"Building trust and security in a digital banking environment: Customer perceptions of security risks in digital banking and how marketing campaigns can address these concerns and promote trust"

By:

MUZAMMAL ABBAS 01-322222-021

MBA 2 YEARS WEEKEND PROGRAM

Supervisor:

NAIMAH KHAN

Department of Business Studies

Bahria University Islamabad

Spring-2024

Majors: MKT

S.No. 21

"Building trust and security in a digital banking environment: Customer perceptions of security risks in digital banking and how marketing campaigns can address these concerns and promote trust"

By:

MUZAMMAL ABBAS 01-322222-021

MBA 2 YEARS WEEKEND PROGRAM

Supervisor:

NAIMAH KHAN

Department of Business Studies

Bahria University Islamabad

Spring-2024

FINAL PROJECT/THESIS APPROVAL SHEET

Viva-Voce Examination

Viva Date / /

Topic of Research: Building trust and security in a digital banking environment: Customer perceptions of security risks in digital banking and how marketing campaigns can address these concerns and promote trust

Names of Student(s): **Enroll #**

- MUZAMMAL ABBAS 01-322222-021

Class: MBA 2 Years (Weekend Program)

Approved by:

NAIMAH KHAN

Supervisor

Examiner-I

Examiner-II

Dr. Syed Haider Ali Shah

Research Coordinator

Dr. Khalil Ullah Muhammad

Head of Department (Business Studies)

Acknowledgments

First In the beginning, all praise belongs to Allah, the Highest, for granting me the strength and wisdom to complete this thesis. His blessings have sustained me throughout this journey.

I would like to express my sincere appreciation to my thesis advisor, Ms. Naimah Khan, from Bahria University, Islamabad. I am particularly grateful for the opportunity she provided me to pursue this research topic. Her guidance has been invaluable throughout the process, Her enthusiasm for the subject matter was truly contagious, and her unwavering honesty and determination were a constant source of inspiration. She offered invaluable insights that helped me to refine my approach to the research and present it in a clear and concise manner. The privilege of working and learning under her mentorship for such an extended period is something I will always cherish. I am also grateful for her unwavering support, and responsiveness, which helped to create a positive and productive research environment.

Finally, I would like to express my deepest gratitude to my parents, whose love, prayers, care, and sacrifices have been instrumental in my education and preparation for the future. The same level of appreciation goes to my sisters and brothers for their unwavering support.

Abstract

This research investigates the intricate interplay between digital security measures, customer perceptions of security risks, and the development of effective marketing campaigns within the digital banking sector in Islamabad and Rawalpindi, Pakistan. The primary objective of this study was to explore how the implementation of security measures impacts customer trust in digital banking, with a particular focus on the mediating role of transparent communication. The investigation delved into various elements of digital banking security, such as encryption, multi-factor authentication, fraud detection systems, and secure mobile banking applications, to understand their impact on customer trust and perceptions of security risks. To achieve this, a total of 306 questionnaires were distributed to digital banking customers in these cities, ensuring a diverse representation of the target population. SPSS was employed to assess the hypotheses, providing a robust analytical framework for understanding the complex relationships between security measures, transparent communication, and customer trust in digital banking. The study's results revealed a significant indirect positive association between security measures and customer trust, mediated by transparent communication. This indicates that while security measures alone can enhance customer trust, their impact is significantly strengthened when banks effectively communicate these measures to customers. An intriguing aspect unearthed in this research is the mediating role of transparent communication in the relationship between security measures and customer trust.

These findings bear particular importance for managers and marketers in the digital banking sector, emphasizing the need for the effective implementation and communication of robust security measures. By focusing on improving digital security capabilities and transparently communicating these efforts, banks can enhance the perceived security and trustworthiness of their services, leading to increased customer trust. The study recommends that organizational leadership incorporate strategies to enhance digital security attributes, such as investing in advanced encryption technologies, implementing multi-factor authentication, and ensuring proactive fraud detection systems, while also focusing on clear and transparent communication about these measures through marketing campaigns.

Table of Contents

Chapter 1

Introduction

1.1 Background of the study

The interest and other services, such as providing financial aid, managing mortgages, and assisting investors in achieving success, were the traditional sources of income for banks. However, the competition from non-financial institutions and numerous other difficulties the banks encountered has worsened the returns for these services, meaning they were unable to make a sizable profit (Stewart & Jürjens, 2018). These days, banks are expected to offer excellent services with improved technology and higher service standards in addition to accepting deposits and disbursing loans. Following the financial crisis of 2008, regulators overseeing the banking industry were acquainted with new guidelines and protocols that establish rules and guidelines for the industry. With the 2008 financial crisis and technological breakthroughs, a practical shift in financial services has occurred (Anagnostopoulos, 2018). Financial technology have become essential for banks to offer their clients easier and more convenient services that are user-friendly. Romanová and Kudinska (2016). Financial technology is the source of the euphemism "FINTECH." This combines the fundamental business functions (transactions, payments) carried out via internet-based technologies, mobile banking, and ATMs. (Koch, Siering, & Gomber, 2017).

