

Original Article

Customer Trust and Security Perception in Digital Banking

Dr. Elena Petrova¹, Dr. Carlos Mendes²

¹Associate Professor, Moscow State University, Russia.

²Professor, University of Lisbon, Portugal.

Received: 01-03-2019

Revised: 01-21-2019

Accepted: 01-27-2019

Published: 02-02-2019

ABSTRACT

Digital banking has improved financial services by enabling secure and convenient transactions through internet and mobile platforms. While it offers greater accessibility and efficiency, customer adoption depends heavily on trust and perceived security. Concerns regarding fraud, data breaches, identity theft, and privacy risks continue to influence users' confidence in digital banking systems. This study investigates the impact of trust, security perception, privacy protection, and service quality on digital banking adoption. Using quantitative analysis, it identifies key factors such as authentication effectiveness, encryption awareness, transaction reliability, and institutional reputation that influence customer trust. The findings show that strong security measures, including two-factor authentication, encryption, and fraud detection systems, significantly enhance customer confidence and willingness to use digital banking services. The study concludes that trust is a critical factor driving customer satisfaction, loyalty, and long-term adoption, while emerging technologies such as biometric authentication, cybersecurity solutions, and AI-based fraud detection will further strengthen digital banking security in the future.

KEYWORDS

Digital Banking, Customer Trust, Security Perception, Information Security, Privacy Protection, Electronic Banking, Cybersecurity, Financial Technology.

1. INTRODUCTION

1.1. Digital Banking and Customer Trust

Digital banking has transformed the banking industry by allowing customers to access their financial needs anytime and anywhere using their mobile apps, internet banking platforms, automated teller machines (ATMs) and electronic payment systems. These technological developments have led to greater efficiency, lower transaction costs and better customer convenience. But as a result of digital banking and no physical contact, there are concerns for transactions, data privacy and system reliability. As a result, the trust of customers has become a pivotal factor in the adoption and retention of digital banking products and services. Customer trust is the level of confidence that a customer has in a financial institution to protect the personal and financial details of its customers and deliver the services with reliability and security. Trust decreases the risks and uncertainties that consumers think exist in online transactions. It is built on solid security, clear communication, compliance and service standards. Customer trust is a strong indicator that they'll use digital banking technologies, confidently use online banking, and stay with the provider over the long haul.

1.2. Security Perception in Digital Financial Services

Security perception is the extent to which customers feel that digital financial services offer them sufficient security in safeguarding their personal information, financial information and online transactions. For digital banking environments, customers are likely to assess the security of a platform before deciding to use its services. A positive security perception alleviates fears of cyber security, fraud, and data breaches, leading to greater trust and uptake of digital financial technologies. There are multiple factors that influence customer perceptions of security in digital financial services.

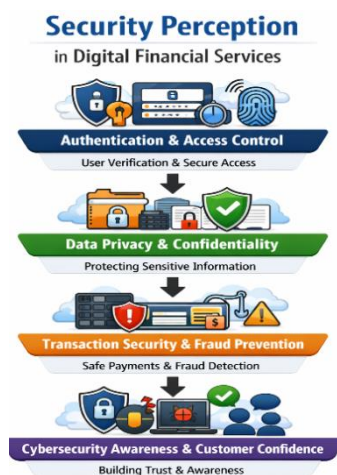


Fig 1 - Security Perception in Digital Financial Services

1.2.1. Authentication and Access Control

Authentication and access control are key features in digital financial security. These are the steps that can be taken to ensure that only the rightful owner of the account has access to the banking

account and can carry out financial transactions. Some of the most popular authentication methods involve password, one-time password (OTP), multi-factor authentication, and biometric (fingerprint or facial recognition). Effective authentication measures provide added security and boost customer trust by minimizing the likelihood of unauthorized entry and identity theft.

1.2.2. Data Privacy and Confidentiality

Data privacy and data confidentiality are important factors affecting perception of security. Consumers believe that financial institutions should secure their personal and financial data from disclosure, misuse and cyberattacks. Customers are assured that their sensitive data is being handled responsibly with effective privacy policies, secure data storage practices and compliance with data protection regulations. Robust privacy safeguards help build trust and customer satisfaction.

