Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

Explore the Relationship between Security Mechanisms and Trust in E-Banking: A Systematic Review

Qais Hammouri[1*], Tha'er Majali[2], Dmaithan Almajali[3], Abdalrazzaq Aloqool[4], Jassim Ahmad Al-Gasawneh[5]

[1, 2, 3, 4, 5]Applied Science Private University, Jordan
*q_alhammouri@asu.edu.jo

Abstract

Internet banking security is one of the main critical issues among online users over the world. High level of threats, lack of trust, and fear of loss are the main barriers to utilize online environment. The main goal of this research is to develop a theoretical framework in order to examine the relationship between security and trust in online banking context. The seventh variables were extracted from the previous literatures that are concentrated on the mechanisms of security issues in Internet banking context: presence of confidentiality, presence of integrity, presence of availability, presence of authentication, presence of authorization, presence of non-repudiation and presence of privacy. The suggested research model is depicted at the end of work for future testing.

Keywords: Privacy; Trust; E-Banking; Integrity; Authentication; Authorization; Availability; Non- Repudiation; Confidentiality.

Introduction

Technological developments in electronics have leaded to the preface of technology-based self-service systems which ensuing in the reorganization of many industries offering their services in electronic format known as "e-service" (Shayganmehr & Montazer, 2020). In the banking sector, diverse electronic delivery channels are gradually most used for delivering services and products, in order to achieve a convenience to customers at low cost (Nayanajith et al., 2021). Online banking is a kind of e-commerce in the field of banking and financial services (Singh & Srivastava, 2020). Nevertheless the hasty development of e-banking capabilities carries risks as well as benefits (Zeng & Wu, 2020). Furthermore, customers regularly perceive risks in conducting electronic transactions and for the most part if the transactions involve money (Kaur & Arora, 2020).

Data availability and increased connectivity provide new models for conducting business, but create new security risks. Then and DeLong (1999) stated "*fear of doing financial transactions over the Internet*", this means that security concern is one of the main reasons driving users to avoid making any purchasing over the Internet (Singh & Srivastava, 2020). Security threat is defined as "*a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and fraud, waste, and abuse*" (Kalakota & Whinston, 1996, p. 224).

Moreover, trust is one of the most challenging issues for the banks (Hapuarachchi & Samarakoon, 2020). Several empirical studies approved that there is a positive relationship between consumer trust and their attitudes toward adoption e-banking services (Al-Gharaibah, 2020; Kimiagari & Baei, 2021;

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

Mulia et al., 2020). Such findings mean that if the customers have affirmative attitudes towards online banking, then they have a tendency to trust the transactions done in this manner. However, consumer attitudes must be given more weight by commercial banks to ensure the success of their online services (Ugwuanyi et al., 2020).

Trust is an important factors influencing people's adoption of any technology (Bradford et al., 2020; Elshwikh, 2017). Trust is the catalyst of any transaction among the buyer and seller; it also plays a vital role to improve customer's satisfaction (Zamry & Nayan, 2020). Trust in e-commerce contexts could be utilized to illustrate and understand the intentions of consumer toward e-services (Mumu et al., 2021). Mainly, customers should be recognized that the online transactions are reliable and trusted if they aware with security mechanisms (Belwal et al., 2020). In this study, we will try to develop a theoretical model that depicts the relationship between the security mechanisms (presence of confidentiality, presence of integrity, presence of availability, presence of authentication, presence of authorization, presence of non-repudiation and presence privacy) and trust toward online banking services. The following sections will discuss e-banking and security mechanisms in e-services context.

Literature Review

Security and privacy issues drive to growing the complexity and uncertainty of online banking services (Hammouri & Abu-Shanab, 2020; Rawwash et al., 2020). The risks associated with online banking are increasing, where mechanisms, policies, and models are developed to assess the credibility of such service to each involved party (Chaimaa et al., 2021). Security and trust issues are considered the most factors that examined to understand online the behavioral intention of online services users like e-banking (Usman et al., 2020). Based on that, this study will deeply explore the security concept in e-banking services through utilizing a set of security mechanisms in order to examine their impact on trust.

