IIUC Business Review, Vol.-10, Issue-1, Dec. 2021
DOI: https://doi.org/10.3329/iiucbr.v10i1.62094

Security of E-Banking transactions in Bangladesh: Does it need more importance from COVID-19 perspective?

Md. Shahidul Islam
Service Engineering Division
Bangladesh Forest Research Institute, Chattogram, Bangladesh
Monir Ahmmed
Department of Economics & Banking
International Islamic University Chittagong (IIUC), Bangladesh
Md. Shahnur Azad Chowdhury
Department of Business Administration
International Islamic University Chittagong (IIUC), Bangladesh

Abstract
Electronic banking service has grown in Bangladesh since 2001. Now, it has become most suitable and convenient fund transfer method in COVID-19 pandemic situation. The security risk issue is the most vital in the e-banking fund transfer. A survey was conducted where the risk factors were measured on five-point Likert scale by 200 bankers and customers in the pandemic period through phone and E-mail. After necessary modification and correction of collected data, descriptive statistics, Cronbach's Alpha, Kolmogorov-Smirnov test, Shapiro-Wilk test, Mann Whitney U test and Kruskal-Wallis H test were conducted in IBM SPSS Statistics 20 and MS Excel 2010to test the hypothesis of the risk factor. Result shows the highest banking transaction risk factor is Account Information Security and lowest banking transaction risk factor is Double Check identity from the perspective of customers. The result also shows that less than 2 years experiences of e-banking are significantly more satisfied than the risk factor of 2 years to 6 years and more than 6 years e-banking experiences.

Keywords E-banking, Security, Risk, COVID-19

Paper type Research paper

Introduction
As the usage of electronic banking increases, banking industry is changing (Jadhav, 2019) which results in the enhanced customer loyalty. E-banking has steadily grown in poorer countries as well (Neger & Uddin, 2020). There are significant risks associated with all of these information flowing from one end to the other via the internet. Many ways exist for information to be hacked or leaked. Financial

IIUC Business Review
Vol.-10, Issue-1, Dec. 2021
pp. 9-24

ISSN 1991-380X

organizations must consider cyber security carefully and take appropriate measures to protect their data. However, the Bangladesh Bank cyber robbery in the recent past has caused concern among think tanks and professionals regarding cyber attacks. The research is focused on determining the most common financial attacks.

Individuals and institutions' reliance on cyberspace for social networking, e-commerce, and internet banking is a developing problem around the world. As we become increasingly reliant on the internet, hackers have a larger cyber realm in which to commit cybercrime. It is also critical for institutions to address the problems they may have in adopting cyber security and securing customer and financial data through the use of technology.

Any lacking in security of e-banking could cause havoc to the banks as well as for the retailers, organizations which perform their transactions through those banks. But, the banks have much more liability than those of the bank's customers. The recent security flaws with respect to ATM card fraud and Bangladesh Bank unauthorized money transfer have shaken the whole banking industry. The banking sector has to rethink about the way it should be dealt with its information systems. They have to review the information system security and control as per the standards explained in books. Such standard are explained in various texts.

1. Research gap

During the pandemic, Bangladesh's private banks advised their customers to use bank applications rather than frequent branch visits for whatever cause. However, no study has yet been published that compares mobile banking performance during the COVID-19 pandemic and pre-Covid period.

Bangladesh has introduced the Digital Security Act of 2018, which addresses the problem of cybercrime. The measure is intended to address growing worries about digital security. It should be highlighted, however, that the Act is part of a larger regulatory ecosystem for information technology During the pandemic, five benefits were realized: location-based services which saved money, services were available at any time, services were convenient, and transaction/data processing was secure. "Ensures security in transaction/data processing" is the lowest ranked IoT benefit. However, hackers could potentially reroute consumers to a fake NatWest website that looks likes exactly a real one. Because of its ease and timesaving benefits, internet banking has become extremely popular in Bangladesh. Only a few research on data security have been discovered. During the pandemic, there was a lot of fraud and violations of the law. Therefore, more attention is required to ensure the security of data processing.

2. Objectives of the study

The following objectives have been identified for the current research study.

- To have idea about e-banking transaction risk.
- To identify the most significant risk factor during COVID-19 situation.
- To identify the actions to be taken to overcome the risk situation during post COVID period.