1.2.3. Transaction Security and Fraud Prevention

Transaction security is the security of financial transactions from fraud, manipulation and unauthorized transactions. To protect customer transactions, financial institutions employ various technologies, such as encryption, secure payment gateways, fraud detection systems, and real-time monitoring tools. Customers will be more likely to trust and use digital financial services regularly if they feel they are actively being protected from fraudulent use, and have access to safe transaction environments in their banks.

1.2.4. Cybersecurity Awareness and Customer Confidence

Cybersecurity awareness is a major factor that influences the security of customers' digital financial services. Educating customers on online risks, safe banking practices, and security features can alleviate concerns about online transactions. Consistent security alerts, awareness-raising initiatives, and clear communication about security protocols boost customer trust. By raising awareness, users can access financial services through digital channels more safely, building trust in financial institutions over the long run.

1.3. Customer Trust and Security Perception in Digital Banking

It's undeniable that customer trust and security perception are tightly related elements that affect the uptake and ongoing utilization of digital banking services. Banks are transitioning more and more from a branch-only business model to an online and mobile presence, and customers are now expected to engage in financial transactions in virtual environments, without direct, face-to-face interaction with the bank. In such environments, trust is a key factor that can influence the ability of the customer to feel comfortable using digital banking services. Trust may be described as the faith customers have in the financial institution's services to be reliable, safe, and efficient, and to safeguard their personal and financial data. Security perception, on the other hand, is a measure of how well customers feel digital banking platforms are able to protect transactions and sensitive information from cyber threats, fraud, and unauthorized access. Customer trust is greatly shaped by a positive security perception. Customers who see such robust security features like encryption technologies, multi-factor authentication, biometric verification, secure payment gateways, and fraud detection systems will feel protected as they conduct online transactions. These security measures

help to lower the risk and boost the trust of the banking platform. On the other hand, news of data breaches, identity theft, phishing and financial fraud can have a detrimental impact on trust and deter customers from utilizing digital banking services. So, it is crucial to have a secure digital environment in order to establish and retain customers' trust. Moreover, institutional reputation, transparency, service reliability, and regulatory conformance are also factors that affect customer trust. When financial institutions make their security policies transparent, address customer concerns appropriately and are consistently reliable, they are more likely to win their customers confidence. When it comes to new technologies in the digital banking landscape, trust is the element that is driving customers to use them, to make more transactions and to build relationships with their banks in the long term. With digital banking on the constant evolution, improving the perception of security is a key priority for financial institutions. Banks can build customer confidence, enhance user satisfaction, and create the path for digital financial services' sustainable growth by investing in modern cybersecurity technologies, educating customers, and adopting clear communication strategies.

2. LITERATURE SURVEY

2.1. Trust Formation in Digital Banking

Trust is a key determinant in the adoption and continued use of digital banking services. Customer willingness to make financial transactions online has been previously demonstrated to be higher when they find a banking platform to be reliable, secure and transparent. Trust helps to diminish uncertainty in the Electronic transaction and makes customers feel better about disclosing sensitive financial information. The trust-building process in digital banking can be enhanced by key factors like reputation, service quality, system reliability, and user-friendly interfaces.

2.1.1. Service Reliability and Customer Trust

Researchers have established that regular service delivery has a significant impact in building customer confidence. Digital banking systems that offer seamless access, ensure the correct execution of transactions, and ensure timely customer support allow the customers to build trust and confidence in the institution. Trust and a positive customer experience are further strengthened by effective complaint resolution mechanisms and positive customer experiences over the long-term.

2.2. Information Security and Customer Confidence

The security of information is an essential part of the trust of customers in digital banking systems. The security of a web based banking platform is a key factor in customer adoption, as highlighted in numerous studies. The implementation of security measures like data encryption, multi-factor authentication, secure communication protocols, and intrusion prevention systems curtails the perceived risks of online transactions. A safe atmosphere in the bank ensures customers that their money and personal details are safeguarded appropriately.

