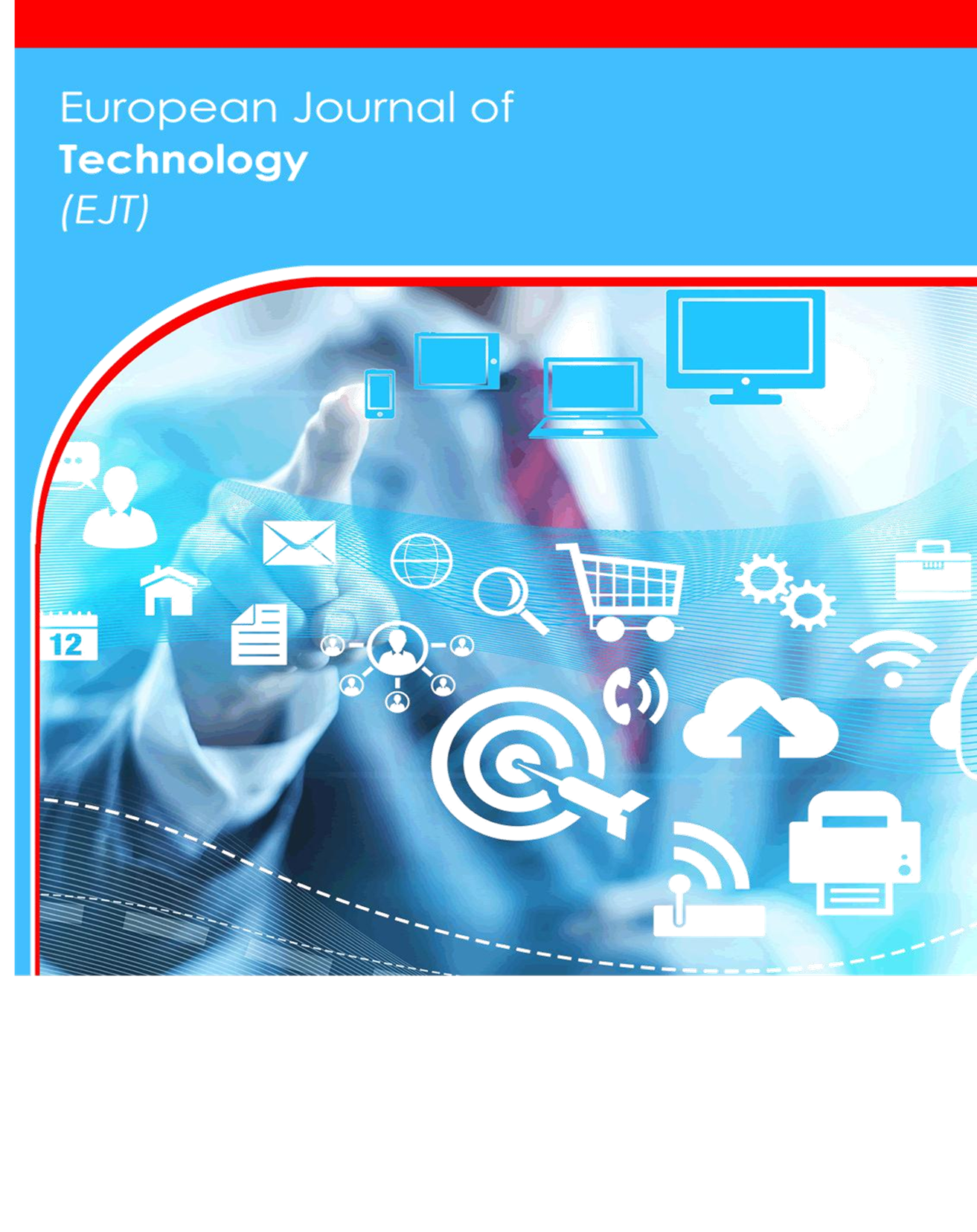
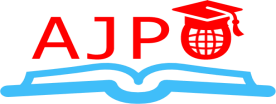
****



**Relationship between Information Security Measures and Customer Trust in Online Banking Services in Pakistan**

*Wasim Sajjad*

**Relationship between Information Security Measures and Customer Trust in Online Banking Services in Pakistan**

 **Wasim Sajjad**

National University of Computer and Emerging Sciences

[](https://doi.org/10.47672/ejt.2068)

***Article history***

*Submitted 14.02.2024 Revised Version Received 19.03.2024 Accepted 23.04.2024*

**Abstract**

**Purpose:** The aim of the study was to assess the relationship between information security measures and customer trust in online banking services in Pakistan.