3. Literature review

Khalil, Ahmad, & Khan conducted an investigation in which they examined the perspective of the clients, they fund that the overall increase in education, particularly computer literacy, as well as the developing large network of Internet Service Providers(ISPs) will provide an enabling environment that will allow the customer to feel secure when doing banking transactions over the internet. Nastaran Mohammad Hosseini, Shidrokh Goudarzi and Mohammad Nazir Ahmad conducted a research in the year 2013 in which they evaluated the following issues-According to the data, trust has a beneficial impact on the uptake of Internet banking services by consumers. Furthermore, the findings indicate that there are a variety of elements that influence confidence in electronic services. The vast bulk of the study has been carried out in the context of Internet-based banking. With these research as a foundation, the review offered in this paper provides an overview of the key characteristics that may influence people's trust in online banking services in general. Redwanuzzaman and Islam (2013) investigated and found that the number of people who utilize electronic banking is growing considerably. It has, however, gained remarkable popularity among bank customers in recent years, and it is hoped that this popularity will continue to grow day by day as the product is nurtured by expert bankers. In their research, Islam & Imran (2020) found that perceived utility, social impact, and perceived enjoyment were all shown to be significant predictors of persons' propensity to use online banking services in Bangladesh. The findings also revealed that perceived utility had the greatest significant impact on an individual's behavioural intention to use online banking in this nation, outweighing social influence by a factor of two to one. In the year 2014, Saquib Shahriar conducted a study and discovered in contrast to international banks, internet-based banking has only lately been offered by a number of big private and national banks, as well as certain regional banks. Despite the fact that many banks have made significant investments in online banking, the adoption of internet banking has not been as rapid as anticipated.

Majumder, and Donghui (2016) conducted study and discovered that customer satisfaction with e-banking and banking issues are both high.

According to the findings of this study, Bangladeshi clients do not have sufficient understanding about e-banking, which is being provided by the banking industry in the country. In accordance with the findings of this study, customer acceptance and usage of e-banking technologies are connected to both individual consumer traits as well as a specific technology. Munir (2017) conducted a research in which it is demonstrated that bank management is responsible for ensuring the security of E-banking transactions for not only customers, but also for their own bank employees. According to Md. Mohiuddin's research published in 2014, in order for E-banking to continue to flourish, the security and privacy components of the system must be enhanced. If the security and privacy concerns are addressed, the future of E-banking has the potential to be very lucrative. It is anticipated that the future of electronic banking will be a system in which customers will be able to communicate with their banks "worry-free," and in which institutions would operate under a single set of rules. Skvarciany and Jurevičienė (2018) conducted a study in the year 2018 in which they found that trust building differs in each of the analyzed countries. According to the experts, the e-banking system is the most effective factor in the trust-building process in Lithuania and Latvia, while the website is the most important component in Estonia. The following?? constraints apply to this investigation: The online survey of individual customers (however, because internet banking is geared toward internet users, this limitation is not critical); the analysis of only the trust-building criteria that have a positive impact; and the assessment of only the subfactors by experts were the only limitations. According to Sadekin and Shaikh (2016) Bangladeshi banks are performing their e-banking services with the assistance of non-technical personnel. The majority of Bangladeshi clients, both male and female, are unaware of the importance of e-bank security. Many of them do not have access to a computer at their place of abode. Female users are more conscientious than their male counterparts. Customers' confidence is dependent on a variety of factors, including security measures, customer awareness, educational qualification, verification of e-transactions, the quality of e-services provided by banks, and the behavior of bankers. It is also possible that consumers' trust may be diminished if they have difficulty in making an electronic transfer, which would result in decreased confidence.

4. The importance of online banking security

Through the widespread use of information technology, the level of various personal and professional work has increased manifold. In particular, there is a growing demand for digital media as a special means of reducing time,

distance, and cost, especially in people's daily financial transactions. Just as it has facilitated the various activities of our lives through digital devices, its use has created issues of concern about security, privacy, security, risk. We obtain financial services such as fund transfers, fund withdrawals, deposits, data exchange, and more important work with which security and privacy have a special relationship through banks. In many cases, customers are not aware or do not realize that being aware is the reason why customers have to suffer an irreparable loss, in this case (Nilsson, Adams, & Herd, 2005).

