Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank Perspectives

Jaafar M. Alghazo and Zafar Kazmi
College of Computer Engineering and Sciences,
Prince Mohammad Bin Fahd University,
Khobar, Saudi Arabia
{jghazo & zkazimi}@pmu.edu.sa

Ghazanfar Latif *
Faculty of Computer Science and Information Technology,
University of Malaysia, Sarawak
Kota Samarahan, Malaysia
glatif@pmu.edu.sa

***Abstract* - Internet banking has become one of the fastest and easiest way of banking. The threat of cyber security attacks set a great challenge for the Internet banking and electronic commerce (E-commerce) industries. In this paper, we first analyse in detail the cyber security of Internet Banking in three emerging countries and then propose a novel model to reduce the cyber security risk to bridge the gap between banks and customers. The proposed model is based on results of surveys conducted on Internet banking in Saudi Arabia, Pakistan, and India. The survey focused on users' practices in Internet banking. The questions were based on user knowledge of cyber security and awareness of common threats in Internet Banking. The results of this study based on 1044 Internet banking users and 92 Internet banking websites shows there is an emerging gap between banks expectation and user actions. The proposed model bridges the gap by increasing the responsibility of banks to reduce cyber security risks for users.**

Index Terms - User Practices, Internet Banking, Cyber Security, E-Commerce, Emerging Countries.

I. Introduction

Internet banking is also known as electronic banking (E-banking), online banking, and virtual banking; it is widely promoted as a convenient banking solution. Internet banking has proved to be an ideal and profitable means of banking in the banking industry. Banks have quickly migrated to this technology in order to reduce cost and improve customer experience [1]. The adoption of technology depends on information gathering and set of users' belief that will help to either accept or reject it [2]. The technology acceptance model (TAM) determines that user acceptance of technology is driven by two factors: the ease of using that technology and its usefulness [3]. The adoption of technology is the greatest challenge for the banking industry. Some of the risks associated with Internet banking are users' behaviour [4]. Internet banking security risks can cause financial losses if the risks are real. Financial sectors and banking sectors are more prone to security attacks [5]. User acceptance is one of the key factors in the acceptance of technology. To work on Internet banking requires a certain level of information technology literacy. Users may not be comfortable in trusting on fully automated system [6].

Despite the fact that banks in emerging countries have integrated security features, user's behaviour causes security vulnerabilities. A lot of internet security threats and vulnerabilities persist. An example is Internet banking users sharing their login credentials with others knowingly or unknowingly. This may lead to compromising the user's account and may lead to security breaches [7]. As new threats continue to emerge, banks will need to adopt new measures to protect users. Banks can do more by deploying information security policies that ensure a safer Internet banking experience. Information technology security policies could consist of items related to users and machine based learning or artificial intelligence, which would learn users' patterns while conducting Internet banking. For example, a bank's artificial intelligence could detect trusted devices like a trusted laptop or a mobile device, which the clients uses for his daily banking activities, and if the user logged in from a different device, the banking system would send a notification to the registered mobile number of the user.

In this study, a novel model is proposed which puts more responsibility on banks to avoid security breaches caused due to negligence or users' lack of awareness. The responses from the conducted survey highlighted two aspects regarding users: 1) user behaviour while conducting Internet banking and 2) user awareness of threats related to Internet banking. Some of the negative responses are related to users' lack of awareness of threats related to Internet banking. It would be difficult for users to cope with the changing technologies and threats. Therefore, the logical solution could be that banks control the process by imposing information technology policies that could help bridge the gap leading to a safer E-banking environment and reducing the possibility of security breaches. The banks can use behavioural study or model that are based on artificial intelligence or machine based learning that could provide an early-detection of users' negligence, or they could target those domains which could lead to a security breach of Internet banking.

This paper will be presented as follows: section 2, will show the related work and literature review, section 3 will detail the research methodology, section 4 will indicate the users' survey results and analysis, section 5 will detail the proposed model, and section 6 will detail the conclusion.