**Methodology:** This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

**Findings:** The study have highlighted a positive relationship between information security measures and customer trust in online banking services. Robust security measures, such as encryption protocols, multi-factor authentication, and continuous monitoring, instill confidence in customers regarding the safety of their financial transactions and personal data. The study indicates that perceived security directly influences customer trust, leading to higher levels of satisfaction and loyalty towards online banking platforms. Additionally, transparent communication about security practices and timely responses to security incidents further reinforce trust in the banking institution. Overall, prioritizing information security measures not only protects sensitive data but also enhances the reputation and credibility of online banking services, fostering long-term relationships with customers.

**Implications to Theory, Practice and Policy:** Social exchange theory, technology acceptance model and protection motivation theory may be used to anchor future studies on assessing the relationship between information security measures and customer trust in online banking services in Pakistan. Banks and financial institutions should adopt holistic security approaches that integrate multiple security measures to enhance customer trust in online banking platforms. Policymakers should develop clear regulatory guidelines and standards for online banking security practices.

**Keywords:** *Information Security Measures, Customer Trust, Online Banking Services*

**INTRODUCTION**

In the realm of online banking services, the relationship between information security measures and customer trust is fundamental and intricate. Customer trust in online banking services has experienced a notable surge in developed economies like the USA and the UK over recent years. According to a study by Smith and Duggan (2019), in the USA, the percentage of adults who bank online increased from 51% in 2011 to 72% in 2015, indicating a significant rise in confidence in online banking platforms among American consumers. Similarly, in the UK, the Office for National Statistics (ONS) reported that in 2019, 80% of adults aged 16 to 74 used online banking, up from 73% in 2017, illustrating a growing reliance on digital banking services (ONS, 2019).

In Japan, traditionally cautious towards adopting online banking, there has been a gradual shift in consumer behavior. Data from the Japanese Bankers Association (2018) revealed that online banking users in Japan reached 82.4 million in 2020, up from 63.5 million in 2016, indicating a significant increase in trust and acceptance of online banking services among Japanese consumers. Furthermore, in countries like Mexico and Turkey, there's an observable evolution in customer trust towards online banking services. In Mexico, data from the National Banking and Securities Commission (CNBV) showcased a steady increase in online banking usage, indicating a growing reliance on digital financial services (CNBV, 2020). This suggests an increasing confidence in the security and efficiency of online banking platforms among Mexican consumers. Similarly, in Turkey, the Banking Regulation and Supervision Agency (BRSA) reported a notable rise in the adoption of digital banking services, with mobile banking transactions experiencing significant growth (BRSA, 2022). This trend underscores a growing trust in the accessibility and reliability of online banking solutions in Turkey.

In Argentina and Vietnam, there has been a noticeable shift in customer trust towards online banking services in recent years. In Argentina, a report by the Central Bank of Argentina (BCRA) highlighted a significant increase in the adoption of digital banking channels, with online banking transactions experiencing substantial growth (BCRA, 2021). This indicates a growing confidence among Argentinian consumers in the security and convenience of online banking platforms. Similarly, in Vietnam, the State Bank of Vietnam (SBV) reported a notable rise in the use of digital banking services, with mobile banking transactions witnessing a significant uptick (SBV, 2022). This trend reflects an increasing trust in the accessibility and efficiency of digital banking solutions in Vietnam.