Financial innovation, or fintech as it is now often known, has captured people's attention and loyalty, as seen by the volume of investments, product offers, businesses, and media attention. It has enormous untapped social benefits. Along with helping to increase financial inclusion and new financial intermediation submissions, it will also replace the traditional financial structure with new technologies and come at a cost that is roughly 2% of the GDP of some advanced economies (Aaron, Rivadeneyra & Sohal, 2017). The financial services innovation that this service offers benefits the people who use it. Businesses benefit from it, but customers also find it to be a simple and quick method of completing transactions, making their lives easier. When basic financial services like payments, credit, savings, insurance, and remittances are accessed and provided through digital channels like the internet, ATMs (automated teller machines), mobile phones, tablets, biometric devices, inevitably enabled cards, and point-of-sale (POS) systems, they are referred to as digital financial services (AFI 2016). By connecting people and companies to an electronic payment system, these technologies replace point of sale (POS) equipment and allow for quick, transparent, and seamless transactions for all involved.

In the modern banking landscape, the arrival of digital technology has catalysed a paradigm shift in how financial services are accessed and disbursed. Digital banking has become identical with suitability, offering customers unique and flexible accessibility to manage their finances remotely. However, amongst the proliferation of digital banking channels, ensuring trust and security has emerged as a supreme concern for both customers and financial institutions.
This thesis delves into the intricate dynamics of trust and security within the digital banking environment, focusing on customer perceptions of security risks and the role of marketing campaigns in addressing these concerns to foster trust. The study aims to provide insights into the factors influencing customer trust in digital banking and the efficacy of marketing strategies in pacifying security fears.

The relevance of this research is underscored by the escalating cybersecurity threats facing the banking sector and the imperative to safeguard customer data and financial assets. As consumers entrust sensitive information to digital platforms, concerns regarding data breaches, identity theft, and financial fraud loom large. Thus, understanding the determinants of customer trust and the perceived effectiveness of security measures is essential for banks to enhance security protocols and reassure customers. Moreover, marketing campaigns play a pivotal role in shaping consumer perceptions and behaviour in the digital realm. Through strategic messaging and communication, banks can instil confidence, educate customers about security measures, and differentiate their offerings from competitors. However, the success of these campaigns' centres on a nuanced understanding of customer attitudes, preferences, and trust-building mechanisms. To address these intricacies, the research adopts an interdisciplinary approach, drawing on insights from psychology, marketing, and cybersecurity. By exploring the psychological underpinnings of trust, the effectiveness of security measures, and the impact of marketing communication on customer perceptions, this research seeks to provide actionable recommendations for banks to enhance trust and security in digital banking.

This research lays the foundation for an in-depth examination of trust, security, and marketing in the digital banking landscape. By elucidating customer perceptions of security risks and the potential of marketing campaigns to mitigate these concerns, this study aims to contribute valuable insights to academia, industry practitioners, and policymakers.

1.2 Problem Statement

The rapid evolution of digital banking has revolutionized the financial industry, offering unprecedented convenience and accessibility to customers. This transformation has facilitated seamless transactions, instant access to financial services, and personalized customer experiences. However, it has also introduced significant security challenges that can undermine customer trust. Despite advancements in security technologies, customers continue to perceive digital banking as fraught with risks such as data breaches, identity theft, and fraud. These security concerns can deter customers from fully embracing digital banking services, impeding the growth and potential of digital banking platforms. Understanding customer perceptions of security risks is critical for financial institutions aiming to build trust and foster a secure digital banking environment. Moreover, effectively addressing these perceptions through strategic marketing campaigns is essential to mitigate fears and promote confidence in digital banking services (Lee & Kim, 2021).

The banking industry, characterized by intense competition and rapid technological advancements, must prioritize security to maintain customer trust. Financial institutions such as JPMorgan Chase, Bank of America, and HSBC have set benchmarks in implementing comprehensive security measures. These institutions invest heavily in cutting-edge cybersecurity technologies, including artificial intelligence, machine learning, and blockchain, to protect customer data and transactions. Furthermore, the banking industry recognizes the importance of transparent communication regarding security practices. For example, JPMorgan Chase's proactive communication strategy includes regular updates on security enhancements and educational initiatives to help customers protect themselves online (Smith & Johnson, 2022). Similarly, Bank of America's commitment to cybersecurity is highlighted through campaigns that emphasize their use of multi-factor authentication, biometric verification, and real-time fraud detection systems (Williams & Nguyen, 2020).