II. Related Work

Numerous studies have been carried out in understanding the adoption of technology in Internet banking. A study was carried out by collecting the responses of 387 users who used Internet banking to understand which factors affected the

customer's perspective of adopting SST (Self Service Technology) and the way the user adopted the technology [8]. The authors developed a readiness model to explain relationships among technology readiness, user-informational-based readiness, customer readiness, and the purpose of adopting SST. In [9], a model is proposed in the Financial Institution Letter that will predict the behaviour of the Internet banking users. The letter highlights that security breaches are due to certain factors associated with aspects of human behaviour including examples such as not unlocking computers, the installation of software from un-trusted sources and password management. It concludes that there is a direct relationship between Internet banking security breaches and customer behaviour.

Martins et al. proposed a model that determines user behaviour based on intention and usage of Internet banking [10]. The conceptual model is a combination of the unified theory of acceptance and the use of technology (UTAUT). In order to test the conceptual model, 249 cases from Bank of Portugal were studied. The proposed model supports a relationship based on performance expectancy and role of risk based on stronger prediction of intention of use of Internet banking. The factors that influence the adoption of Internet banking in the Republic of Yemen is determined in [11]. Information was gathered by conducting a survey of 1500 users. By using the theory of reason action (TRA) model, it was extended by relative advantage, perceived risk, mass media, family influence, and scepticism. The model provided a good understanding that influences the user's Internet banking intention. The model explained 68.3% of the variance in the behavioural intention. Yuen et al. investigated the cultural difference in the adoption of Internet banking in the USA and Malaysia [12]. The research study provides marketing recommendation to influence users in adopting Internet banking based on cultural dimension. Questionnaires were designed using structural equation modelling and a survey was conducted on 1050 Internet banking users. The result concluded that due to cultural differences, consumers had a different pattern in adopting Internet banking. An empirical study was conducted to understand the adoption of Internet banking amongst customers in Jordan [13]. A population sample of 476 random customers' responses were analysed. In the dimension of study, factor analysis-varimax rotation was used and simple regression was used to see the influence on perceived privacy and security, ease of use, quality of service and customer feedback on Internet banking. All the factors chosen for the study were independent, but the factor that had the most impact in influencing the customer's trust was the quality of service provided on the website. The acceptance of Internet banking was found in the audience that had a high level of education and computer literacy.

A review of 165 research papers related to Internet banking was done in [14]. The result derived from the paper showed that the adoption of Internet banking was one of the growing fields that excited researchers. The paper was classified into 3 main themes: 1) whether the paper sought to describe the phenomenon, 2) whether it sought understanding the relationship between the factors and drive option, and 3) whether it sought to draw a conclusion based on population, channels and method. A study was carried out to analyse the factors that encourage users to adopt Internet banking in Saudi Arabia [15]. The research construct was developed on Technology Acceptance Model (TAM) with added extra control variables. The paper studied factors influencing customers for adopting online banking; it used responses of 400 customers. The responses showed that the quality of Internet, social influence, and computer efficiency had a great impact on perceived usefulness (PU) and perceived ease of use (PEU) for online banking acceptance, education and trust.

III. Research Methodology

In this study, the research methodology is designed by selecting 3 emerging countries, namely Saudi Arabia, India, and Pakistan. A survey was designed with a questionnaire divided into two parts; the general practice of users on the Internet banking and awareness of the threats related to Internet banking. Based on the survey's positive and negative responses, a model is proposed that can bridge the gap between the expectations of banks and users' behavioural response when it comes to Internet banking. To support the argument about the importance of internet banking, detailed analysis about the total Internet users against the total population of each selected country is summarized in Table 1 [16]. Statistical analysis is also done for total internet banking users against overall banking users as shown in Table 2 [17-19]. A detailed analysis of security measures provided at the login webpages of the selected banks was also done as shown in Table 3. The work flow of the proposed methodology is shown in Fig. 1.