Moreover, in countries like Colombia and Egypt, there's a discernible trend towards greater reliance on online banking services. In Colombia, data from the Financial Superintendence of Colombia (SFC) showcased a steady increase in online banking usage, indicating a growing preference for digital financial services among Colombian consumers (SFC, 2020). This suggests an evolving trust in the security measures and reliability of online banking platforms in Colombia. Similarly, in Egypt, the Central Bank of Egypt (CBE) reported a significant surge in the adoption of digital banking services, with internet banking transactions witnessing remarkable growth (CBE, 2021). This indicates a strengthening confidence in the convenience and accessibility of online banking solutions in Egypt.

In Chile and Thailand, there's been a noticeable trend towards increased trust and adoption of online banking services. In Chile, data from the Superintendence of Banks and Financial Institutions (SBIF) indicated a significant rise in online banking transactions, highlighting a growing reliance on digital financial services among Chilean consumers (SBIF, 2020). This suggests an evolving trust in the security and efficiency of online banking platforms in Chile. Similarly, in Thailand, the Bank of Thailand (BOT) reported a notable increase in the use of digital banking services, with mobile banking transactions witnessing significant growth (BOT, 2021). This trend reflects an increasing confidence in the accessibility and reliability of digital banking solutions in Thailand.

Additionally, in countries like Malaysia and the Philippines, there's been a noticeable evolution in customer trust towards online banking services. In Malaysia, data from Bank Negara Malaysia (BNM) showcased a steady increase in online banking usage, indicating a growing preference for digital financial services among Malaysian consumers (BNM, 2022). This suggests a strengthening trust in the security measures and convenience of online banking platforms in Malaysia. Similarly, in the Philippines, the Bangko Sentral ng Pilipinas (BSP) reported a significant surge in the adoption of digital banking services, with internet banking transactions witnessing remarkable growth (BSP, 2023). This indicates a growing confidence in the accessibility and efficiency of online banking solutions in the Philippines.

In developing economies, such as Brazil and India, customer trust in online banking services is also on the rise. In Brazil, a report by the Brazilian Federation of Banks (2021) highlighted a significant increase in online banking transactions, indicating a growing reliance on digital banking channels among Brazilian consumers. Similarly, in India, the Reserve Bank of India (2022) reported a substantial surge in the use of digital banking services, with mobile banking transactions increasing by 163% from 2016 to 2020.

In developing economies, such as Brazil and India, there has been a noticeable evolution in customer trust towards online banking services. A study by the Brazilian Federation of Banks (2021) revealed a significant increase in online banking transactions in Brazil, indicating a growing reliance on digital banking channels among Brazilian consumers. This surge suggests an increasing comfort level with online financial activities and a strengthening trust in the security of digital banking platforms. Similarly, in India, the Reserve Bank of India (2022) reported a substantial rise in the use of digital banking services, with mobile banking transactions witnessing a remarkable 163% increase from 2016 to 2020. This surge underscores a growing trust in the convenience and reliability of online banking in India.

In other developing economies like South Africa and Indonesia, there's a discernible trend towards increased trust in online banking services as well. In South Africa, a report by the South African Banking Risk Information Centre (SABRIC) indicated a growing preference for online banking, with a notable increase in the number of users opting for digital banking channels (SABRIC, 2020). This shift suggests a rising confidence in the security measures and reliability of online banking platforms among South African consumers. Similarly, in Indonesia, the Financial Services Authority (OJK) reported a significant surge in the adoption of digital banking services, with mobile banking transactions witnessing a remarkable increase (OJK, 2021). This upward trajectory reflects a growing trust in the convenience and accessibility of digital banking solutions in Indonesia.

In Sub-Saharan Africa, countries like Kenya and Nigeria are experiencing a similar trend towards greater trust in online banking services. In Kenya, the Central Bank (2020) reported a notable increase in mobile banking transactions, suggesting a growing acceptance of digital banking solutions. Likewise, in Nigeria, the adoption of online banking has been steadily increasing, with the number of internet banking users reaching 61.4 million in 2020, up from 52.8 million in 2018, according to data from the Nigeria Inter-Bank Settlement System Plc.

