet Banking and Commerce, 18(2), 1 – 13.
[6] Abu-Shanab, E. & Pearson, J. (2007). Internet Banking in Jordan: The Unified Theory of Acceptance and Use of Technology (UTAUT) Perspective. Journal of Systems and Information Technology, 9 (1), 78-97.
[7] Abu-Shanab, E. Pearson, J. & Setterstrom, A. (2010). Internet Banking and Customers' Acceptance in Jordan: The Unified Model's Perspective. Communications of the Association for Information Systems (CAIS), 26 (23), 493-525.
[8] Auta, E. (2010). E-Banking in Developing Economy: Empirical Evidence from Nigeria. Journal of applied quantitative methods, 5(2), 212 – 222.
[9] Jassal, R. & Sehgal, R. (2013). Online Banking Security Flaws: A Study. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 1016 – 1021.
[10] Nigudge, S. & Pathan, M. (2014). E-banking: Services, Importance in Business, Advantages, Challenges and Adoption in India. Asian Journal of Management Sciences, 2(3), 190-192.
[11] Chakrabarty, K. (2013). Fraud in the banking sector – causes, concerns and Cures. The National Conference on Financial Fraud organized by ASSOCHAM, July 26, 2013, New Delhi, India, pp 1 – 13. Accessed from the Internet in November 2014 from: http://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=826
[12] Kovach, S. & Ruggiero, W. (2011). Online Banking Fraud Detection Based on Local and Global Behavior. The Fifth International Conference on Digital Society, Guadeloupe, France, 166 – 171.
[13] Wei, W., Li, J., Cao, L., Ou, Y. & Chen, J. (2012). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web, 16(4), 449- 475.
[14] Brar, T., Sharma, D. & Khurmi, S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, Proceedings of 'I-Society 2012', Punjab, India.
[15] Vrincianu, M. & Popa, L. (2010). Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests. Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests, 12(28), 388 – 403.
[16] Peotta, L., Holtz, M., David, B., Deus, F. & Sousa Jr, R. (2011). A Formal Classification of Interest Banking Attacks and Vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), 186 – 197.
[17] Dalton, G. & Colombi, J. (2006). Analyzing Attack Trees using Generalized Stochastic Petri Nets. Proceedings of the 2006 IEEE Workshop on Information Assurance, NY, USA, 116 – 123.
[18] Bolton, R. & Hand, D. (2002). Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.
[19] French, A. (2012). A Case Study on E-Banking Security – When Security Becomes Too Sophisticated for the User to Access Their Information. Journal of Internet Banking and Commerce, 17(2), 1- 14.
[20] Bahl, S. (2012). E-Banking: Challenges & Policy Implications. International Journal of Computing & Business Research, Proceedings of 'I-Society 2012', Punjab, India.
[21] MdNor, K., Abu-Shanab, E. & Pearson, J. (2008). Internet Banking Acceptance In Malaysia Based On The Theory Of Reasoned Action. Journal of Information Systems and Technology Management, 5(1), 3-14.
[22] Abu-Shanab, E., Khasawneh, R. & Smadi, I. (2013). Authentication Mechanisms For E-Voting. A book chapter in "Human Centered System design for E-Governance" edited by Saqib Saeed & Chris Reddick., IGI Global, USA, (2013).
[23] Sinjilawi, Y., AL-Nabhan, M. & Abu-Shanab, E. (2014). Addressing Security and Privacy Issues in Cloud Computing. Journal of Emerging Technologies in Web Intelligence, Vol. 6(2), May 2014, pp. 192-199.
[24] Saranya, K. & Gunasri, K. (2013). Challenges in E-Banking. International Journal of scientific research and management (IJSRM), a special issue of journal with no volume or issue number, pp 22 – 27. Accessed in November 2014 from the Internet from: http://ijsrm.in/special%20Issue%201/5%20ijsrm.Pdf
[25] Alafeef, M., Singh, D., Ahmad, K., Abu-Shanab, E. (2013). Usability Testing for Mobile Banking Prototype in Jordan. Proceedings of the 2nd International Conference on Computer Engineering &Mathematical Sciences (ICCEMS 2013), 5-6 December 2013, Kuala Lumpur, Malaysia, pp. 48-54.
[26] Abu-Shanab, E. & Haddad, E. (2015). The Influence of Smart Phones on Human Health and Behavior: Jordanians' Perceptions. International Journal of Computer Networks and Applications, March-April, 2015, Vol. 2(2), pp. 52-56.

Authors

Dr. Emad A. Abu-Shanab earned his PhD in business administration, in the MIS area from Southern Illinois University – Carbondale, USA, his MBA from Wilfrid Laurier University in Canada, and his Bachelor in civil engineering from Yarmouk University (YU) in Jordan. He is an associate professor in MIS. His research interest is in areas like E-government, technology acceptance, E-marketing, E-CRM, Digital divide, and E-learning. Published many articles in journals and conferences, and authored three books in e-government. Dr. Abu-Shanab worked as an assistant dean for students' affairs, quality assurance officer in Oman, and the director of Faculty Development Center at YU.

.

Salam H. Matalqa obtained her M.S degree in Computer Information Systems (CIS) in June 2015, from Yarmouk University, Irbid, Jordan, and her B.S. degree in Computer Information Systems in January 2009, from the same university. Her research interests tend to focus on areas of database systems, information retrieval, data mining and E-banking.