High-profile data breaches in 2017 prompted increased scrutiny of banks and businesses to ensure that they have adequate security measures in place. Natwest was chastised for failing to employ an encrypted https (Hypertext Transfer Protocol Secure) connection on the customer portion of their website. An external security expert noticed the lack of an encrypted https and informed the public via Twitter. Because of this security issue, hackers could potentially reroute consumers to a fake NatWest website that looks exactly like the real one. Despite the fact that the team was able to remedy the issue in less than 48 hours, the vulnerability exposed NatWest to a slew of security and legal risks (Haque, 2019).

Because of its ease and timesaving benefits, internet banking has become extremely popular in Bangladesh. It has shuttered physical branches for many customers. When it comes to switching from ‘offline' to ‘online' banking, however, security is still a major worry for customers, and banks must assure both client satisfaction in terms of convenience as well as rigorous regulatory limitations in order to stay in business.

Naturally, financial institutions must secure consumer data in order to preserve safety, security, integrity, and privacy of information systems. The DPA mandates that businesses take necessary technological and organizational measures to protect personal data against unauthorized or unlawful processing, as well as accidental loss, deletion, or damage. Despite the fact that the DPA does not specify how appropriate organizational and technical measures should be implemented in accordance with this principle, data controllers must ensure that data is not compromised in any way. (Alam, Jesmin, Faruk, & Nur-Al-Ahad, 2021).??

5. Various type of attack on internet

i. Phishing: Phishing is an e-mail deception method in which an attacker sends a legitimate-looking email to the recipients with the aim of collecting personal and financial information. Phishing is the act of impersonating a real person or company over the internet in order to get credentials, passwords, credit card details, and, in some situations, money.

ii. Spyware and Adware: When referring to any form of application that shows unsolicited advertisements at the time of software being used which are downloaded from internet, the term "ad supported software" also known as "adware" or "advertising supported software" comes to mind. Adware is frequently included in software packages purchased by computer users. Adware is occasionally included in software by its creators in order to recoup development costs or to offer the product at reduced cost. This adware may be programmed to gather information about which websites a user search or move, send that information back to the organization, and then deliver advertisements based on that data. Although the adverts?? generated by adware may be considered an inconvenience, a distracting, or a violation of secrecy by the user, the revenue received by the designer may be used to improve, maintain and develop new products. A user may choose to buying a licensed or registered products without adware where this adware-free products might also contain some extra features.

iii. Computer virus: When a computer virus is executed, it multiplies by making replicas of itself (potentially changed) into other computer programs, files or important segment of Hard Disk Drive (HDD), once this reproduction occurs in the affected zones are referred to as "infected". Virus often causes many harmful activities on affected or infected areas like damaging memory space or killing CPU time, altering private information and displaying that information on the screen of users, logging their keystrokes, spamming their contacts or even making the system inoperable. Viruses, on the other hand, are own replicating programs on computer systems that installed themselves without permission or knowledge of users, not all of which contain a harmful message or seek to disguise themselves.

iv. Trojans: Trojans are another type of malevolent software that perform actions that have not been authorized by the user such as deleting, blocking, modifying and copying data from original sources. It also causes the performance bottleneck in the computing system or the network of computing system.

v. Key loggers: A key logger, also known as a keystroke by logger or system monitor, is a computer hardware or software application for recording every keystroke typed on a keyboard of computer device. As a physical device, a key logger is a tiny battery-powered plug that connects the user's keyboard to their computer. It is very easy for someone who wishes to monitor a user's activity to physically hide such a device "in plain sight" because the device matches a conventional keyboard connector.