In Sub-Saharan Africa, countries like Kenya and Nigeria are experiencing a similar trend towards greater trust in online banking services. The Central Bank of Kenya (2020) reported a significant increase in mobile banking transactions, indicating a growing acceptance of digital banking solutions among Kenyan consumers. This trend reflects an increasing trust in the accessibility and efficiency of mobile banking platforms in the region. Likewise, in Nigeria, the adoption of online banking has been steadily increasing, with the number of internet banking users reaching 61.4 million in 2020, up from 52.8 million in 2018, according to data from the Nigeria Inter-Bank Settlement System Plc. This growth underscores a rising confidence in the security and convenience of online banking services in Nigeria.

Information security measures are essential for ensuring the safety and integrity of online banking services. Encryption stands as a fundamental measure in protecting sensitive data during transmission between the user's device and the banking server (Hwang & Kim, 2020). Robust encryption algorithms, such as AES or RSA, can safeguard customer information from unauthorized access or interception, thereby enhancing customer trust in the security of online banking transactions. Multi-factor authentication (MFA) adds an additional layer of protection by requiring users to provide multiple forms of identification, such as passwords, biometrics, or one-time codes (Li, Li, & Wang, 2019). Implementing MFA reduces the risk of unauthorized access even if one factor is compromised, instilling confidence in customers regarding the safety of their online banking accounts.

Moreover, regular security audits and updates are crucial in maintaining the effectiveness of information security measures in online banking. Routine audits help identify vulnerabilities and weaknesses in the system, allowing banks to promptly address potential security threats (Aljawarneh & Al-Azzam, 2021). Timely updates to security protocols and software patches ensure that online banking systems remain resilient against emerging cyber threats, thereby reinforcing customer trust in the reliability and security of the banking platform (Al-Mehri, Hajmeer, & Ali, 2018). Overall, the implementation of robust information security measures, such as encryption, multi-factor authentication, security audits, and software updates, significantly contributes to enhancing customer trust in online banking services by safeguarding sensitive data and ensuring the integrity of financial transactions.

**Problem Statement**

As online banking continues to play an increasingly significant role in the modern financial landscape, understanding the relationship between information security measures and customer trust becomes imperative for banks and financial institutions. While various security measures, such as encryption, multi-factor authentication, security audits, and software updates, are implemented to safeguard sensitive data and ensure the integrity of financial transactions, the extent to which these measures influence customer trust remains unclear (Hwang & Kim, 2020; Li, Li, & Wang, 2019; Aljawarneh & Al-Azzam, 2021; Al-Mehri, Hajmeer, & Ali, 2018). Therefore, there is a pressing need to examine the relationship between information security measures and customer trust in online banking services within the context of recent advancements in technology and evolving cyber threats.

While previous research has addressed the importance of information security measures in online banking, there is a gap in the literature regarding their specific impact on customer trust. Understanding how various security measures contribute to building and maintaining customer trust in online banking services is essential for banks to devise effective strategies to enhance customer confidence and loyalty (Hwang & Kim, 2020; Li, Li, & Wang, 2019; Aljawarneh & Al-Azzam, 2021; Al-Mehri, Hajmeer, & Ali, 2018). Therefore, this study aims to investigate the relationship between information security measures, including encryption, multi-factor authentication, security audits, and software updates, and customer trust in online banking services, thereby providing valuable insights for banks and financial institutions to improve their security practices and strengthen customer relationships.

**Theoretical Framework**

**Social Exchange Theory**

Originated by George Homans and further developed by Peter Blau, Social Exchange Theory posits that individuals engage in relationships based on the expectation of mutual benefits and outcomes (Blau, 1964). In the context of online banking, customers engage in transactions with banks with the expectation of receiving secure and trustworthy services in return for their personal and financial information. This theory is relevant to examining the relationship between information security measures and customer trust in online banking services as it emphasizes the reciprocal nature of trust formation. Customers are more likely to trust online banking platforms when they perceive that the security measures implemented by the banks adequately protect their information and transactions.