E-Banking

Although the study of financial services has obtained increased attention over the last few years; there is still to pose challenges for academics and marketers alike. Changing social trends and technological advancements like increasing the preferences of convenience and customer pro activities caused to intense restructuring of the financial services sector (Almajali & Hammouri , 2021; Cruz-García et al., 2020). Internet technology have changed the procedures of financial transactions through allowing customers to perform banking operations on their own, without the need to visit the physical branch office (Khatoon et al., 2020). However, there is still a group of customers favor to visit a bank branch to complete their transactions. Boustani (2020), reported that there are several factors that drive them to visit a bank including: force of habit, perceived greater safety, an unwillingness to learn new ways of banking, trust in the branch, the ability to combine visits to the bank with other activities like shopping, the sense of security of their money that a traditional physical location can bring. Such preferences might be changed during time where online banking services become trusted and secure.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

Online banking has emerged as one of the most profitable ecommerce applications over the last decade (Thusi & Maduku, 2020), which can be defined as the financial service through which customers may perform banking transactions electronically through the Internet and networks via smart devices like smart phones and laptops (Nazaritehrani & Mashali, 2020). Furthermore, the major benefits of online banking where the online banking services helps banks to keep and enhance the loyalty of their obtainable customers, provide opportunity to the banks to increase market share, increase customer satisfaction, reduce operational and administrative cost and to improve banks‘ competitive positions against their rivals (Kimiagari & Baei, 2021). Moreover, conducting online banking transactions assist to reduce the difficulties that are related with driving to the bank, the cost of petrol, and parking. Online banking also allows customers to conduct banking transactions 24 hours a day, 7 days a week, and 365 days a year (AlBalushi, 2021).

Security in E-banking

Security in online banking context is becoming a critical issue hindering the adoption of online banking services. Information about the destinations, activities, and demographic qualities of people using online banking is very valuable to online businesses. Away from the general anxieties with exchange personal information, people may specifically have concerns about becoming increasingly recognition due to increasing the required of personal data (Kumar, M., & Gupta, 2020). Security is considered the main operational risk of e-banking, some of the specific problems cut across risk categories like breach of security letting unauthorized access to customer information (Hammouri et a;., 2021; Safari & Soleimani, 2020). Such security issues may expose the bank to legal and reputational risks. Moreover, risk perception can be classified into six categories as the following: financial risk, time risk, psychological risk, performance risk, confidentiality risk and safety risk. Basically, risk perception could be higher for electronic banking services (Abhilash et al., 2021).

Using open networks such as the Internet environment as a channel to the e-banking environment; issues concerning web security become critical (Santander et al., 2020). Perceived web security refers to the extent to which user believes that the World Wide Web is secure for transmitting sensitive information (Ardiansah et al., 2020). On the other hand, the growth of e-services and use of the Internet face painful setbacks due to the unequal security measures and new emerging threats regarding wireless communications (Gavrilă et al., 2020). However, this will lead to dampen user adoption rate of e-banking technology (Hossain et al., 2020). To reduce the negative effect of such threat, decision makers of online banking should provide all the necessary policies and procedures with regards to privacy, return and fraud protection policies to find more secure e-banking websites and applications (Liyanaarachchi et al, 2020).

Factors Influencing Consumers' Trust to Use E-Banking

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

Several studies approved that perceived security is one of the main factors influencing customers trust to in using online services (Aribake & Mat Aji, 2020; Hammouri et al., 2021; Hossain et al., 2020; Kaur, S., & Arora, 2020; Zalloum et al., 2019). There are common security threats in online environment include user's concerns about confidentiality, integrity, availability, authentication, authorization, non-repudiation and privacy (Alotaibi, 2021). The perception of risk in terms of privacy in m-payment has negative impact on different perspectives like the intention to use mobile commerce, good reputation of online vendors, enticing promises, good encryption security and transparency, reduce the influence of risk and improves the intention to use e-banking (Trinh et al., 2020).

Presence of Confidentiality

The term of confidentiality refers to the extent to which that the communication among users and service provider is not accessible to other parties. Unauthorized access of data and information should be prevented (Klinefelter, 2011). It also aims to include confidentiality of information that is passed over the network and also the confidentiality of information that is stored at storage locations (Prakosa & Sumantika, 2021). Confidentiality is considered as a predictor of trust, because it leads to protect the personal data from unauthorized accessed, it also drives to improve the level of trust for users (Talib et al., 2020). Confidentiality is a security mechanism includes cryptography which refers to the process of encryption of data during transmission and storage it (Shukla, 2021).