2.2.1. Security Features and User Perception

Visible security measures have been shown to positively impact user perceptions and create greater trust in digital banking. One critical consumer worry is cyber threats, identity theft and unauthorized access to accounts. This means that banks that proactively inform their customers about their security protocols and keep them updated on security measures will be more likely to instill trust and improve user satisfaction.

2.2.2. Privacy Protection and Risk Perception

Protecting privacy is one of the main concerns of banking customers when it comes to their digital banking experience. Banks are responsible for protecting the personal, financial and transactional data of its customers from unauthorized access and misuse. Existing studies indicate that privacy concerns may be detrimental to customers' adoption intentions when customers feel there is a high risk of exposure of their data. By encouraging the adoption of effective privacy management practices, these concerns can be minimised and a trustworthy digital banking environment can be established.

2.2.3. Transparency and Privacy Assurance

Research shows that open data collection policies and communication has a positive impact on trust among consumers. Banks and financial institutions with clear statements about how they collect, store and use data can minimize customer apprehension. By ensuring privacy is protected, these mechanisms also help build customer trust, loyalty, and engagement to digital banking solutions, leading to a more positive customer experience.

2.4. Emerging Security Technologies

The current landscape of the digital banking sector has seen a rise in the significance of advanced security technologies in enhancing banking systems. In recent years, sophisticated security technologies have come to play a more critical role in bolstering digital banking platforms. Advanced technologies like biometric authentication, artificial intelligence (AI), machine learning (ML), behavioral analytics and blockchain-based security solutions are gaining traction in financial institutions. They help to better identify and prevent fraudulent operations and increase the overall security of electronic transactions.

2.4.1. Advanced Authentication and Fraud Detection

Biometric authentication systems like fingerprint recognition, facial recognition and iris scanning have been reported to offer more robust security than traditional password-based authentication systems. Likewise, AI and ML-driven fraud detection tools can process transactional information in real-time, and flag suspicious activities in real time with high accuracy. Such innovations not only minimize security vulnerabilities but also boost customer trust and help build a secure and reliable digital banking environment.

3. METHODOLOGY

3.1. Conceptual Research Framework

The conceptual research framework was developed to analyze the relationship between security related factors and customers' behavior in digital banking. It suggests that the security features provided by banks lead to customers' perception of security, which in turn lead to trust, intension to use and long-term loyalty.



Fig 2 - Conceptual Research Framework

3.1.1. Security Features

Security features are the technical and procedural measures that digital banking institutions take to ensure the security of customer data and financial transactions. These include data encryption, multi factor authentication, and biometric verification, secure payment gateways, fraud monitoring and intrusion detection. Securing products decreases vulnerabilities and enables customers to feel secure that their personal and financial data is secure from cyber threats and unauthorized access.

3.1.2. Perceived Security

Perceived security is how customers think that a digital banking platform is safe and reliable. It signifies how confident customers are that their transactions and personal data are secure from fraud, hacking, and data breaches. A banking system that customers see as secure helps to reduce uncertainty and risk, and enhances comfort with digital banking services. In this regard, the perception of security is important in the customer attitudes towards online banking.

3.1.3. Customer Trust

Customer trust is the confidence that the digital banking institution places on users to carry out transactions correctly, securely and reliably. Customers can trust a service when they always know they have access to secure services, the communication is clear, and the services perform as they expect. Trust fosters confidence in financial safety and privacy, which empowers consumers to utilize digital banking solutions for economic transactions. Trust promotes confidence in monetary security and personal privacy, promoting customers to depend on digital banking choices for their economic needs. This is the gap between what is perceived to be safe and what is actually engaging the customer.

3.1.4. Usage Intention

Usage intention is a customer's intention to use digital banking services in the future and how likely they are to do so. It captures positive behavioral intentions based on positive perceptions of security and trust. When customers are confident about a banking platform's security and trust in its ability to provide them with sufficient security, they are more likely to engage in online transactions, use mobile banking apps, and make use of other digital financial services. Hence, it is concluded that intention to use is a significant indicator of the actual adoption and continued use of technologies used in digital banking.