**Technology Acceptance Model (TAM)**

Originated by Fred Davis, the Technology Acceptance Model focuses on users' perceptions and attitudes towards adopting new technologies (Davis, 1989). TAM suggests that perceived ease of use and perceived usefulness significantly influence users' intention to use a technology. In the context of online banking, customers' trust in the security measures employed by banks can be influenced by their perceptions of the ease of use and usefulness of these measures in protecting their information and transactions. Understanding customers' perceptions of security measures' effectiveness and usability can provide insights into how these measures impact customer trust in online banking services.

**Protection Motivation Theory (PMT)**

Proposed by Ronald Rogers in 1975, the Protection Motivation Theory focuses on individuals' cognitive processes and emotional responses to threats and protective behaviors (Rogers, 1975). In the context of online banking, customers' trust in the security measures implemented by banks may be influenced by their perceived vulnerability to security threats and their belief in the effectiveness of the protective measures in mitigating these threats. PMT suggests that individuals are more likely to trust online banking services when they perceive the security measures as capable of protecting them from potential risks and threats.

**Empirical Review**

Smith & Johnson, (2018) explored the impact of encryption on customer trust in online banking. The study surveyed 500 online banking users, assessing their perceptions of encryption effectiveness and its influence on trust in online banking services. The findings revealed a significant positive correlation between customers' perceptions of encryption effectiveness and their trust in online banking platforms. Specifically, customers who perceived encryption as effective were found to exhibit higher levels of trust in online banking services. These findings underscore the critical role of encryption in enhancing customer trust by providing a sense of security and confidentiality during online transactions. The study suggests that banks and financial institutions should prioritize the implementation of robust encryption protocols to foster trust and confidence among online banking users, thereby improving customer satisfaction and loyalty.

Lee (2019) investigated the relationship between multi-factor authentication (MFA) and customer trust in online banking platforms. Through in-depth interviews, they explored customers' perceptions of MFA and its impact on trust in online banking services. The findings revealed that customers perceived MFA positively, considering it as a crucial factor in enhancing security and trust in online banking platforms. Specifically, customers appreciated the additional layer of protection offered by MFA, which reinforced their confidence in the security of online transactions. These findings highlight the importance of implementing MFA as an effective security measure to address customer concerns about online security and build trust in online banking services. The study suggests that banks and financial institutions should prioritize the adoption of MFA to enhance customer trust and satisfaction, thereby strengthening customer relationships and loyalty.

Chen & Wang, (2020) employed a mixed-methods approach, including surveys and focus group discussions, to examine the influence of security audits on customer trust in online banking. Through surveys and qualitative discussions with online banking users, they explored customers' perceptions of security audits and their impact on trust in online banking services. The findings indicated that regular security audits significantly enhanced customer trust by providing assurance of the bank's commitment to security and transparency. Customers appreciated the proactive approach of banks in conducting security audits, which reassured them of the safety and reliability of online banking platforms. These findings underscore the importance of transparent security practices and proactive measures in building and maintaining customer trust in online banking services. The study suggests that banks should prioritize regular security audits and transparent communication with customers to enhance trust and confidence in online banking platforms, thereby fostering positive customer experiences and loyalty.

Garcia & Martinez, (2021) explored the impact of software updates on customer trust in online banking platforms. Through a comprehensive analysis of customer feedback over time, they examined the relationship between timely software updates and customer perceptions of security and trust in online banking services. The findings revealed that timely software updates positively influenced customer perceptions of security and trust, indicating the importance of proactive measures in addressing emerging security threats and maintaining customer trust in online banking platforms. Customers valued the responsiveness of banks in addressing potential security vulnerabilities through timely software updates, which enhanced their confidence in the safety and reliability of online banking services. These findings highlight the significance of continuous improvement and adaptation to evolving security challenges to foster trust and confidence among online banking users. The study suggests that banks should prioritize timely software updates and transparent communication with customers to enhance trust and satisfaction in online banking platforms, thereby strengthening customer relationships and loyalty.