Presence of Integrity

Integrity is one of the main components of CIA triangle model. The term means that information should remain unchanged (Sarfraz et al., 2021). Integrity leads to improve trust of online banking based on the reliability of e-banking operations and accuracy of financial transactions (Shayganmehr & Montazer, 2021). Furthermore, integrity as a security mechanism in e-banking context includes several techniques like data encryption, digital signatures and hash functions (Jibril et al., 2020).

Presence of Availability

The concept of availability refers to that information needed by users should be accessible without any bounded restrictions (Shukla et al., 2021). Moreover, availability reflects that the system is reliable and ensures that only authorized people who can access for that system in any time and from any place (Chaimaa et al., 2021). In e-banking context, Internet banking diffusion is fully influenced by data availability (Carranza et al., 2021), and back up servers is one of security mechanisms for availability (Taylor, 2021).

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

Presence of Authentication

The term of authentication is refers to the verification of sender and receiver when communicating over a network (Guo et al., 2021). Authentication concept should be considered entity authentication and data authentication (Chaimaa et al, 2021). Entity authentication deals with verification of the entities involved in a communication, and data authentication deals with the validity of the data during entities transactions (Al Farawn et al., 2020). In e-banking context, authentication with fingerprint and smart card, authentication with bank card and passwords and authentication with digital signatures and passwords are considered as the causative group, while authentication with a bank card, biometric authentication and disposal codes and authentication with digital signatures are considered the effective group (Sepehri-Rad et al., 2019).

Presence of Authorization

The concept of authorization refers to ensure that user accessing information should have the permission to view, manipulate and use (Jøsang, 2017). It has also the rights to send and receive requests from other parties within a system. Permission is one of the major constructs influencing users' behavior to trust in e-banking services (Ghali, 2021). In e-banking context, access control polices is considered a security mechanism for authorization (Mogos & Jamail, 2021).

Presence of Non-Repudiation

The term of non-repudiation refers that the process of sending, receiving and manipulating data or information cannot deny participants involved in a communication process (Fang et al., 2020). Non-repudiation is one of the most important mechanisms that lead to increase the accountability and thus, improve technology adoption (Mohamed, 2020). Digital signatures and certificates are examples of security mechanisms for non-repudiation in e-banking context (Wang & Long, 2020).

Presence of Privacy

Privacy is one of the main important issues that play a significant role to trust in e-banking systems (Bilisbekov et al., 2021; Hammouri et al., 2016; Schomakers et al., 2020). Most of the users are reluctant to adopt and use e-banking services due to the privacy issues (Nayanajith et al., 2021). Loss of privacy leads to loss of confidentiality (Schwab et al., 2011). The main objective of privacy is to ensure that the user information is not accessible to unauthorized people (Mothukuri et al., 2021). Disclosure policies are considered as security mechanisms for privacy in e-banking context (Koskela et al., 2021). Thus, privacy is considered as major factor of building trust and a long-term relationship between the parties over a network (Hammouri & Abu-Shanab, 2017; Kumar, M., & Gupta, 2020).