Despite these efforts, the industry faces an ongoing challenge in changing customer perceptions. The proliferation of high-profile cyber-attacks and data breaches across various sectors contributes to a general sense of vulnerability among consumers. To counter this, banks are employing sophisticated marketing strategies to reassure customers about the safety of their digital platforms. For instance, Citibank's "Safety is Our Priority" campaign effectively

showcased their comprehensive security measures, resulting in increased customer trust and higher adoption rates of their digital services (Chen et al., 2015).

This research seeks to explore the nature and extent of customer security concerns in the digital banking landscape and to identify how targeted marketing strategies can alleviate these concerns. By examining the interplay between perceived security risks and trust-building measures, this study aims to provide actionable insights for financial institutions to enhance customer trust and ensure a secure digital banking experience.

The study will analyse how industry best practices can be adapted and applied across various financial institutions to address customer concerns and promote a secure digital banking environment. By focusing on successful case studies and innovative security protocols, the research will provide a roadmap for banks to mitigate security risks and foster a culture of trust and reliability. This, in turn, is crucial for the sustained growth and success of digital banking platforms in an increasingly digital world.

1.3 Research Objectives

To investigate the direct impact of the implementation of security measures on customer perception of security risks in digital banking.

To investigate the direct impact of the level of transparency in communication about the security measures taken by the bank on customer perception of security risks in digital banking.

To assess the mediating role of the level of transparency in communication about the security measures taken by the bank on the relationship between the implementation of security measures and customer perception of security risks.

1.4 Research Questions

How does the implementation of security measures directly impact customer perception of security risks in digital banking?

How does the level of transparency in communication about the security measures taken by the bank directly impact customer perception of security risks in digital banking?

What is the mediating role of the level of transparency in communication about the security measures taken by the bank on the relationship between the implementation of security measures and customer perception of security risks in digital banking?

1.5 Research Gap:

1.5.1 Evidence Gap

Previous studies on building trust and security in digital banking have predominantly been conducted in more developed regions, such as North America and Europe, where the technological infrastructure, regulatory environment, and consumer behaviour significantly differ from those in developing countries. These regions benefit from advanced technology, higher internet penetration rates, and more established digital banking frameworks. Consequently, the insights and findings from these studies may not be directly applicable or fully relevant to the unique socio-economic, cultural, and technological context of developing countries like Pakistan (Khan, Rizvi, & Shaikh, 2018; Saeed et al., 2019).

In Pakistan, factors such as varying levels of digital literacy, differing trust levels in financial institutions, and distinct cultural attitudes towards technology and security play a crucial role in shaping customer perceptions and behaviours. Moreover, the financial inclusion landscape in Pakistan presents its own set of challenges and opportunities, which are not adequately addressed by existing research focused on developed markets. This gap underscores the necessity for context-specific research that not only acknowledges but also deeply investigates these distinct factors, thereby providing more accurate and actionable insights for improving digital banking trust and security in Pakistan. Such research could help in developing tailored

strategies that resonate with the local population, ultimately fostering greater adoption and trust in digital banking services.

1.5.2 Knowledge Gap

There is a noticeable lack of comprehensive research that integrates both technical security measures and marketing strategies in the context of digital banking. Existing studies tend to treat these aspects in isolation, focusing either on the technical aspects of security or on marketing strategies without exploring their combined effect on customer trust.

Technical security measures, such as encryption, multi-factor authentication, and fraud detection systems, are essential for protecting customer data and preventing breaches. However, the effectiveness of these measures can be significantly enhanced when complemented by strategic marketing efforts that communicate their presence and benefits to customers (Cruz et al., 2019; Lee & Turban, 2020). Marketing strategies, including transparent communication, customer education, and targeted campaigns, play a vital role in shaping customer perceptions and trust. Understanding the interplay between these security measures and marketing strategies is crucial for developing holistic approaches that effectively build and sustain customer trust in digital banking.

By integrating these elements, future research can provide a more nuanced understanding of how technical and marketing efforts can work synergistically to enhance customer trust. This comprehensive approach is essential for addressing the multifaceted nature of trust in digital banking, which is influenced by both the actual security measures in place and how these measures are perceived and understood by customers.

1.5.3 Educational Gap

Previous studies frequently neglect the importance of customer education and awareness about digital banking security measures. While technical solutions are essential, ensuring that these security protocols are recognized and trusted by customers is equally vital. Many customers

may not fully understand the significance of certain security measures, leading to underutilization or mistrust (White, 2020; Balaji et al., 2021).

Comprehensive education and awareness initiatives can bridge this gap by informing customers about the various security measures in place and how they protect their financial data. Such initiatives can include targeted communication campaigns, user-friendly educational resources, and interactive training sessions. These efforts can help demystify complex security concepts, making them more accessible and understandable to the average customer.