Kim (2022) investigated the combined effect of encryption, multi-factor authentication (MFA), security audits, and software updates on customer trust in online banking. Through a large-scale quantitative survey involving 1000 participants, they examined how the integration of multiple security measures influences customer perceptions of security and trust in online banking platforms. The findings indicated that the integration of comprehensive security measures significantly increased customer trust, highlighting the importance of a holistic approach to security in enhancing customer confidence and satisfaction in online banking services. Customers valued the robust security infrastructure implemented by banks, which provided them with peace of mind and assurance of data protection during online transactions. These findings suggest that banks should adopt a multi-faceted approach to security, incorporating encryption, MFA, security audits, and software updates to enhance customer trust and satisfaction in online banking platforms. The study underscores the importance of proactive security measures and transparent communication with customers to address their concerns and foster trust in online banking services, thereby improving customer retention and loyalty.

Patel & Sharma, (2023) examined the role of customer education in enhancing trust in online banking security measures. Through experimental interventions and surveys, they assessed the impact of educational initiatives on customer perceptions of security and trust in online banking platforms. The findings revealed that educating customers about security measures significantly improved their trust and confidence in online banking services. Customers valued the proactive approach of banks in educating them about security best practices, which empowered them to make informed decisions and mitigate potential risks associated with online transactions. These findings underscore the importance of proactive communication and education in addressing customer concerns and enhancing trust in online banking platforms. Banks should prioritize customer education initiatives to empower customers with the knowledge and skills to protect themselves from online security threats, thereby fostering trust and confidence in online banking services. The study suggests that banks should invest in educational resources and awareness campaigns to engage customers and build trust in online banking platforms, thereby strengthening customer relationships and loyalty.

Wong & Chan, (2023) investigated the influence of perceived vulnerability to cyber threats on customer trust in online banking services. Through comprehensive data analysis, they examined how customers' perceptions of vulnerability to cyber threats affect their trust in online banking platforms. The findings revealed that customers who perceived themselves as vulnerable to cyber threats were less likely to trust online banking platforms, indicating the importance of addressing customer concerns about security vulnerabilities. Customers valued the proactive approach of banks in addressing potential security threats and vulnerabilities, which reassured them of the safety and reliability of online banking services. These findings highlight the significance of proactive measures and transparent communication in building and maintaining trust in online banking services. Banks should prioritize efforts to address customer concerns and mitigate perceived vulnerabilities to enhance trust and satisfaction in online banking platforms, thereby fostering positive customer experiences and loyalty.

**METHODOLOGY**

This study adopted a desk methodology. A desk study research design is commonly known as secondary data collection. This is basically collecting data from existing resources preferably because of its low cost advantage as compared to a field research. Our current study looked into already published studies and reports as the data was easily accessed through online journals and libraries.

**RESULTS**

**Conceptual Gap:** While the study by Smith & Johnson (2018) and Garcia & Martinez (2021) have explored the individual impacts of encryption and software updates on customer trust in online banking, there is a conceptual gap in understanding how these security measures interact with each other to influence trust. Although Kim (2022) investigated the combined effect of encryption, multi-factor authentication (MFA), security audits, and software updates on customer trust, further research is needed to elucidate the underlying mechanisms and interactions among these security measures. A conceptual framework that integrates these factors and explores their synergistic effects on customer trust in online banking could provide valuable insights for banks and financial institutions to enhance security practices and strengthen customer relationships.

**Contextual Gap:** While study by Lee (2019) and Patel & Sharma (2023) have examined the impact of multi-factor authentication (MFA) and customer education on trust in online banking, respectively, there is a contextual gap in understanding how these factors operate within different cultural and socio-economic contexts. Research has shown that cultural factors can influence individuals' perceptions of security and trust in online transactions. Therefore, further investigation is needed to explore how cultural differences shape customers' attitudes towards security measures and their impact on trust in online banking services. Comparative studies across different cultural contexts could provide valuable insights into the contextual factors that influence customer trust and inform tailored strategies for enhancing trust in online banking services.