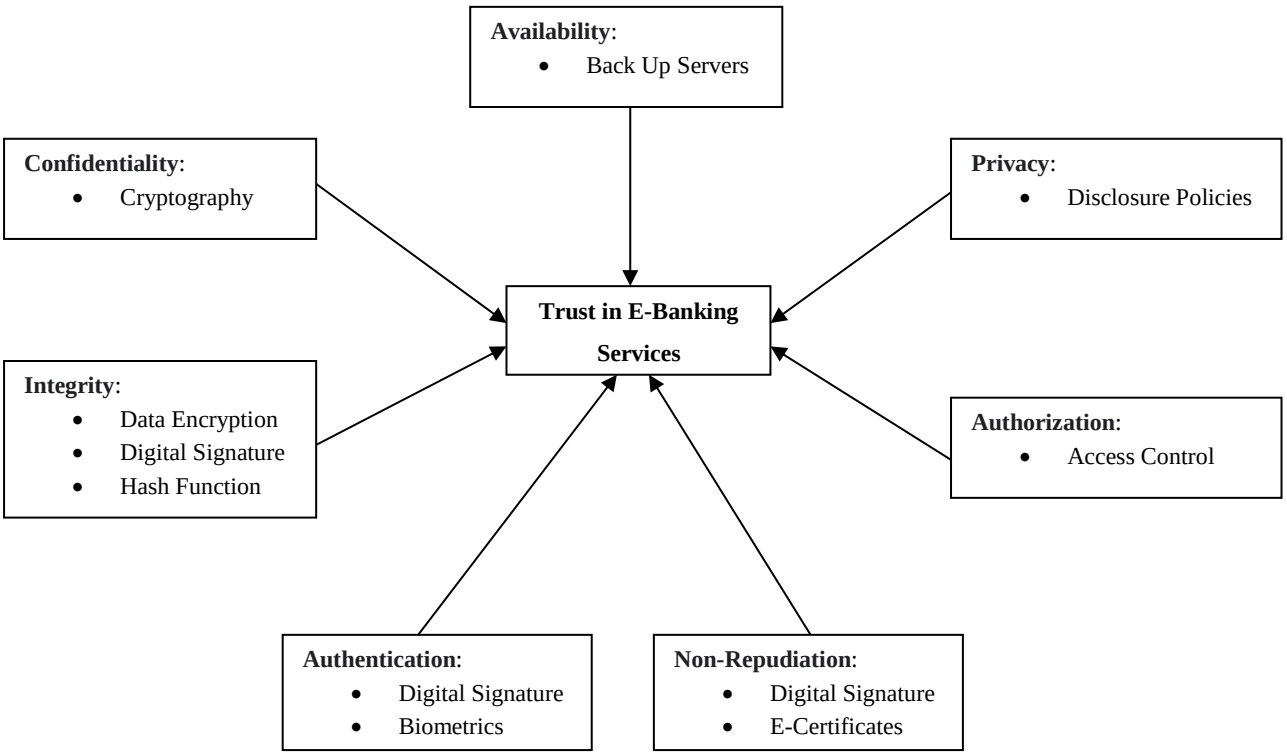
Discussion and Conclusion

This research is concentrated on theoretical framework, based on the previous related research in related to the current study. In this study, we utilized several security mechanisms including presence of confidentiality, presence of integrity, presence of availability, presence of authentication, presence

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

of authorization, presence of non-repudiation and presence of privacy constructs to identify the impact of these factors on consumers' trust toward using e-banking systems in Jordan. Each mechanism includes several techniques that might be utilized to ensure their impact on trust of e-banking services. The figure below describes the proposed model.

Future research is recommended to test such model with e-banking services users or organizations as the unit of analysis. The researchers are looking forward to developing a survey in the future to distribute and fill by users or organizations to test the framework practically to confirm the results of previous studies in relationship between security mechanisms and trust in e-banking environment.



References:

[1] Abhilash, V. S., Vipin, H., & Pillai, S. V. (2021). A Study on the E-banking Services and Risk Perception with Reference to Trivandrum. *Asian Journal of Economics, Finance and Management*, 43-52.

[2] Al Farawn, A., Rjeib, H. D., Ali, N. S., & Al-Sadawi, B. (2020). Secured e-payment system based on automated authentication data and iterated salted hash algorithm. *Int J Pow Elec & Dri Syst ISSN*, *2088*(8694), 8694.

[3] AlBalushi, T. H. (2021). E-Services Quality: A Perspective of Service Providers and Service Users. In *E-Service*. IntechOpen.

[4] Al-Gharaibah, O. B. (2020). Predictors of E-banking Service Adoption in Malaysia Using an Extended Technology Acceptance Model. *Int. J. Contemp. Manag. Inf. Technol*, *1*(1), 23-29.

[5] Alotaibi, A. F. (2021). A Comprehensive Survey on Security Threats and Countermeasures of Cloud Computing Environment. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(9), 1978-1990.

[6] Ardiansah, M., Chariri, A., Rahardja, S., & Udin, U. (2020). The effect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. *Management Science Letters*, *10*(7), 1473-1480.