Ensuring that customers are well-informed about digital banking security not only enhances their trust but also encourages more secure online behaviours. For instance, educated customers are more likely to adopt recommended security practices, such as using strong passwords, enabling multi-factor authentication, and recognizing phishing attempts. This gap highlights the need for more focused research on the role of customer education in enhancing the effectiveness of digital security measures and building long-term trust in digital banking.

1.6 Research Significance

Pakistan has 33 banks total; there are 5 international banks, 5 local governmental banks, and 15 private banks. These banks all offer a wide range of online banking options in addition to other services. In essence, e-banking services help users with account statements, credit card services, mobile banking, point-of-sale services, money transfers, bill payments, and account-related inquiries, among other things. Since all banks offer nearly identical products to their clients, Pakistan's financial institutions are more competitive. Thus, banking institutions in Pakistan face a significant problem in the long run in developing and maintaining strong customer connections. For this reason, thorough scientific research on client e-loyalty is required. It ought to be more beneficial for banking institutions' policymakers. Research on banking consumer trust, contentment, and loyalty towards E-banking services is still necessary, even though e-banking services in Pakistan are constantly improving (Alansari & Al-Sartawi, 2021). The National Payment System Strategy (NPSS) for the nation's digital payment network has been introduced by the State Bank of Pakistan. 2008 saw the launch of digital financial services in Pakistan following the adoption of branchless laws. With the country's approval of the national inclusion plan in 2015, which aims to create a dynamic and inclusive financial

system, the growth of financial services has risen. These regulations pushed private sector investment in microfinance organizations by digital financial service providers. As a result, telebanking, online banking, ATMs, credit cards, and debit cards have become efficient means of distributing conventional banking goods. Leading mobile phone providers Telenor and Jazz, which provide basic financial services like simple paisa and jazz cash to unbanked individuals, are the best examples of non-banking systems. With these services, customers can open an account without going to a bank branch, transfer money, make deposits or withdrawals, pay their energy bills and cell bills, and more. Easy Paisa has 7.29 million over-the-counter users, whereas Jazz Cash has approximately 8 million monthly active customers.

Chapter 2

Literature Review

2.1 Customer Perceptions of Security Risks in Digital Banking

The digital uprising in banking has deeply reshaped the financial landscape, offering matchless ease and access to financial services round-the-clock. However, this shift has also brought about a pressing concern: the necessity to instil trust and security in a virtual realm. With customers increasingly relying on digital platforms for their financial transactions, it becomes imperative to realize and address their angsts regarding security. This literature review delves into existing research on customer perceptions of security risks in digital banking and examines how marketing campaigns can alleviate these concerns and nurture trust.

Customer perceptions of security risks in digital banking are influenced by various factors, including the perceived weakness of digital channels, concerns about data privacy, and experiences with security breaches. Culnan and Armstrong (1999) highlight the importance of procedural fairness in shaping individuals' perceptions of privacy and trust in online transactions. Similarly, Dinev and Hart (2006) propose an extended privacy calculus model, which emphasizes the role of perceived benefits, risks, and trust in influencing consumers' willingness.

The effectiveness of security-related communication strategies in digital banking largely depends on their ability to align with customers' risk perceptions and concerns. Research by Xiao and Benbasat (2007) emphasizes the importance of tailoring communication messages to address customers' specific security concerns and preferences. Additionally, a study by Yousafzai et al. (2009) found that personalized communication strategies can enhance customers' perceptions of security and trust in online banking platforms. By adopting a customer-centric approach to security communication, financial institutions can effectively address customers' perceptions of security risks and foster trust in digital banking services to disclose personal information online.

Moreover, research by Komiak and Benbasat (2006) underscores the significance of personalization and familiarity in fostering trust and adoption of online banking services. They argue that personalized recommendations and familiar interfaces can mitigate perceived risks and enhance user trust. Conversely, Siponen and Vance (2010) explore the phenomenon of neutralization, whereby employees rationalize violations of information security policies.

Understanding these cognitive mechanisms is crucial for designing effective security measures and communication strategies in digital banking.

Addressing these concerns requires a comprehensive understanding of the factors shaping customers' perceptions of security risks in digital banking. Research by Kim et al. (2017) highlights that perceived susceptibility to security threats, perceived severity of potential security breaches, and perceived benefits of digital banking influence customers' perceptions of security risks. Additionally, the study by Metawa and Almossawi (2017) identifies perceived control as a significant factor affecting customers' perceptions of security risks in online banking. By examining these factors, financial institutions can develop targeted strategies to mitigate customers' concerns and promote trust in digital banking platforms.