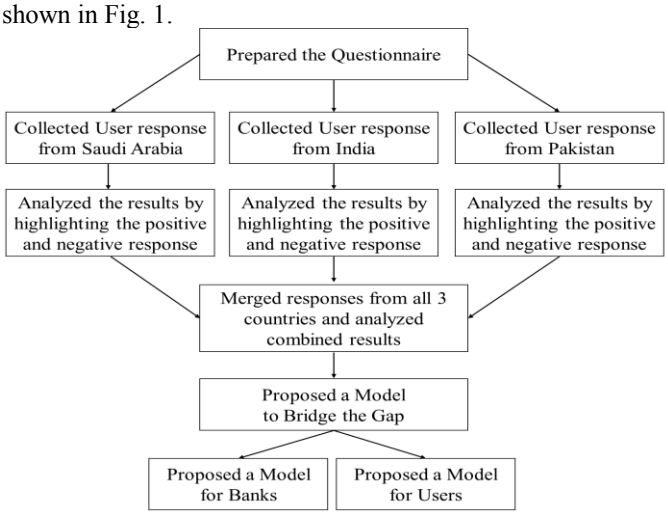

Fig. 1 Workflow of the proposed research methodology.

A. User Practices for Internet Banking

Some of the practices that a user is expected to follow while in the Internet banking environment.

1) Maintaining an up to date operating system on personal computers that can protect the user from malware.

Downloading software from a 3rd party is a common practice by users. Most of the users are unaware of the malicious codes that are hidden in the software.

2) Using a browser with fewer vulnerabilities. Browsers are the most likely items targeted by cyber attackers. Users' data can be compromised if their browsers are not frequently updated.

3) Password management. Choosing a complex password which includes a combination of capital and small letters, numbers, and special characters. This can make the password difficult to guess and avoid unauthorized access.

4) Reading banking agreement. As per our survey, users do not read the online banking agreement which highlights the user's responsibilities and the point that banks would like to educate users about the sensitive nature of Internet banking. The online banking agreement consists of information for protecting the user's password, credit cards, and pin number. Banks in Saudi Arabia provide their customers with the service level agreement (SLA) in hard copy and outline some information on their websites. Mostly, the bank assumes that if the user has signed the agreement it is clear that he/she has understood the terms and conditions for using online banking.

5) Changing one's Internet banking password once every six months. A good information technology practice is to change one's password very six months.

6) Antivirus. Antivirus is a computer software that looks or scans for known viruses on a computer. After detecting the virus or any suspicious program residing on the computer, the software acts to either delete or quarantine the virus.

7) Keeping a pattern of guessing or a biometric lock on smart phones. Users who use mobile banking can make their phones vulnerable if they do not put a pattern lock or biometric lock on their phones.

TABLE 1 Internet Users with Growth Rate

	Saudi Arabia	**India**	**Pakistan**
Number of Internet Users	20.81 millions	462.12 millions	34.35 millions
Total Population	32.16 millions	1326.80 millions	192.82 millions
Penetration	64.7 %	34.8 %	17.8 %
Growth in 1 year	2.8 %	30.5 %	9.7 %
Growth in 3 years	13.9 %	139.1 %	44.6 %
Growth in 5 years	52.2 %	267.9 %	119.7 %

TABLE 2 Internet Banking increased usage in different countries

		Saudi Arabia	**India**	**Pakistan**	**Total**
Banking Users	Number of Banks	25	92	55	172
	Number of Customer	14 million	470 millions	26.4 millions	510.4 millions
	Penetration	43.5%	35.5%	13.7%	30.9 %
Internet Banking Users	Banks providing Internet banking	25	51	16	92
	Customer using E Banking	8.4 million	14.5 million	1.8 millions	24.7 millions

B. User awareness of threats related to Internet Banking

An Internet banking security system can be compromised by customers themselves through a malicious program residing on the user's PC or by the user opening unsolicited emails. As Internet banking users are also not aware of cyber security risks, they can fall victim to frauds like phishing and social engineering attack.

1) Phishing: Phishing is used to lure victims into giving away their passwords or other information willingly. Identity thieves phish for passwords and financial information in the cyber world [20]. Phishing is a form of social engineering attack that tends to convince a victim to give away personal information like credit card details, pin numbers, and social security number so that the thieves can use this information against them [21]. Once the phishing threat has become real, it has a negative effect on the organization, revenues, and customers [22]. Even educated users are vulnerable to phishing attacks and it is shown that social engineering has reached levels at which users can be educated about phishing attacks and yet still fall prey to phishing attacks because of their trusting nature [23].