[7] Aribake, F. O., & Mat Aji, Z. (2020). The Mediating Role of Perceived Security on the Relationship Between Internet Banking Users and Their Determinants. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *11*(2).

[8] Belwal, R., Al Shibli, R., & Belwal, S. (2020). Consumer protection and electronic commerce in the Sultanate of Oman. *Journal of Information, Communication and Ethics in Society*.

[9] Bilisbekov, N., Sarfo, C., Dandis, A., & Eid, M. (2021). Linking bank advertising to customer attitudes: The role of cognitive and affective trust. *Management science letters*, *11*(4), 1083-1092.

[10] Boustani, N. M. (2020). Traditional Banks and Fintech: Survival, Future and Threats. In *ICT for an Inclusive World* (pp. 345-359). Springer, Cham.

[11] Bradford, B., Yesberg, J. A., Jackson, J., & Dawson, P. (2020). Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology*, *60*(6), 1502-1522.

[12] Carranza, R., Díaz, E., Sánchez-Camacho, C., & Martín-Consuegra, D. (2021). e-Banking adoption: an opportunity for customer value co-creation. *Frontiers in Psychology*, *11*, 4003.

[13] Chaimaa, B., Najib, E., & Rachid, H. (2021). E-banking Overview: Concepts, Challenges and Solutions. *Wireless Personal Communications*, *117*(2), 1059-1078.

[14] Cruz-García, P., Forte, A., & Peiró-Palomino, J. (2020). On the drivers of profitability in the banking industry in restructuring times: a Bayesian perspective. *Applied Economic Analysis*.

[15] Elshwikh, Y. (2017). A trust and reputation model for quality assessment of online content. *International Journal of Advanced Computer Science and Applications*, *8*(3), 58-61.

[16] Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 1-15.

[17] Gavrilă, V., Băjenaru, L., Tomescu, M., & Dobre, C. (2020, June). Security Measures Analysis Related to Intellit Platform. In *2020 13th International Conference on Communications (COMM)* (pp. 93-96). IEEE.

[18] Ghali, Z. (2021). Motives of customers'e-loyalty towards e-banking services: a study in Saudi Arabia. *Journal of Decision Systems*, 1-22.

[19] Guo, C., Campbell, B., Kapadia, A., Reiter, M. K., & Caine, K. (2021). Effect of Mood, Location, Trust, and Presence of Others on Video-Based Social Authentication. In *30th {USENIX} Security Symposium ({USENIX} Security 21)*.

[20] Hammouri, Q., & Abu-Shanab, E. (2017, May). The antecedents of trust in social commerce. In *2017 8th International Conference on Information Technology (ICIT)* (pp. 648-652). IEEE.

[21] Hammouri, Q., & Abu-Shanab, E. A. (2020). Major Factors Influencing the Adoption of Cloud Computing in Jordan. *International Journal of Technology and Human Interaction (IJTHI)*, *16*(4), 55-69.

[22] Hammouri, Q., Abu-Shanab, E., & Manasrah, A. (2016). Examining the Impact of Privacy, Security and Law on Trust in Mobile Computing. *Saba Journal Of information Technology And Networking (SJITN)-ISSN: 2312-4989*, *4*(1).

[23] Hammouri, Q. M., Abu-Shanab, E. A., & Nusairat, N. M. (2021). Attitudes Toward Implementing E-Government in Health Insurance Administration. *International Journal of Electronic Government Research (IJEGR)*, *17*(2), 1-18.

[24] Almajali, D. A., & Hammouri, Q. (2021). Predictors of Online Shopping During Covid-19 Pandemic in Developing Country: Qualitative Analysis. *Annals of the Romanian Society for Cell Biology*, *25*(6), 12970-12977.

[25] Hammouri, Q., Al-Gasawneh, J. A., Nusairat, N. M., Hanandeh, A., & Barakat, S. (2021). The Determinants of Trust and its Influence on Online Buying Intention: An Empirical Study on Social Commerce in Jordan. *Annals of the Romanian Society for Cell Biology*, 4522-4539.