The effectiveness of marketing campaigns in promoting trust in digital banking hinges on their ability to resonate with customers' perceptions of security risks. Research by Belanche et al. (2019) underscores the importance of tailoring marketing messages to align with customers' risk perceptions and concerns. Similarly, a study by Liao et al. (2019) emphasizes the role of transparency and authenticity in marketing communications, suggesting that clear and honest messaging can enhance customers' trust in digital banking platforms. By aligning marketing campaigns with customers' perceptions of security risks, financial institutions can enhance the effectiveness of their promotional efforts and build stronger relationships with customers.

Customer perceptions of security risks in digital banking play a pivotal role in shaping their trust and confidence in online financial services. Research by Alalwan et al. (2018) underscores the significance of these perceptions, indicating that customers' perceived security risks significantly influence their intention to adopt digital banking channels. Additionally, the study by Alsolami et al. (2020) found that customers' perceptions of security risks are a primary factor affecting their trust in online banking platforms. These findings highlight the importance of understanding and addressing customers' perceptions of security risks in the context of digital banking.

Understanding the factors shaping these perceptions, including the evaluation of security measures, trust in online transactions, and communication strategies, is essential for financial institutions to effectively address customers' concerns and promote trust in digital banking platforms.

Additionally, cultural and demographic factors influence customers' perceptions of security risks in digital banking. For instance, research by Li and Zhang (2018) suggests that cultural attitudes toward technology and risk-taking behaviour impact individuals' willingness to engage with digital banking services. Similarly, age, income level, and prior experience with cyber incidents have been identified as significant predictors of perceived security risks in online banking (Chen et al., 2017).

The critical role of communication and marketing strategies in addressing customer concerns about security risks in digital banking. Effective communication of security measures and protocols can enhance customers' perceptions of safety and trustworthiness (Liu et al., 2016). Likewise, marketing campaigns that emphasize the robustness of security features and highlight the benefits of digital banking can help alleviate fears and promote adoption among hesitant customers (Wang et al., 2018).

Hypothesis 1: The implementation of security measures has a significant direct positive impact on customer perception of security risks.

2.2 Factors Influencing Customer Trust in Digital Banking

Customer trust in digital banking is shaped by a myriad of factors, including perceived security, reliability, competence, and benevolence of the banking institution. Smith, Milberg, and Burke (1996) identify information privacy concerns as a key determinant of individuals' trust in organizational practices. They argue that organizations must address privacy issues transparently to build and maintain trust among customers. Building trust and security in the digital environment is paramount for fostering customer confidence in digital banking platforms. Research by Pavlou and Gefen (2004) suggests that trust plays a crucial role in shaping customers' perceptions of security risks and their willingness to engage in online transactions. Furthermore, the study by McKnight et al. (2002) highlights the significant influence of trust on customers' intentions to adopt digital banking services. These findings underscore the importance of trust as a key dependent variable in understanding customers' perceptions of security risks in digital banking.

Customer acuities of security risks in digital banking are closely intertwined with their trust in the security measures implemented by financial institutions. Research by Kim et al. (2013) indicates that customers' trust in the reliability and effectiveness of security protocols

significantly influences their perceptions of security risks in online banking. Moreover, a study by Dhamija et al. (2000) found that customers' trust in the security of online transactions is a critical determinant of their willingness to disclose sensitive information. By enhancing trust in digital banking platforms, financial institutions can mitigate customers' perceptions of security risks and promote a sense of confidence in online financial services.

Effective marketing campaigns play a key role in shaping customers' perceptions of trust and security in digital banking. Research by Chen et al. (2019) suggests that marketing messages emphasizing the security features and benefits of digital banking platforms can positively influence customers' perceptions of security risks. Additionally, the study by Wu and Lu (2013) found that marketing communications focusing on the reliability and trustworthiness of financial institutions can enhance customers' trust in online banking services. By aligning marketing campaigns with customers' perceptions of security risks, financial institutions can effectively address concerns and foster trust in digital banking platforms.

Customer awareness initiatives are essential for edifice trust and security in the digital atmosphere. Research by Li and Kim (2018) emphasizes the importance of educating customers about security best practices and the risks associated with online banking. Similarly, a study by Aladwani (2006) suggests that increasing customers' awareness of security measures can enhance their trust in digital banking platforms. By empowering customers with knowledge and information, financial institutions can install confidence and promote a sense of security in digital banking transactions.