2) Social Engineering: It is used to convince the victim through a sense of excitement or fear, or establish trust with the victims to give away their valuable information willingly [23-24]. The key aspect is trust in social engineering. For example, a user may be promised prize money or financial interest that may be transferred into his account if the user provides his banks details. In most cases, the user gets distracted and fails to analyse the message or content of the message out of excitement. The social engineering aspect is that the user willingly provides his confidential information to the identity thief; the information is then used to commit fraud or destroy the user's assets [25].

IV. User Response and Results

Banks in the emerging countries do highlight the security practices that an Internet banking user should follow. Banks which provide E-banking do mention Information Technology security practice for the users to follows in order to ensure a safer experience. Based on the banks chosen from emerging countries, Table 3 was generated by visiting all 92 banks (providing Internet banking) website login pages and collected data about the security risk information on their login pages. The table highlights the security practices listed for the users to follow. With the emergence of new security threats, users may not be able to cope with the everyday changes made by the banks. For example, banks in Saudi Arabia provide a two-factor authentication in which once a user is logged in successfully, a onetime password (OTP) is sent on the customer's registered mobile number which the user has to enter before being redirected to the Internet banking webpage. All transaction notifications are sent via SMS. Banks in India also provide a two-factor authentication, where a user needs to have a separate password for login and a separate password for transactions. In order to perform a transaction, the user has to enter an OTP reference number, which is sent as OTP to the

registered mobile number and a password for transaction. In Pakistan, a similar two-factor authentication is used.

TABLE 3 Security risk information provided at the login webpage by 92 Banks

	Information provided for Online Banking Customers regarding Security	Percentage of banks
1	Phishing	57%
2	Social Engineering	42%
3	Virus and Spyware that affects customers PC	57%
4	Customer Role in Protecting his information online	100%
5	Banks advising Customers not to use public network	57%
6	Not to give out personal banking information to anyone calling from the bank	100%
7	Hotline call service to report any incident related to online fraud or theft	71%
8	SSL Lock	57%
9	Password Policy	57%
10	Online agreement between the banks and its customer	42%
11	Updating Browser for Security reason	100%
12	Keeping the Antivirus up to date	85%
13	Information relevant to online secure banking available at first login page	100%

The survey was conducted in Saudi Arabia, India and Pakistan. The survey was sent online to 2000 individuals and we received 1044 responses including 352 from Saudi Arabia, 272 from India and 420 from Pakistan, a response rate of 52.2%. As indicated previously, the survey was divided into two parts: one concentrating on the users' practices in the E-banking environment and one concentrating on user awareness of Internet banking security risks. Fig. 2 summarizes the results of the survey per country and overall results. For example, it is indicated that only 41% of respondents are aware of phishing attacks. The results were carefully analysed in order to formulate a model to reduce the cyber security threats in an E-banking environment.

V. Bridging the Gap: Proposed Model for Internet Banking Security

Based on a detailed analysis of the results obtained in table 3, the vulnerabilities of Internet banking environment were identified. The major responsibility of maintaining a secure Internet banking experience lies with the customer; customer must choose an appropriate browser and update the browser; he must choose appropriate antivirus and update the antivirus; he must be aware of phishing attacks, be aware of Malware, remember to update passwords every six months, choose a complex password, etc. In this paper, we propose a novel model that shifts some of these responsibilities to the banks. Banks have state-of-the-art Information Technology Operations and Centers. By investing a bit more, the banks can take some of the responsibilities away from the customer and reduce the risk of security threats, thereby offering a fairly secure environment for their customers. The model proposed in Fig. 3 highlights some of the practices that are to be divided between Internet banking users and the banks information technology security policies. The proposed model bridges the gap between the users and the Bank. The model states that the banks can enforce their security policies to ensure safer banking experience for users. On the other hand, users should follow the instructions provided by the bank to ensure a safe Internet banking experience.