3.1.5. Customer Loyalty

Customer loyalty is the fidelity a customer has toward one digital banking service provider as compared to another. Favored customers remain loyal to the bank, refer it to their friends and family and are not likely to switch to another bank. Building loyalty involves good experiences, regular performance of security and trust that is maintained over time. For digital banking, customers who regularly access secure and reliable services are more likely to remain loyal to their bank and have a long-term banking relationship, which helps to boost customer retention and organization growth.

3.2. Data Collection and Variables

The data collection is an essential part of this research, as it is necessary to gather the data needed to research how customers perceive their trust and security in digital banking. The study collects primary data from digital banking users by using a structured questionnaire to gauge different security-related and trust-related factors. The survey comprises statements on important variables that impact customers' perceptions and use of digital banking services. The respondents will be asked to respond using a five-point Likert scale (1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree) to each statement. This method of measurement allows customer attitudes, perceptions and experiences of digital banking security and trust to be quantified. A few important variables are taken into consideration in this study. Authentication Security is the strength of user authentication systems like passwords, one-time passwords (OTP), biometric authentication and multi-factor authentication. Implementing robust authentication methods can make unauthorized access more difficult and boost customer trust. Privacy Protection refers to how assured customers are of the confidentiality and protection of personal and financial data, and its use for the wrong purpose. Good privacy protection mitigates fear of data leaks and identity theft. Transaction Reliability is the effectiveness, consistency and reliability of the transactions which transaction in digital banking is defined as successful fund transfer, successful payment processing, and successful account management activities. With reliable transactions, customer satisfaction and trust go hand-in-hand. Another vital variable is Institutional Reputation, which defines the level of trust, credibility and image the banking institution has. A good reputation can go hand in hand with improved security and service. Customer Trust is the trust that customers put in digital banking services to be carried out securely, accurately, and consistently. Lastly, Security Perception is the overall perception of security customers have when engaging with digital banking platforms. These factors together help to understand the factors that affect customer trust, customer security

perception, and intention to use digital banking services, and long-term customer loyalty. All the data collected are analyzed statistically and used for hypothesis testing in the study.

3.3. Trust Evaluation Model

The Trust Evaluation Model is designed to address the factors that drive customer trust in digital banking services. Trust is regarded as a multi-dimensional construct which is affected by multiple security features and organizational factors. In this research, the customers' trust is conceptualized as a function of four factors which are perceived security, protection of privacy, reliability of transactions, and institutional reputation. Each of these factors is assumed to be a part of the overall level of trust that customers have in the digital banking platform. The study aims to uncover the most pivotal factors driving customer trust and understand their impact on the adoption and ongoing use of digital banking services by examining these relationships. Customer Trust (CT) is the dependent variable in the model, reflecting the customers' confidence in the safety, reliability, and effectiveness of digital banking services. Perceived Security (PS) is the view that customers have of the security of their financial data and transactions from the threat of cyber attacks, fraud and unauthorised access. The greater the perception of security, the higher the trust in the banking platform. Privacy Protection (PP) is the degree of privacy that customers feel their personal and financial data is protected and is treated responsibly by the bank. Perceived risks and trust are lowered with strong privacy protection measures. Transaction Reliability (TR) is the consistency, accuracy and dependability of banking transactions. Digital banking systems that execute transactions correctly and deliver continuous service are more likely to win the trust of their customers. Institutional Reputation (IR) is the reputation, image and trustworthiness of the financial institution providing digital banking services. When the bank has a good reputation, customers feel more confident in the bank. The model gives weight coefficients (α), β), γ), δ)) to these variables. These coefficients show the relative influence of perceived security, perceived levels of privacy protection, perceived transaction reliability and perceived institutional reputation on customer trust. The larger the coefficient is, the more it will affect the formation of trust. These relationships are assessed to offer a systematic way of thinking about how each of these components of security and organizational performance contribute to customer trust in a digital banking setting. This model can help financial institutions identify which strategies will boost customer trust and drive digital banking uptake.