Furthermore, research by Gefen, Karahanna, and Straub (2003) underscores the importance of perceived security in influencing consumers' trust and intention to engage in online transactions. They propose a model of trust in technology, which highlights the role of perceived security, system quality, and information quality in shaping user trust. Similarly, Pavlou and Gefen (2004) emphasize the importance of trust in e-commerce transactions, highlighting the impact of perceived risk and uncertainty on consumer behaviour. In research by McKnight, Choudhury, and Kacmar (2002) explore the role of interpersonal trust in shaping individuals' trust in online transactions. They argue that interpersonal trust, characterized by integrity, benevolence, and ability, can transfer to trust in online platforms. Understanding these relation studies underscore the crucial role that security concerns play in shaping user behaviour and influencing the adoption of digital banking platforms. Rafferty & Fajar (2022)

underscore security as a major determinant of user behaviour, potentially serving as a barrier to the adoption of digital banking services. Similarly, Cai et al. (2023) stress the significance of perceived security (PIB) in fostering trust and confidence among users of digital banking services. This literature finds various causes of customer security worries in the digital territory. Moscato and Altschuller (2012) and Laksamana et al. (2022) pinpoint data security and privacy as primary concerns, with customers fearing unauthorized access to their financial information and its potential misuse for fraudulent activities. Moreover, the frequency of phishing scams and malware targeting online banking users further make worse these worries (Akthar et al., 2023). Security dynamics are crucial for banks to foster trust and loyalty among digital banking customers.

Trust and security in the digital environment are imperative for fostering customer confidence in digital banking platforms. Trust serves as a crucial dependent variable that significantly influences customers' perceptions of security risks and their willingness to engage in online transactions. By enhancing trust through effective marketing campaigns, customer education, and awareness initiatives, financial institutions can mitigate customers' concerns and promote a sense of security and confidence in digital banking services.

2.3 The Role of Marketing Campaigns in Addressing Security Concerns and Promoting Trust

Marketing campaigns play can help to addressing security concerns and promoting trust in the digital banking environment. Through strategic communication and messaging, banks can educate customers about security measures, demonstrate their commitment to protecting customer data, and differentiate their offerings from competitors. However, the effectiveness of marketing campaigns depends on a nuanced understanding of customer attitudes, preferences, and trust-building mechanisms.

Research by Chen and Zhang (2014) highlights the impact of marketing communication on consumer perceptions of security and trust in online banking. They propose a model of trust transfer, which suggests that trust in the banking institution can transfer to trust in online channels through effective marketing communication. Similarly, Beldad, de Jong, and Steehouder (2010) emphasize the role of website quality and usability in shaping consumer trust and satisfaction in online banking.

Moreover, research by Luo and Ba (2012) explores the influence of social media on consumer trust and engagement in financial services. They argue that social media platforms can serve as powerful tools for banks to engage with customers, address their concerns, and build trust through transparent communication. Understanding the dynamics of social media marketing is essential for banks to leverage these platforms effectively in promoting trust and security in digital banking.

Marketing campaigns exert considerable influence in addressing customer security concerns and fostering trust in digital banking. Research by Saeidi et al. (2015) suggests that transparency about data security practices and ethical data processing significantly enhances customer satisfaction and trust. Similarly, Herden et al. (2021) underscores the importance of marketing campaigns that emphasize a commitment to ethical data practices and highlight the positive societal impact of secure digital banking.

The design of marketing campaigns themselves can shape user trust. Ashrafi & Easmin (2023) suggest that marketing materials showcasing robust authentication methods, such as biometrics, can enhance user confidence in the security of digital banking platforms. Customer trust in digital banking serves as a crucial mediating variable in the relationship between perceptions of security risks and actual behaviour. Research by Gefen et al. (2003) suggests that trust mediates the effect of perceived security risks on customers' intentions to use online banking services. Additionally, the study by Hair et al. (2019) found that trust partially mediates the relationship between security perceptions and customers' willingness to adopt digital banking platforms. These findings underscore the pivotal role of trust as a mediating variable in understanding how perceptions of security risks influence customers' behaviour in digital banking environments. Still, customer trust in digital banking platforms is influenced by their perceptions of the reliability and credibility of security measures deployed by financial institutions. Research by McKnight and Choudhury (2002) indicates that perceived security directly affects customers' trust in online banking services. Similarly, a study by Wang et al. (2016) found that customers' perceptions of security significantly impact their trust in the security infrastructure of digital banking platforms. By mediating the relationship between security perceptions and trust, financial institutions can effectively mitigate customers' concerns and foster confidence in digital banking services. Likewise, the design and functionality of digital banking platforms play a crucial role in shaping customers' trust in online transactions. Research by Pavlou (2003) suggests that the usability and transparency of

digital banking interfaces influence customers' perceptions of trustworthiness. Additionally, the study by Flavián et al. (2006) found that the perceived ease of use and reliability of digital banking platforms positively affect customers' trust in online banking services. By enhancing the user experience and ensuring the reliability of digital banking platforms, financial institutions can bolster customers' trust and mitigate concerns about security risks.