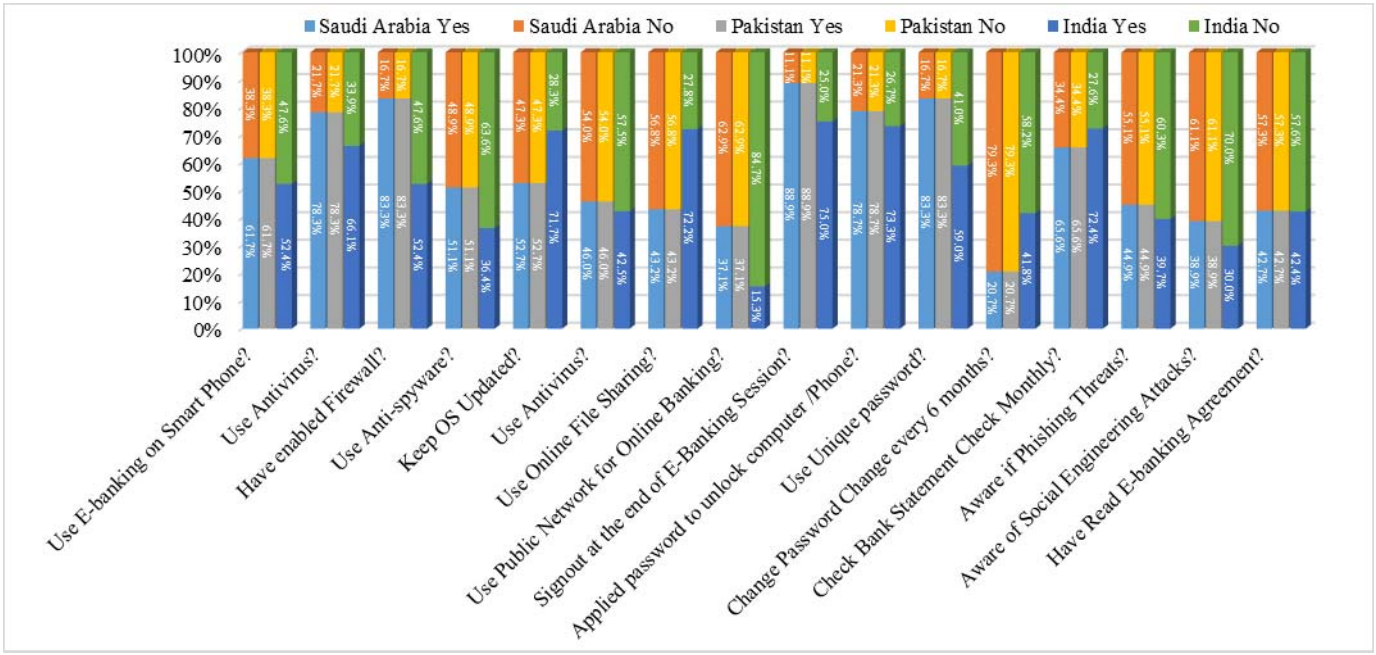

Fig. 2. Survey results from 1044 respondents

Internet banking users should change password every three months, however the bank is responsible to ensure this by expiring the users' password every three months and forcing them to choose a new password. The users should choose a complex password that should not be easy to guess, however it is the bank responsibility to allow only passwords that have combination of capital and small letters, numbers and special characters. Any password that does not have these features will not be accepted. The bank should also enforce that the user should not use the previous two passwords. The Bank can enforce users to use virtual keyboard provided on the webpage by disabling the sensitive fields as there is a chance for the user device to be infected by a malware or a key logger program that detects the key stroke and can compromise the password security.