[26] Hapuarachchi, C., & Samarakoon, A. (2020). Drivers Affecting Online Banking Usage of Private Commercial Banks in Sri Lanka. *Asian Journal of Economics, Business and Accounting*, 1-10.

[27] Hossain, S. A., Bao, Y., Hasan, N., & Islam, M. F. (2020). Perception and prediction of intention to use online banking systems: An empirical study using extended TAM. *International Journal of Research in Business and Social Science (2147-4478)*, *9*(1), 112-116.

[28] Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In *International Conference on Cyber Warfare and Security* (pp. 270-XV). Academic Conferences International Limited.

[29] Jøsang, A. (2017, September). A consistent definition of authorization. In *International Workshop on Security and Trust Management* (pp. 134-144). Springer, Cham.

[30] Kalakota, R., & Whinston, A. B. (1996). *Frontiers of electronic commerce*. Addison Wesley Longman Publishing Co., Inc.

[31] Kaur, S., & Arora, S. (2020). Role of perceived risk in online banking and its impact on behavioral intention: trust as a moderator. *Journal of Asia Business Studies*.

[32] Khatoon, S., Zhengliang, X., & Hussain, H. (2020). The Mediating Effect of customer satisfaction on the relationship between Electronic banking service quality and customer Purchase intention: Evidence from the Qatar banking sector. *SAGE Open*, *10*(2), 2158244020935887.

[33] Kimiagari, S., & Baei, F. (2021). Promoting e-banking actual usage: mix of technology acceptance model and technology-organisation-environment framework. *Enterprise Information Systems*, 1-57.

[34] Klinefelter, A. (2011). When to Research is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking. *Va. JL & Tech.*, *16*, 1.

[35] Koskela, A., Jälkö, J., Prediger, L., & Honkela, A. (2021, March). Tight differential privacy for discrete-valued mechanisms and for the subsampled gaussian mechanism using fft. In *International Conference on Artificial Intelligence and Statistics* (pp. 3358-3366). PMLR.

[36] Kumar, M., & Gupta, S. (2020). Security perception of e-banking users in India: an analytical hierarchy process. *Banks and Bank Systems*, *15*(1), 11.

[37] Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2020). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*.

[38] Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 1065-1072.

[39] Mohamed, K. S. (2020). Cryptography Concepts: Integrity, Authentication, Availability, Access Control, and Non-repudiation. In *New Frontiers in Cryptography* (pp. 41-63). Springer, Cham.

[40] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. *Future Generation Computer Systems*, *115*, 619-640.

[41] Mulia, D., Usman, H., & Parwanto, N. B. (2020). The role of customer intimacy in increasing Islamic bank customer loyalty in using e-banking and m-banking. *Journal of Islamic Marketing*.

[42] Mumu, J. R., Saona, P., Mamun, M. A. A., & Azad, M. A. K. (2021). Is Trust Gender Biased? A Bibliometric Review of Trust in E-Commerce. *Journal of Internet Commerce*, 1-29.

[43] Nayanajith, D. A. G., Dissanayake, D. M. R., Weerasiri, R. A. S., & Damunupola, K. A. (2021). Perceived Trust of E-Services, Perceived Usefulness and Adoption of E-Banking amongst the Students of University of Kelaniya: A Relational Study. *Vidyodaya Journal of Management*, *7*(1).

[44] Nazaritehrani, A., & Mashali, B. (2020). Development of E-banking channels and market share in developing countries. *Financial Innovation*, *6*(1), 12.

[45] Prakosa, A., & Sumantika, A. (2021, March). An Analysis of Online Shoppers' Acceptance and Trust toward Electronic Marketplace using TAM Model. In *Journal of Physics: Conference Series* (Vol. 1823, No. 1, p. 012008). IOP Publishing.

[46] Rawwash, H., Masad, F., Enaizan, O., Eneizan, B., Adaileh, M., Saleh, A., & Almestarihi, R. (2020). Factors affecting Jordanian electronic banking services. *Management Science Letters*, *10*(4), 915-922.

[47] Safari, S., & Soleimani, R. (2020). E-banking Operational Risk Man-agement Analysis by Self Assessment Approach (A Case Study: a State Bank). *Commercial Strategies*, *9*(47), 309-320.