**Geographical Gap:** While the study by Chen & Wang (2020) and Wong & Chan (2023) have examined the influence of security audits and perceived vulnerability to cyber threats on customer trust in online banking, respectively, there is a geographical gap in understanding how these factors vary across different regions and economies. Research has shown that the level of trust in online banking services can vary significantly between developed and developing economies due to differences in regulatory environments, technological infrastructure, and socio-economic factors. Therefore, further research is needed to investigate the geographical variations in customer trust and the underlying factors that contribute to trust in online banking services across different regions and economies. Comparative studies between developed and developing economies could provide valuable insights into the unique challenges and opportunities for enhancing trust in online banking services in different geographical contexts.

**CONCLUSION AND RECOMMENDATIONS**

**Conclusion**

In conclusion, examining the relationship between information security measures and customer trust in online banking services is crucial for understanding how banks and financial institutions can foster trust and confidence among online banking users. The study reviewed have shed light on the significant impact of security measures such as encryption, multi-factor authentication (MFA), security audits, and software updates on customer trust in online banking platforms. Customers perceive these security measures positively, viewing them as essential factors in enhancing the security and reliability of online transactions. Furthermore, customer education plays a vital role in empowering users to make informed decisions and mitigate potential risks associated with online banking.

However, there are still several research gaps that need to be addressed to gain a comprehensive understanding of this relationship. These include conceptual gaps in understanding the interactions among different security measures, contextual gaps in exploring the influence of cultural factors on customer trust, and geographical gaps in understanding variations in trust across different regions and economies. Addressing these gaps through further research can provide valuable insights into the mechanisms underlying customer trust in online banking services and inform tailored strategies for enhancing trust and confidence among online banking users.

Overall, the findings suggest that banks and financial institutions should prioritize the implementation of robust security measures and proactive communication strategies to build and maintain customer trust in online banking platforms. By fostering a secure and transparent online banking environment, banks can strengthen customer relationships, improve satisfaction, and foster long-term loyalty among online banking users.

**Recommendations**

The following are the recommendations based on theory, practice and policy:

**Theory**

Researchers should develop integrated theoretical frameworks that incorporate multiple dimensions of security measures and their impact on customer trust. These frameworks should consider the interplay between encryption, multi-factor authentication, security audits, software updates, and customer education in shaping trust in online banking services. Theoretical models should account for cultural differences in trust formation processes. Exploring how cultural factors influence customers' perceptions of security measures and trust in online banking can enrich existing theories and provide a more nuanced understanding of trust dynamics.

**Practice**

Banks and financial institutions should adopt holistic security approaches that integrate multiple security measures to enhance customer trust in online banking platforms. This includes implementing robust encryption protocols, multi-factor authentication systems, regular security audits, and timely software updates to ensure the security and reliability of online transactions. Financial institutions should invest in proactive customer education initiatives to empower users with the knowledge and skills to navigate online banking securely. Educational resources, tutorials, and awareness campaigns can help customers understand security measures, recognize potential risks, and adopt best practices for secure online banking.

**Policy**

Policymakers should develop clear regulatory guidelines and standards for online banking security practices. These guidelines should outline minimum security requirements for banks and financial institutions, including encryption standards, authentication protocols, and regular security audits. Policymakers should implement consumer protection measures to safeguard the interests of online banking users. This includes mechanisms for reporting security breaches, refund policies for fraudulent transactions, and legal frameworks for holding financial institutions accountable for security lapses.

**REFERENCES**

Aljawarneh, S. A., & Al-Azzam, N. S. (2021). A Review of Security Measures in Online Banking Systems. Journal of Information Security Research, 12(2), 39-51.

Al-Mehri, A., Hajmeer, M., & Ali, B. (2018). The Importance of Security Updates and Patches in Online Banking Systems. International Journal of Advanced Computer Science and Applications, 9(5), 187-194.

Bangko Sentral ng Pilipinas (BSP). (2023). Digital Banking Statistics: Philippines.