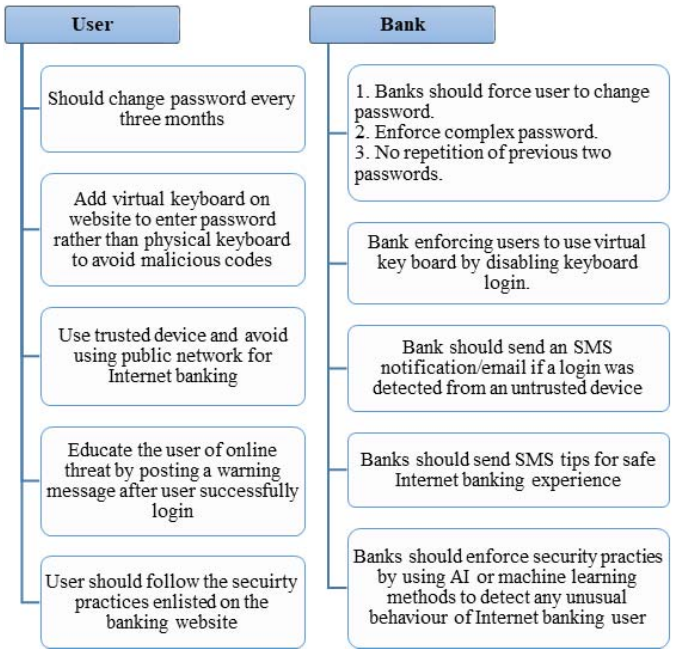

Fig. 3. Proposed security model required to decrease the security risks in Internet banking

Banks should use the concept of trusted device to ensure the user identity. If the user try to login from an untrusted device the bank system should send an SMS alert to confirm if it was the intended user. Education of the users is a key component to ensure safe Internet banking experience. The banks can provide security warning on their webpages after the user has successfully logged in to familiarize users on the threats that are risk for Internet banking. Banks should also use AI or machine learning tools to detect abnormalities in the electronic transactions based on user patterns and take appropriate action.

Information security is a critical part of the Internet banking process. Therefore, banks can improve the security features from their side by securing their servers and the communication between the user and Internet banking server. Table 4 describes the list of security features that each bank should incorporate to ensure the security of user's data and communication.

TABLE 4 Security Features of the Internet banking proposed model

#	Security Feature	Description
1	SSL Certificate	Secure Socket Layer (SSL) certificate should be installed for Internet banking website and other substitute websites representing banks.
2	Device Registration	User access device (laptops, smartphones, tablets etc.) should be registered and device will only be able to access Internet banking systems after verification.
3	System based Alarms	Setup of server based different alarms should be implemented to monitor and control the bank transactions and access of the user accounts etc.
4	Group Policies Settings	Group policies should be applied to make sure that specific users have minimum required access of the banking system resources.
5	MFA	Multifactor Authentication (MFA) method should be used to access the Internet banking administration console to make the infrastructure more secure.
6	SNS	Simple notification should be enabled to the Internet banking services to which will send SMS and email notifications based on the implemented alarms.
7	Inbound / Outbound Rules	Inbound / Outbound access rules should be applied and only specific communication ports (e.g. HTTPS) remain open while rest of the ports should be blocked.
8	Data Encryption	Encryption should be enabled to all the stored data on server by using encryption tools (e.g. bit-locker).
9	Users Access Permissions	Based on the requirement, service based administrative users need to be created with minimum required access polices.
10	Private Key with Password	To make the internet banking infrastructure access more secure, private keys with passwords should be used.

VI. Conclusion

The Internet banking service is offered by banks to provide convenience for their customers, however there is great benefits to banks as well. The most important benefit to banks is the reduction in operational cost be incorporating many services on their online portal. Therefore, the banks should take more responsibility to ensure a more secure Internet banking environment for their customers. In this paper, we proposed a model that incorporates more responsibility on banks to ensure that the Information Technology policies are adhered by customers. For example, the banks should force customers to change their passwords every three months through expiring their passwords. The banks should also integrate the latest Information Security Technologies to ensure that the communication is secure between bank and customers. The proposed model would provide a more secure Internet banking environment which would be of mutual interest to both banks and customers.

References

[1] Xue, M., Hitt, L.M. and Chen, P.Y., 2011. Determinants and outcomes of internet banking adoption. Management science, 57(2), pp.291-307.

[2] Akhlaq, M.A., 2011. Internet banking in Pakistan: finding complexities. Journal of internet banking and commerce, 16(1), p.1.