[48] Santander, C. J. M., Moreno, H., & Alvarez, M. B. H. (2020, October). The evolution from Traditional to Intelligent Web Security: Systematic Literature Review. In *2020 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1-9). IEEE.

[49] Sarfraz, M., Alsoraya, D., AlBathali, A., & Al-Mayyas, O. (2021). An Automated Management System for Student e-Services. *Information Sciences Letters*, *10*(1), 9.

[50] Schomakers, E. M., Biermann, H., & Ziefle, M. (2020, July). Understanding Privacy and Trust in Smart Home Environments. In *International Conference on Human-Computer Interaction* (pp. 513-532). Springer, Cham.

[51] Schwab, A. P., Frank, L., & Gligorov, N. (2011). Saying privacy, meaning confidentiality. *The American Journal of Bioethics*, *11*(11), 44-45.

[52] Sepehri-Rad, A., Sadjadi, S., & Sadi-Nezhad, S. (2019). An application of DEMATEL for transaction authentication in online banking. *International Journal of Data and Network Science*, *3*(2), 71-76.

[53] Shayganmehr, M., & Montazer, G. A. (2020). An extended model for assessing E-Services of Iranian Universities Websites Using Mixed MCDM method. *Education and Information Technologies*, 1-35.

[54] Shayganmehr, M., & Montazer, G. A. (2021). A novel hybrid assessment model to evaluate e-services websites of Iranian municipalities. *Artificial Intelligence Review*, 1-35.

[55] Shukla, A. K. (2021). Proposed E-Services Quality Model and its Impact on the Indian Society. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 4231-4242.

[56] Singh, S., & Srivastava, R. K. (2020). Understanding the intention to use mobile banking by existing online banking customers: an empirical study. *Journal of Financial Services Marketing*, *25*(3), 86-96.

[57] Talib, Z. M., Haruna, S., & Kassim, N. M. (2020). Assessing Trust and Intention to Continue Using Internet Banking Through Security Dimension Impact: A Partial Least Squares Analysis. *International Journal of Enterprise Information Systems (IJEIS)*, *16*(2), 134-147.

[58] Taylor, A. R. E. (2021). Standing by for data loss: Failure, preparedness and the cloud. *ephemera: theory & politics in organization*, *21*(1).

[59] Then, N. K., & DeLong, M. R. (1999). Apparel shopping on the web. *Journal of Family and Consumer Sciences*, *91*(3), 65.

[60] Thusi, P., & Maduku, D. K. (2020). South African millennials' acceptance and use of retail mobile banking apps: An integrated perspective. *Computers in Human Behavior*, *111*, 106405.

[61] Trinh, H. N., Tran, H. H., & Vuong, D. H. Q. (2020). Determinants of consumers' intention to use credit card: a perspective of multifaceted perceived risk. *Asian Journal of Economics and Banking*.

[62] Ugwuanyi, C. C., Uduji, J. I., & Oreedu, C. (2020). Customer experience with self-service technologies in banking sector: Evidence from Nigeria. *International Journal of Business and Systems Research*, *14*(4), 241-270.

[63] Usman, O., Monoarfa, T., & Marsofiyati, M. (2020). E-Banking and mobile banking effects on customer satisfaction. *Accounting*, *6*(6), 1117-1128.

[64] Wang, M., & Long, Y. (2020, November). SM9 Digital Signature with Non-repudiation. In *2020 16th International Conference on Computational Intelligence and Security (CIS)* (pp. 356-361). IEEE.

[65] Zalloum, L., Alghadeer, H., & Nusairat, N. (2019). The Effect of Using Mobile Banking Services Applications on Electronic Word of Mouth: The Mediating Role of Perceived Trust. *International Business Research*, *12*(9), 62-80.

[66] Zamry, A. D., & Nayan, S. M. (2020). What Is the Relationship Between Trust and Customer Satisfaction?. *Journal of Undergraduate Social Science and Technology*, *2*(2).

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 17083-17093
Received 25 April 2021; Accepted 08 May 2021.

[67] Zeng, L., & Wu, N. (2020, January). Research on the service quality of personal online banking from the perspective of the new generation. In *5th International Conference on Economics, Management, Law and Education (EMLE 2019)* (pp. 741-745). Atlantis Press.