3.4. Methodological Flowchart

The methodological flowchart shows the sequence of the steps taken during the research process to assess customer trust and security perception on digital banking. Each stage helps to systematically gather, analyse and interpret data, which will yield reliable and meaningful results from the study.



Fig 3 - Methodological Flowchart

3.5. Customer Survey

The research process starts with a customer survey to collect feedback on the experience and opinion of digital banking services. The structured questionnaire is circulated to digital banking users to gather the perception about security, privacy, trust and service quality. The survey is the main source of information and helps the researchers to get an understanding of customer attitudes on different aspects of digital banking. A five-point Likert scale is used in the formulation of the questions to determine the degree of agreement the respondents have for each of the statements.

3.6. Data Collection

Once the survey has been carried out, the survey data is gathered and sorted for analysis. This step is to validate the completeness and accuracy of the data collected, so that the accuracy of the collected data is reliable. Data about the demographic characteristics and answers with regard to security attributes, trust factors and utilization conduct is accumulated in a structured data source. Proper data collection procedures help minimize errors and provide a solid foundation for subsequent analytical processes.

3.7. Security Perception Analysis

The gathered data is then analysed to evaluate customers' perceptions on security of digital banking. This stage is about assessing user experience of authentication methods, privacy safeguards, encryption solutions, and security for transactions. The analysis reveals which factors have the greatest impact on customers' perception of security when using their digital banking services. It is important to understand security perceptions as they have a direct impact on customer confidence and their willingness to conduct online financial transactions.

3.8. Trust Evaluation

After the security perception analysis, security trust levels are calculated based on the proposed trust evaluation model. This stage looks at how perceived security, privacy protection, transaction reliability and reputation build customer trust. These variables are used in statistical methods to assess the magnitude of the relationships that exist between them. The trust evaluation process aims to identify the determinants that play a crucial role in developing customer trust in digital banking systems.

3.9. Statistical Assessment

Statistic assessment is done to verify the results of the research and to test the relationships of variables proposed. Descriptive statistics, correlation analysis, regression analysis and reliability testing can be used. These approaches can be used to measure the effect of various factors on customers' trust and security perception. Data analysis helps to confirm the results of the study are statistically valid and supported by empirical evidence.

3.10. Results Interpretation

The last step is to interpret the results from the statistical analysis. The results are discussed in light of the research aims and literature. Significant trends, relationships and patterns are found that help explain customer trust and perceptions of security in digital banking. The analysis of results offers valuable insights that can guide banking institutions in refining their security protocols, boosting customer trust, and optimizing customer satisfaction and loyalty in digital banking settings.

4. RESULT AND DISCUSSION

4.1. Security Perception Analysis

The security perception analysis indicates that security is among the most important considerations that customers consider when deciding on their trust and confidence in digital banking services. As more and more financial transactions shift to the online and mobile venues, consumers are becoming more cognizant of the possibility of a hack, identity theft, phishing attack or unauthorized use of their accounts. This means the level of security that they think banks are providing on their digital platforms has a significant impact on their willingness to engage with them. The results suggest that customers are very concerned about security measures which safeguard their personal and financial data whilst transacting online. A positive perception of security translates to low levels of uncertainty and risk, creating a positive attitude towards the adoption and continued use of digital banking services. The respondents give the highest importance ratings to authentication systems and privacy protection measures among the different security related factors. Secure authentication features like multi-factor, one-time passwords, biometric verification, and secure logon are especially important to customers because they help keep customers safe from unauthorized logon. In the same way, the importance of privacy protection is key to security perceptions; customers trust that their banks will protect their sensitive personal and transactional information from misuse, disclosure or cyberattacks. The study results indicate that if customers are made aware of the security policy of banking institutions and the commitment these

institutions have towards securing customer data they are more likely to trust the banking institution. The study also reveals that strong and visible security measures are a critical factor in boosting trust in digital banking platforms. Encryption technologies, fraud monitoring systems, security alerts, secure payment gateways and real-time transaction notifications give reassurance to customers that their financial activity is being actively protected. Customers know that banks will continually invest in cutting-edge security hardware and continually upgrade and update security systems, so they feel that the risk of transacting in the bank is less. This perception positively impacts on trust and has a positive effect on the usage of digital banking services. Overall, the findings indicate that security perception is a key factor in driving customer trust, making it crucial for financial institutions to invest in robust cybersecurity measures and adopt clear security protocols to foster customer confidence and encourage continued use of their digital banking platforms.