6. Computer protection against the attacks on internet

For many corporate companies, security technique [9, 10] is a hot topic. It is clear that the services provided by the banks to their customers must ensure their clients' safety. As a result, such clients became more pleased to this service. In some ways, a banking institution has, therefore, some responsibility to keep things in order. Banks are required to supply some security principles in order to protect E-banking. Because numerous transactions are conducted via electronic media in this instance, banks are unable to operate without protecting their financial activities. For security purposes, Islam (2015) has offered the following way to guard against computer assaults:

i. Authentication: Authentication is a process that ensures the impression that both parties are involved through a discussion between the transaction or the data exchange. This is usually done through two types of methods i) Password authentication and ii) Biometric authentication.

ii. Confidentiality: It works to protect data from many hackers or an unauthorized users during data transfer over the Internet. For example, anybody wants to secure the information of his ATM card at the time of spending over the Cyber space.

iii. Data integrity: Data integrity ensures data security, accuracy and consistency throughout the time of data transmission. It also ensures data traceability and searchability to its original source during data transmission. For instance, the ATM card number is secured , and the messages do not contain any information about the online order.

iv. Non-repudiation: This usually ensures that no user can ignore a valid issue of security arrangements for stopping an information from fraudulence. Sometimes, it might be extremely costly for e-business transections that wish to ensure that a consumer cannot deny having ordered to decide whether to buy or sell desire consumptions.

7. Analysis

Hypothesis H0: 1

There is no significant difference of e-bank risk factor value for gender.

Alternative Hypothesis:

There is significant difference of e-bank risk factor value for gender.

Hypothesis H0: 2

There is no significant difference of e-bank risk factor value for e-banking

role.
Alternative Hypothesis:
There is significant difference of e-bank risk factor value for e-banking role.
Hypothesis H0: 3
There is no significant difference of e-bank risk factor value for e-banking experience.
Alternative Hypothesis:
There is significant difference of e-bank risk factor value for e-banking experience.

8. Methods

Recently, electronic banking is the first growing phenomenon in the field of e-commerce in fund transfer of Bangladesh during COVID-19 pandemic situation for last few years. Security is the most important risk issue of e-commerce fund transfer. To measure the security risk issue a survey questionnaire was developed in the study with the help of service provider (banker), service receiver (customer) and service facilitator (network engineer). After discussion with the respondents, necessary modification and correction were made to distribute the final questionnaire to 200 respondents in the commercial and port city Chattogram (22°14' and 22°24' N Latitude and between 91°46' and 91°53' E Longitude) of Bangladesh. The survey response was collected form 80 (40%) service provider (banker) and 120 (60%) service receiver (customer) during March 2021 to April 2021 by direct communication and E-mail. For the study132 male (66%) and 68 female (34%) respondents were selected through random sampling methods. 57 respondents (28.5%) have started e-banking during COVID 19 situation (less than 2 years), 106 respondents (53%) have medium e-banking (2 years to 6 years) experience and 37 respondents (18.5%) have long (more than 6 years) experience. The response data were coded in IBM SPSS Statistics 20 and MS Excel 2010 after necessary modification and correction. The descriptive statistics and Cronbach's Alpha values of the response data were calculated for data validity and reliability. The rick factor of each measured variable was determined as the standard deviation. Then data normality was checked by Kolmogorov-Smirnov test and Shapiro-Wilk test. Finally, Mann Whitney U test and Kruskal-Wallis M test were conducted to test the hypothesis of the risk factor among the demographic factors.

9. Result and discussion

The descriptive statistics of the risk factor of the survey response data is shown in Table 1.

Table 1
Descriptive statistics and risk factor

Sl. Questionnaire	Variable name	N	Min	Max	Sum	Mean	Standard deviation/Risk
1. Double check protection of identity to access with multiple devices pass ward	Double Check Identity	200	2	5	697	3.49	0.913
2. Quick notification activities of authentication to make the system more reliable and convenient	Quick Notification Authentication	200	2	5	706	3.53	0.918
3. Quick notification of any irregular suspicious account activity/transaction	Quick Notification Activity	200	2	5	705	3.53	0.935
4. Proper help of a new card/lost bank card/block bank account/ held up payment	e-Banking Proper Help	200	2	5	724	3.62	0.949
5. Instant support of help desk of operation mistake/transfer money or anything else	Mistake Instant Support	200	2	5	723	3.62	0.939
6. Provide full security of account information and privacy of account maintenance	Account Information Security	200	2	5	702	3.51	0.940
7. Afraid of hacking of bank account	Afraid Account Hacking	200	2	5	701	3.51	0.930
8. Afraid of e-banking services for possible disadvantages/risks	Afraid Banking Service	200	2	5	714	3.57	0.916

The minimum survey response value is 2 and maximum value is 5 of the 200-survey respondents. The mean and standard deviation of Double Check identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are 3.49 ± 0.913, 3.53± 0.918, 3.53± 0.935, 3.62± 0.949, 3.62± 0.939, 3.51± 0.940, 3.51± 0.930and 3.57± 0.916 respectively. Here risk has been measured as the standard deviation of survey response data. So, the highest banking transaction risk factor is Account Information Security (0.940) and lowest banking transaction risk factor is Double Check identity (0.913).