Effective marketing campaigns can serve as a catalyst in fostering customer trust in digital banking platforms. Research by Kim and Park (2019) suggests that marketing messages emphasizing the reliability and security of digital banking services can positively influence customers' perceptions of trust. Similarly, a study by Wu and Wang (2019) found that marketing communications highlighting the robustness of security measures can enhance customers' trust in online banking platforms. By mediating the relationship between security perceptions and trust, marketing campaigns play a crucial role in addressing customers' concerns and promoting confidence in digital banking services.

In conclusion, customer trust in digital banking serves as an essential mediating variable in relationship between perceptions of security risks and actual behaviour. Trust influences customers' willingness to engage with digital banking platforms and mitigates anxieties about security risks. By understanding the factors shaping trust in digital banking, financial institutions can develop targeted strategies to foster confidence and promote the adoption of digital financial services.

This literature review has provided a comprehensive overview of existing research relevant to the study's focus on trust, security, and marketing in the digital banking environment. By synthesizing insights from diverse disciplinary perspectives, including psychology, marketing, and cybersecurity, this review lays the foundation for the subsequent empirical investigation. Building on the theoretical frameworks and empirical findings outlined in this review, the study aims to contribute novel insights to academia, industry practitioners, and policymakers seeking to enhance trust and security in digital banking.

Hypothesis 2: The implementation of security measures has a significant direct positive impact on the level of transparency in communication about security measures.

Hypothesis 3: The level of transparency in communication about security measures has a significant direct impact on customer perception of security risks and trust.

2.4 Relationship between all variables

In the context of building trust and security in digital banking, understanding the relationships between the variables is crucial for developing effective strategies to address customer concerns and enhance trust. The variables in this study include the independent variable (implementation of security measures), the dependent variable (customer perception of security risk and trust), and the mediating variable (level of transparency in communication about security measures taken by the bank). This section explores how these variables interact with each other and their impact on customer perceptions and trust in digital banking.

2.4.1 Implementation of Security Measures and Customer Perception of Security Risks and Trust

The implementation of security measures is a critical independent variable that directly influences customer perception of security risks and trust in digital banking. Effective security measures, such as robust encryption, multi-factor authentication, and regular security audits, can significantly reduce perceived security risks. Research indicates that customers are more likely to trust digital banking platforms that demonstrate a strong commitment to security (Kim et al., 2013). Therefore, the implementation of comprehensive security measures is essential for fostering a sense of safety and trust among customers.

Customer perception of security risks and trust serves as the dependent variable in this study. Perceived security risks refer to customers' concerns about the potential threats and vulnerabilities associated with using digital banking services. Trust, on the other hand, encompasses customers' confidence in the reliability, integrity, and security of the digital banking platform. Research shows that perceived security risks negatively impact trust, which in turn affects customers' willingness to engage with digital banking services (McKnight et al., 2002). Thus, reducing perceived security risks is critical for building and maintaining trust in digital banking.

2.4.2 Level of Transparency in Communication and Customer Perception of Security Risks and Trust

The level of transparency in communication about security measures taken by the bank acts as a mediating variable. Transparent communication involves providing clear, accurate, and timely information about the security measures implemented to protect customer data and transactions. Studies

have shown that transparency in communication can enhance customer trust by alleviating concerns and demonstrating the bank's commitment to security (Liu et al., 2016). When customers are well-informed about the security protocols in place, their perception of security risks decreases, and their trust in the digital banking platform increases.

The interaction between the implementation of security measures and the level of transparency in communication plays a pivotal role in shaping customer perceptions of security risks and trust. Effective security measures, when communicated transparently, can significantly enhance customer trust and reduce perceived security risks. For instance, a bank that implements advanced security technologies and regularly updates customers about these measures is likely to be perceived as more trustworthy. Conversely, a lack of transparency can undermine the effectiveness of even the most robust security measures, as customers may remain sceptical about the platform's security.

Hypothesis 4: The level of transparency in communication about security measures mediates the relationship between the implementation of security measures and customer perception of security risks and trust.

2.4 Underpinning Theories

Technology Acceptance Model (TAM)

TAM focuses on understanding users' acceptance and usage of technology based on their perceptions of its usefulness and ease of use. In the context of digital banking, TAM can elucidate how customers' perceptions of security risks and the effectiveness of marketing campaigns influence their trust in online banking platforms. Perceived security risks directly influence perceived usefulness, while marketing campaigns can shape perceptions of ease of use and usefulness through persuasive messaging. The Technology Acceptance Model (TAM) is a widely used theoretical framework in the field of Information Systems and Technology Management. It was developed by Fred Davis in the late 1980s and later extended by Fred Davis and Richard Bagozzi. TAM seeks to explain and predict users' acceptance and adoption of new information technologies or systems based on their perceptions of usefulness and ease of use. In a perceived usefulness an individual believes that using a particular technology or system would enhance their job performance, productivity, or effectiveness. It is influenced by