4.2. Customer Perception Results

The customer perception analysis identifies relative weightage to different security factors in building trust and confidence on digital banking services. The findings suggest that security features such as robust authentication systems, secure transaction processing, and privacy safeguards are top priorities for customers. The percentage values are the percentage of those who had positive perceptions of each security factor.

Table 1: Customer Perception Results

Security Factor	Positive Response (%)
Two-Factor Authentication	92
Transaction Reliability	89
Data Privacy Protection	87
Institutional Reputation	84
Encryption Awareness	82
Fraud Detection Systems	80

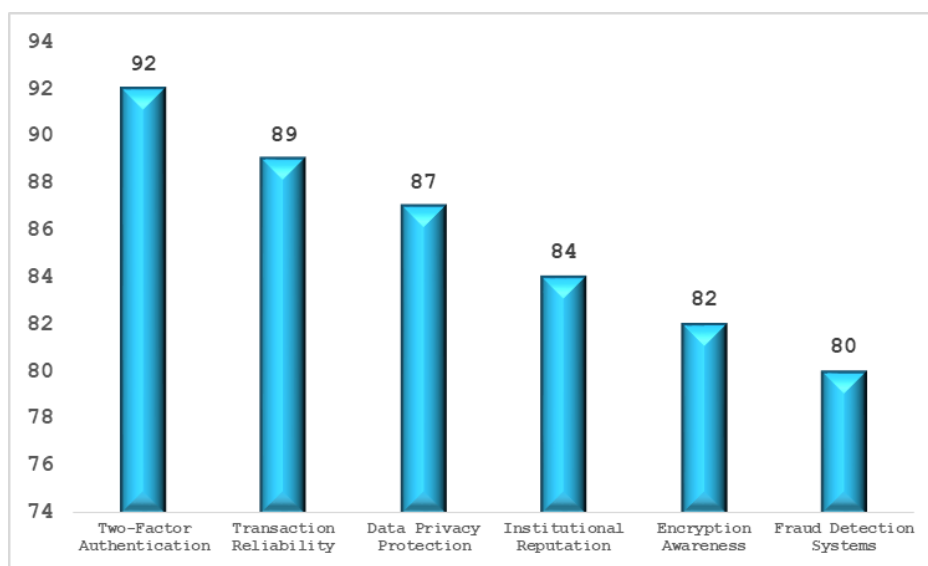


Fig 4 - Customer Perception Results

4.2.1. Two-Factor Authentication (92%)

The two-factor authentication (92%) had the highest positive response rate, which means customers view it as one of the most crucial security measures in digital banking. In this form of authentication, the user will need to provide two pieces of authentication, e.g., a password and a one-time password (OTP) sent to the mobile device. This extra layer of security is seen as a valuable addition to the security of their accounts and is very effective at stopping unauthorized access and cyber threats to accounts. Strong customer confidence in advanced authentication technologies, as shown by the high response rate.

4.2.2. Transaction Reliability (89%)

89% of the customers responded positively to transaction reliability, highlighting the value of correct and dependable financial transactions. Digital banking systems are expected to perform payment processing, account transfers, and updates without errors or delays. By ensuring that transactions are processed reliably, companies can reduce the risk of financial losses and service disruptions, which can lead to higher levels of customer satisfaction and trust. The results indicate that reliable transaction performance is one of the main factors in customers' ongoing usage of digital banking platforms.

4.2.3. Data Privacy Protection (87%)

87% of the respondents agreed that data privacy protection was handled favorably, showing that customers are very concerned with the security of their personal and financial data. Respondents believe banks need to have very robust privacy policies and security measures in place to ensure that sensitive data is not accessed, disclosed, or misused by anyone without authorization. When privacy is a top priority, it alleviates customer concerns about identity theft and data breaches, thereby promoting a greater feeling of safety and trust within digital banking offerings.