Table 2
Normality and hypothesis test

Sl.	Variable name	Cronbach's Alpha	Kolmogorov-Smirnov test statistic (sig.)	Shapiro-Wilk test statistic (sig.)	Mann-Whitney U Test Z (Sig.) for gender	Mann-Whitney U test Z (Sig.) for e-Bank role	Kruskal Wallis H Test Chi-Square (Sig.) for e-Bank experience
1.	Double Check Identity		0.227 (0.000)	0.878 (0.000)	0.358 (0.720)	4.497 (0.000)	6.256 (0.044)
2.	Quick Notification Authentication		0.213 (0.000)	0.880 (0.000)	0.104 (0.916)	3.930 (0.000)	11.097 (0.004)
3.	Quick Notification Activity		0.238 (0.000)	0.874 (0.000)	1.309 (0.190)	4.246 (0.000)	7.317 (0.026)
4.	e-Banking Proper Help		0.206 (0.000)	0.879 (0.000)	0.334 (0.738)	4.452 (0.000)	9.273 (0.010)
5.	Mistake Instant Support	0.956	0.214 (0.000)	0.879 (0.000)	0.580 (0.561)	5.425 (0.000)	5.910 (0.050)
6.	Account Information Security		0.231 (0.000)	0.877 (0.000)	0.929 (0.352)	4.162 (0.000)	6.572 (0.037)
7.	Afraid Account Hacking		0.207 (0.000)	0.881 (0.000)	0.683 (0.494)	5.290 (0.000)	8.681 (0.013)
8.	Afraid Banking Service		0.216 (0.000)	0.879 (0.000)	0.963 (0.335)	4.471 (0.000)	9.238 (0.010)

The Cronbach's Alpha value (0.956) shows (in Table 2) the survey response data values are most reliable and consistent. The Kolmogorov-Smirnov test statistic of the Double Check identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are0.227, 0.213, 0.238, 0.206, 0.214, 0.231, 0.207 and 0.216 respectively (at the significance level 0.000). Also, the Shapiro-Wilk test statistic value of Double Check identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are0.878, 0.880, 0.874, 0.879, 0.879, 0.877, 0.881 and 0.879

respectively (at the significance level 0.000). So, the survey questionnaire response values of each factor are ordinal data and not normally distributed ($p < 0.05$). So, Mann-Whitney U test and Kruskal Wallis H Test were selected to determine the significant difference of risk factor value for each demographic variables and result is shown in Table 2. The gender risk factor value (Figure 1), e-banking role risk factor value (Figure 2) and bank experience risk factor value (Figure 3) have been shown as follows.

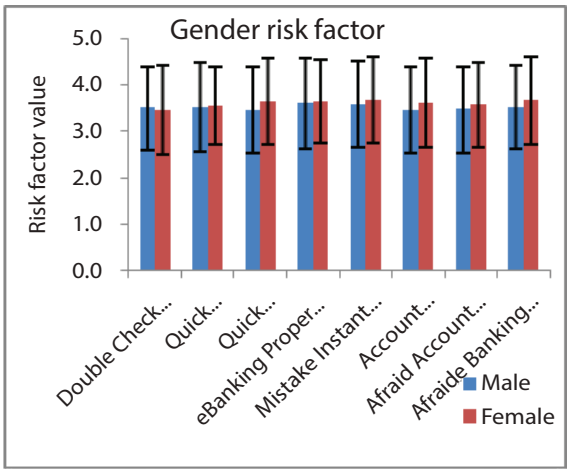

Figure 1
Gender risk factor

The gender risk factor value (Figure 1) for male is higher for Double Check Identity and lower for the other factors. The Z statistic of Mann-Whitney U Test for Double Check Identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake Instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are0.358 (p 0.720), 0.104 (p 0.916), 1.309 (p 0.190), 0.334 (p 0.738), 0.580 (p 0.561), 0.929 (p 0.352), 0.683 (p 0.494) and 0.963 (p 0.335) respectively. Therefore, the hypothesis 1 is accepted. So, there is no significant difference of e-bank risk factor value for gender.