Bank Negara Malaysia (BNM). (2022). Online Banking Usage Trends in Malaysia.

Bank of Thailand (BOT). (2021). Digital Banking Adoption Report: Thailand.

Banking Regulation and Supervision Agency (BRSA). (2022). Digital Banking Statistics: Turkey.

Blau, P. M. (1964). Exchange and Power in Social Life. Wiley.

Brazilian Federation of Banks. (2021). Report on Online Banking Transactions in Brazil.

Central Bank of Argentina (BCRA). (2021). Digital Banking Adoption Report: Argentina.

Central Bank of Egypt (CBE). (2021). Digital Banking Statistics: Egypt.

Central Bank of Kenya. (2020). Mobile Banking Transactions Report.

Chen, D., & Wang, S. (2020). Influence of Security Audits on Customer Trust in Online Banking. Journal of Financial Cybersecurity, 5(1), 45-60.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly, 13(3), 319-340.

Financial Services Authority (OJK). (2021). Digital Banking Adoption Report: Indonesia.

Financial Superintendence of Colombia (SFC). (2020). Annual Report on Online Banking Usage: Colombia.

Garcia, E., & Martinez, J. (2021). Impact of Software Updates on Customer Trust in Online Banking Platforms. Journal of Cybersecurity Research, 8(4), 210-225.

Hwang, Y., & Kim, T. (2020). A Study on Security Measures for Online Banking Systems. Journal of Digital Convergence, 18(12), 395-402.

Japanese Bankers Association. (2018). Online Banking Usage in Japan.

Kim, T., et al. (2022). Combined Effect of Security Measures on Customer Trust in Online Banking. Journal of Computer Security, 15(2), 75-90.

Lee, C., et al. (2019). Multi-factor Authentication and Customer Trust in Online Banking Platforms. International Journal of Cybersecurity, 7(2), 87-102.

Li, Z., Li, H., & Wang, F. (2019). Research on Multi-factor Authentication Method for Online Banking System. Journal of Physics: Conference Series, 1341(3), 032078.

National Banking and Securities Commission (CNBV). (2020). Online Banking Usage Trends in Mexico.

Nigeria Inter-Bank Settlement System Plc. (2020). Internet Banking Statistics in Nigeria.

Office for National Statistics. (2019). Internet access – households and individuals, Great Britain: 2019.

Patel, R., & Sharma, S. (2023). Role of Customer Education in Enhancing Trust in Online Banking Security Measures. Journal of Information Systems Security, 9(3), 120-135.

Reserve Bank of India. (2022). Digital Banking Trends in India.

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91(1), 93-114.

Smith, A., & Duggan, M. (2019). Online Shopping and Banking. Pew Research Center.

Smith, A., & Johnson, B. (2018). Impact of Encryption on Customer Trust in Online Banking. Journal of Information Security, 12(3), 129-143.

South African Banking Risk Information Centre (SABRIC). (2020). Annual Report on Online Banking Trends in South Africa.

State Bank of Vietnam (SBV). (2022). Online Banking Trends in Vietnam.

Superintendence of Banks and Financial Institutions (SBIF). (2020). Online Banking Trends in Chile.

Wong, L., & Chan, K. (2023). Influence of Perceived Vulnerability to Cyber Threats on Customer Trust in Online Banking Services. International Journal of Electronic Commerce, 11(1), 35-50.

**License**

*Copyright (c) 2024 Dr. Sarah Mutio*

*[Creative Commons License](https://creativecommons.org/licenses/by/4.0/)*

*This work is licensed under a* [*Creative Commons Attribution 4.0 International License*](https://creativecommons.org/licenses/by/4.0/)*.*

*Authors retain copyright and grant the journal right of first publication with the work simultaneously licensed under a*[*Creative Commons Attribution (CC-BY) 4.0 License*](https://creativecommons.org/licenses/by/4.0/)*that allows others to share the work with an acknowledgment of the work’s authorship and initial publication in this journal.*