4.2.4. Institutional Reputation (84%)

With 84% of the positive response rate, institutional reputation was the highest, and it is seen that the credibility and public image of a bank plays a crucial role in establishing customer trust. Well-known and trusted financial institutions are more likely to attract customers to their digital banking services. A good reputation will convey reliability, professionalism, and attention to security for the customer. The findings suggest that customers perceive lower service quality and security measures of banks that lack a reputable brand, and this is reflected in their trust and usage.

4.2.5. Encryption Awareness (82%)

The awareness level of the customers about encryption was positive at 82%, indicating awareness of the importance of such technologies for securing online transactions. Encryption is the process of transforming data into a code that only authorized users with keys or passwords can read. When customers are aware of the importance of encryption, they are more likely to view digital banking platforms as secure and trustworthy. The results indicate that further increasing user awareness of encryption technologies can improve users' trust in online banking services.

4.2.6. *Fraud Detection Systems (80%)*

80% of the respondents said they were satisfied with fraud detection systems, which shows that customers appreciate the ability of banks to detect and deter suspicious activity. AI, machine learning, and behavioral analytics are used in the advanced fraud detection technologies to keep an eye on transactions and spot unusual patterns in real-time. When customers are aware that banks are actively watching for suspicious activity in their accounts and alerting them immediately, it makes them feel more secure. Fraud detection is one of the key security determinants even though it scores the lowest percentage of all the factors evaluated, but it is still a major factor in overall security perception and customer trust.

4.2.7. *Summary of Findings*

Security features that are relevant to customers' accounts and financial transactions clearly resonate with the customer, as evidenced by the results. Two-factor authentication, transaction reliability, protection of data privacy were the most influential, with institutional reputation, encryption awareness, and fraud detection systems showing strong positive effects. The results highlight the importance of comprehensive security measures to boost customer trust, adoption of digital banking, and customer loyalty in the long term.

4.3. Discussion

The results of this research indicate that there is a positive and strong association between perceived security and customer's trust in digital banking services. If customers think that a banking website offers sufficient protection against breaches, frauds, or unauthorized usage then they will be more inclined to go for the banking institution and actively use the digital services. Security perception is vital to minimizing the uncertainty and risk that is often linked with financial transactions conducted online. By instilling a sense of security with strong security measures, customers are more likely to embrace digital banking technologies and maintain their use of them for everyday financial transactions. This is in line with earlier studies that show that security is one of the major factors that can help to promote trust and technology acceptance in online banking settings. The importance of Security Awareness Programs and transparent communication to enhance customer trust is also emphasized in the study. When it comes to security, customers often assess it not just on technical aspects, but on how they work. Educating customers regularly about security practices, cyber threats and security measures can help increase awareness and help decrease the anxiety that customers may experience with their digital transactions. Also, clear information about privacy policies, data protection measures, and security updates encourages customers to trust the institution's dedication to protecting their interests. These efforts play a major role in the building of trust and promote customer retention. Another key conclusion is that the reputation of institutions plays a significant role in shaping customer trust. A proven track record of reliable service and financial stability, along with customer familiarity, has a positive impact on the customers' perception of trustworthiness for well-established financial institutions. A good reputation is likely to lead customers to expect greater security and service quality from a financial institution, which makes them more inclined to use the financial institution's online banking. Furthermore, the use of cutting-

edge cybersecurity solutions like biometric authentication, artificial intelligence-powered fraud detection, behavioral analytics, and real-time monitoring further contributes to the perception of safety and reliability for customers. The bank has been proactive in its security management and risk mitigation efforts, as evidenced by these technologies. In conclusion, the results indicate that a mix of robust security practices, customer education, clear communication, and institutional trust and credibility is vital to establishing trust, growing digital banking adoption, and achieving long-term customer loyalty in a digital financial system.