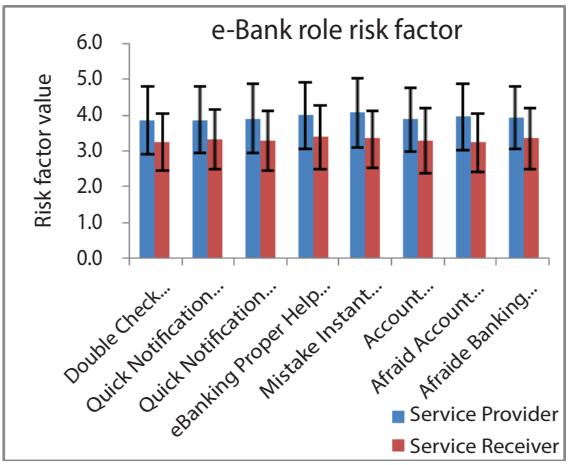

Figure 2
e-banking role risk factor

The result (in Figure 2) shows that the risk factors are higher for bankers (service provider) and lower for customer (service receiver). It indicates that bankers are more satisfied with the risk factor than the customers. The Z statistic of Mann-Whitney U Test for Double Check Identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake Instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are4.497 (p 0.000), 3.930 (p 0.000), 4.246 (p 0.000), 4.452 (p 0.000), 5.425 (p 0.000), 4.162 (p 0.000), 5.290 (p 0.000) and 4.471 (p 0.000) respectively. Therefore, the hypothesis 2 is rejected. So, the e-bank risk factor values of bankers are significantly higher than the customers. It may be mentioned that there is a significant gap between the bankers and the customer satisfaction on e-bank fund transfer. So, it may be concluded that bankers may take necessary protective action to increase the customer service. As a result, customer satisfaction will increase and they should also be used to more electronic banking for COVID-19 situation in future.

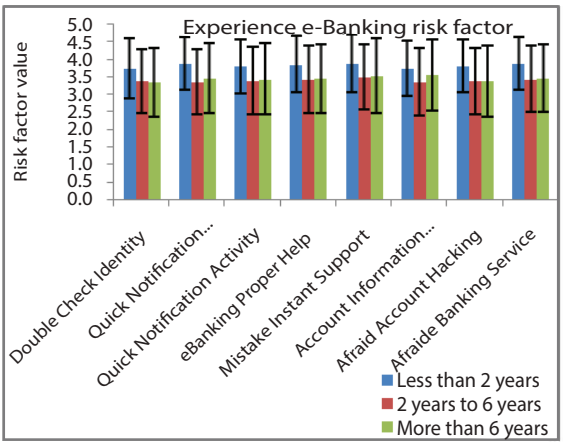

Figure 3
Experience risk factor

The result (in Figure 3) shows that the risk factors of 2 years to 6 years and more than 6 years experiences are similar. But, the risk factors of less than 2 years experiences are much higher for than 2 years to 6 years and more than 6 years experiences. It indicates that less than 2 years experiences are more satisfied than the risk factor of 2 years to 6 years and more than 6 years experiences. The Chi-Square statistic of Kruskal Wallis H Test for Double Check Identity, Quick Notification Authentication, Quick Notification Activity, e-Banking Proper Help, Mistake Instant Support, Account Information Security, Afraid Account Hacking and Afraid Banking Service are6.256 (p 0.044), 11.097 (p 0.004), 7.317 (p 0.026), 9.273 (p 0.010), 5.910 (p 0.050), 6.572 (p 0.037), 8.681 (p 0.013) and 9.238 (p 0.010) respectively. Therefore, the hypothesis 3 is rejected. So, the e-bank risk factor values of less than 2-year experiences are significantly higher than that of the 2 years to 6 years and more than 6 years experiences. It may be mentioned that there is a significant gap between the less than 2 years experiences with the 2 years to 6 years and more than 6 years experiences. The reason may be the e-banking started less than 2 years experiences was most essential and suitable in COVID-19 situation. As a result, the less than 2 years experiences e-banking are highly satisfied. So, the bankers may take necessary protective action to keep hold the customer satisfaction and increase the e-Banking market in the COVID-19 situation in future.