[3] Cheung, R. and Vogel, D., 2013. Predicting user acceptance of collaborative technologies: An extension of the technology acceptance model for e-learning. Computers & Education, 63, pp.160-175.
[4] Martins, C., Oliveira, T. and Popovič, A., 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), pp.1-13.
[5] Ivan, I., Ciurea, C., Doinea, M. and Avramiea, A., 2012. Collaborative Management of Risks and Complexity in Banking Systems. Informatica Economica, 16(2), pp.128-141.
[6] Gharaibeh, N., 2013. The impact of customer knowledge on the security of E-banking. International Journal of Computer Science and Security (IJCSS), 7(2), p.81.
[7] Council, F.F.I.E., 2005. Authentication in an internet banking environment. Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC). Retrieved March, 18, p.2005.
[8] 1 Chen, C.J., 2016, July. User Adoption Decisions in Self-Service Technologies: A Study of the Internet Banking. In Advanced Applied Informatics (IIAI-AAI), 2016 5th IIAI International Congress on (pp. 1207-1208). IEEE.
[9] Kesharwani, A. and Singh Bisht, S., 2012. The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model. International Journal of Bank Marketing, 30(4), pp.303-322.
[10] Martins, C., Oliveira, T. and Popovič, A., 2014. Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), pp.1-13.
[11] Al-Ajam, A.S. and Md Nor, K., 2015. Challenges of adoption of internet banking service in Yemen. International journal of bank marketing, 33(2), pp.178-194.
[12] Yuen, Y.Y., Yeow, P.H. and Lim, N., 2015. Internet banking acceptance in the United States and Malaysia: a cross-cultural examination. Marketing Intelligence & Planning, 33(3), pp.292-308.
[13] Alwan, H.A. and Al-Zubi, A.I., 2016. Determinants of Internet Banking Adoption among Customers of Commercial Banks: An Empirical Study in the Jordanian Banking Sector. International Journal of Business and Management, 11(3), p.95.
[14] Hanafizadeh, P., Keating, B.W. and Khedmatgozar, H.R., 2014. A systematic review of Internet banking adoption. Telematics and informatics, 31(3), pp.492-510.
[15] Al-Somali, S.A., Gholami, R. and Clegg, B., 2009. An investigation into the acceptance of online banking in Saudi Arabia. Technovation, 29(2), pp.130-141.
[16] Internetlivestats (2017), accessed on January 8, 2017 from http://www.internetlivestats.com/
[17] Saudi Arabian Monetary Agency (SAMA) annual report (2016): http://www.sama.gov.sa/en-US/EconomicReports/Pages/AnnualReport.aspx
[18] Baharat Poddar, Yashraj E., Neetu Chitkara, Abhinav Bansel, 2016. Productivity in Indian Banking. Bostan Consulting Group, Aug, 16.
[19] State Bank of Pakistan annual report (2015/2016): http://www.sbp.org.pk/reports/annual/index.htm
[20] Kierkegaard, S., 2007. Swallowing the Bait, Hook, Line, and Sinker: Phishing, Pharming, and Now Rat-ing!. In Managing Information Assurance in Financial Services (pp. 241-260). IGI Global.
[21] Gan, G.G.G., 2008. Phishing: A Growing Challenge for Internet Banking Providers in Malaysia. Communications of the IBIMA, 5, pp. 133-142.
[22] Dhanalakshmi, R., Prabhu, C. and Chellapan, C., 2011. Detection of phishing websites and secure transactions. IJCNS, 1(11), pp.15-21.
[23] Alghazo, J.M. and Kazimi, Z., 2013. Social Engineering in Phishing Attacks in the Eastern Province of Saudi Arabia. Asian Journal of Information Technology, 12(3), pp. 91-98.
[24] Gao, W. and Kim, J., 2007. Robbing the cradle is like taking candy from a baby. In Proceedings of the Annual Conference of the Security Policy Institute (GCSPI), pp. 23-37.
[25] Dodge, R.C., Carver, C. and Ferguson, A.J., 2007. Phishing for user security awareness. Computers & Security, 26(1), pp.73-80.