5. CONCLUSION

Digital banking has become a game-changer in the financial services landscape, offering customers easy access to financial services via the Internet and mobile devices. The advent of digital technologies has dramatically transformed the financial transactions landscape, providing advantages like accessibility, efficiency, speed, and cost reduction. In spite of these benefits, customer trust and security perception are still key factors that impact on the successful uptake and sustainability of digital banking services. Security is a crucial factor in customers' choice to engage with digital banking platforms, as they are often asked to provide sensitive personal and financial data online. Thus, for financial institutions aiming to enhance the customer relationships and cultivate the use of digital services, it is crucial to understand the elements that contribute to the formation of trust. The current research aimed to examine the impact of perceived security, privacy protection, transaction reliability, and institutional reputation on customer trust in a digital banking context. The results demonstrate that security perception has the greatest influence on the formation of trust. When customers feel that their digital banking services are secure from cyber threats, fraud, identity theft and unauthorized access, they are more likely to adopt and continue using them. The use of security measures like two-factor authentication, encryption technologies, secure communication protocols, privacy protection measures, and fraud detection systems is crucial to building customer confidence. These security measures diminish the risks felt by customers when using online platforms, making online banking safer and more appealing to customers. The study also proves that institutional reputation plays a significant role in customer trust and confidence. Customers tend to trust financial institutions that are known for their reliability, transparency, and service quality. Existing banks have existing customer base and credibility in history which is good for their perceptions of security and reliability. Moreover, the clear disclosure of security policies, privacy policies, and risk management plans can help build trust and alleviate customer concerns about digital transactions. The suggested trust evaluation framework provides a structured approach to analyzing the combined effect of various factors on customers' trust in digital banking services. The results indicate that financial institutions need to be investing in sophisticated cybersecurity solutions, customer education initiatives, secure authentication systems, and monitoring solutions. These programs can reduce the security risks and enhance customer satisfaction, loyalty, and retention. The study could extend to the impact of new technologies like artificial intelligence, blockchain, biometric authentication, and behavioral analytics on digital banking security and trust, which could be a focus for future research. In the digital financial landscape, security perception and

customer trust will continue to be a critical strategic pillar for sustainable growth and a competitive advantage for banks.

REFERENCES

- [1] Gefen David, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," *MIS Quarterly*, vol. 27, no. 1, pp. 51-90, 2003.
- [2] Yousafzai Shumaila Y., J. G. Pallister, and G. R. Foxall, "A proposed model of e-trust for electronic banking," *Technovation*, vol. 23, no. 11, pp. 847-860, 2003.
- [3] McKnight D. Harrison, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce," *Information Systems Research*, vol. 13, no. 3, pp. 334-359, 2002.
- [4] Flavián Carlos, M. Guinalíu, and R. Gurrea, "The role played by perceived usability, satisfaction and consumer trust on website loyalty," *Information & Management*, vol. 43, no. 1, pp. 1-14, 2006.
- [5] Lee Ming-Chi, "Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit," *Electronic Commerce Research and Applications*, vol. 8, no. 3, pp. 130-141, 2009.
- [6] Suh Bomil and I. Han, "The impact of customer trust and perception of security control on the acceptance of electronic commerce," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 135-161, 2003.
- [7] Belanger France, J. S. Hiller, and W. J. Smith, "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes," *Journal of Strategic Information Systems*, vol. 11, no. 3-4, pp. 245-270, 2002.
- [8] Pikkarainen Tero, K. Pikkarainen, H. Karjaluoto, and S. Pahnla, "Consumer acceptance of online banking: An extension of the technology acceptance model," *Internet Research*, vol. 14, no. 3, pp. 224-235, 2004.
- [9] Roca Juan Carlos, J. J. García, and J. J. de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Information Management & Computer Security*, vol. 17, no. 2, pp. 96-113, 2009.
- [10] Liao Ziqi and M. T. Cheung, "Internet-based e-banking and consumer attitudes: An empirical study," *Information & Management*, vol. 39, no. 4, pp. 283-295, 2002.
- [11] Venkatesh Viswanath, J. Y. L. Thong, and X. Xu, "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology," *MIS Quarterly*, vol. 36, no. 1, pp. 157-178, 2012.
- [12] Jain Anil K., A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.
- [13] Goodfellow Ian, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.