Conclusion

Electronic banking is the most suitable and convenient fund transfer method in COVID-19 pandemic situation. In the current research study, it is observed that the highest banking transaction risk factor is Account Information Security and lowest banking transaction risk factor is Double Check Identity. It is observed that there is no significant difference of e-bank risk factor value for gender. But the e-bank risk factor values of bankers (service provider) are significantly higher than the customers (service receiver), which shows a significant gap between the bankers and the customer satisfaction on e-bank fund transfer. So, bankers may take necessary protective action in increasing the customer service to more electronic banking for COVID-19 situation in future. Finally, the result shows that less than 2 years experiences of e-banking are significantly more satisfied than the risk factor of 2 years to 6 years and more than 6 years e-banking experiences. Now the bankers may take necessary protective action to keep hold the customer satisfaction and increase the e-Banking market in the COVID-19 situation in future.

References

Alam, M. J., Jesmin, J., Faruk, M., & Nur-Al-Ahad, M. (2021). Development of E-banking in Bangladesh: A survey study. *Financial Markets, Institutions and Risks, 5*(2), 42-51. http://doi.org/10.21272/fmir.5(2).42-51.2021

Goudarzi, S., Ahmad, M. N., Soleymani, S. A., & Mohammadhosseini, N. (2013). Impact of trust on internet banking adoption: A literature review. *Australian Journal of Basic and Applied Sciences, 7*(7), 334-347.

Haque, A. K. M. (2019). Need for critical cyber defense, security strategy and privacy policy in Bangladesh–hype or reality? *International journal of Managing Information Technology (IJMIT), 11*(1), 37-50.

Imran, S. A., & Islam, M. T. (2020, December). *COVID-19 mRNA vaccine degradation prediction using regularized LSTM Model.* Paper presented at 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE) (pp. 328-331), IEEE.

Islam, M. M. (2015). Challenges and prospects of internet banking in Bangladesh: banker's (service providers) point of view. *International Journal of Computer Science and Technology, 6*(2), 355-359.

Jadhav, A. A. (2019). Study on impact of covid-19 on customer satisfaction towards e-banking services. *Osmania Journal of International Business Studies (OJIBS), 14*(1-2), 59-65.

Majumder, S. C., & Donghui, Z. (2016). Relationship between remittance and economic growth in Bangladesh: An autoregressive distributed lag model (ARDL). *European Researcher. Series A,* (3), 156-167.

Mohiuddin, M. (2014). Trend and development of E-Banking: A study on Bangladesh. *IOSR Journal of Business and Management, 16*(5), 16-24.

Munir, A. R. (2017). Factors affecting the acceptance of mobile banking services in Makassar Indonesia. *Conference of the International Journal of Arts & Sciences, 1*(01), 113–122.

Neger, M., & Uddin, B. (2020). Factors affecting consumers' internet shopping behavior during the COVID-19 pandemic: Evidence from Bangladesh. *Chinese Business Review, 19*(3), 91-104.

Nilsson, M., Adams, A., & Herd, S. (2005, April). Building security and trust in online banking. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems,* 1701-1704.

Redwanuzzaman, M., & Islam, M. A. (2013). Problematic issues of E-Banking management in Bangladesh. *Asian Business Review, 3*(1), 26-30.

Sadekin, M. S., & Shaikh, M. A. H. (2016). Effect of e-banking on banking sector of Bangladesh. *International Journal of Economics, Finance and Management Sciences, 4*(3), 93-97.

Shahriar, S. (2014, October 1-2). *Acceptance of internet banking in Bangladesh: Evidence from Bangladesh.* Paper presented at International Conference on Business, Law and Corporate Social Responsibility (ICBLCSR'14) (pp. 1-2). Phuket, Thailand.

Skvarciany, V., & Jurevičienė, D. (2018). Factors influencing individual customers trust in internet banking: Case of Baltic states. *Sustainability, 10*(12), 4809.

Corresponding author
Md. Shahnur Azad Chowdhury can be contacted at: tipu_iiuc@yahoo.com