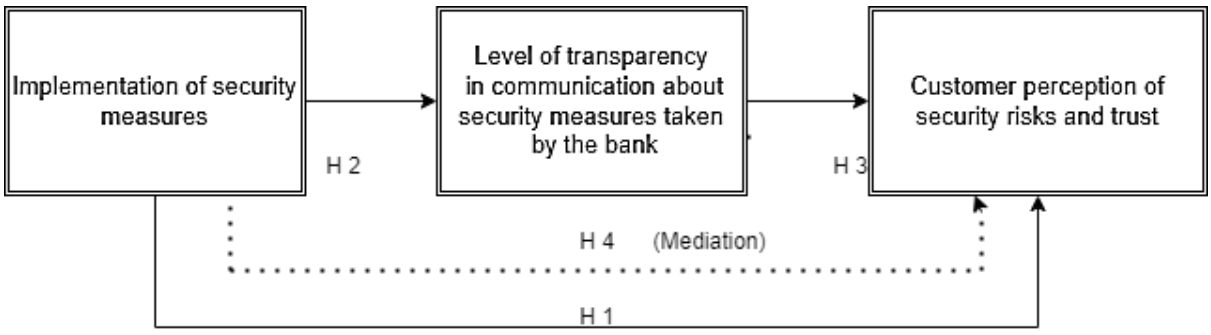
factors such as the perceived utility, benefits, and advantages of the technology in fulfilling users' needs and goals. An individual's perception of the level of effort and cognitive demand required when using a specific technology or system. It is influenced by various factors such as the technology's complexity, simplicity, and user-friendly attributes in terms of navigation, interaction, and learning curve. These elements collectively shape users' perceptions of how straightforward and hassle-free it would be to engage with the technology. The overall user-friendliness of the technology plays a significant role in shaping perceptions of ease of use. User-friendly features such as drag-and-drop functionality, context-sensitive help, and error prevention mechanisms contribute to a positive user experience and facilitate smooth interactions. The ease of navigation within the technology or system influences users' perceptions of ease of use. Intuitive navigation structures, consistent menu layouts, and logical information architecture make it easier for users to find what they need and accomplish their tasks efficiently. The complexity of the technology or system affects users' perceptions of ease of use. Complex interfaces or functionalities may be perceived as more difficult to use, while simpler designs and features are often seen as easier to navigate and interact with.

Trust Theory

Trust theory, a foundational component of TAM, explores how users' trust in a system influences their willingness to use it. In the context of digital banking, customers' trust in the security measures and reliability of online platforms significantly impacts their adoption and usage behaviours. Trust theory posits that trust is built upon perceived security, integrity, and benevolence, all of which are crucial in digital banking environments where customers entrust their financial information and transactions. Trust can be broadly defined as the willingness of an individual (trustor) to be vulnerable to the actions of another party (trustee) based on positive expectations about the trustee's intentions, reliability, competence, and integrity. Trust involves a degree of risk-taking, as the trustor relies on the trustee to act in their best interests and fulfil their obligations. Trust can be conceptualized as comprising multiple dimensions or components, including Cognitive Trust which refers to the rational assessment of the trustee's capabilities, reliability, and integrity based on past experiences, reputation, and observable behaviours, however affective trust involves emotional or affective attachments to the trustee, reflecting feelings of confidence, comfort, and security in the relationship. Trust fosters the development of strong, positive relationships based on mutual respect, cooperation, and

reciprocity. It reduces transaction costs by facilitating smoother interactions, reducing the need for elaborate contracts or monitoring mechanisms, and promoting cooperation. Organizational effectiveness, employee morale, customer satisfaction, and financial performance by fostering a positive work environment and facilitating collaboration and innovation by trust. In the context of digital banking, trust theory helps elucidate how customers' trust in the security measures, reliability, and integrity of online banking platforms influences their perceptions of security risks and their willingness to engage in online transactions. Financial institutions can leverage trust theory insights to design and implement strategies that enhance trust, mitigate security concerns, and promote customer confidence in digital banking services. This may include enhancing transparency, demonstrating trustworthiness, and building strong, positive relationships with customers through effective communication, service quality, and ethical practices.

2.5 Conceptual Framework



Chapter 3

Methodology

3.1 Introduction

Research methodology is defined as a systematic and scientific way of finding facts and exploring new dimensions (Rajasekar et al., 2016). It is the search for useful and new information on a specific topic that you have chosen. The research methodology aims to prove the facts that have been stated already. The research is conducted with the help of study, observation, experiments, comparison, reasoning, analysis, etc. This study explores the impact of implementing security measures on customer perception of security risk and trust in digital banking, with the mediating role of transparency in communication about security measures taken by banks. The research philosophy will be discussed first, followed by the methods of data collection and analysis.

3.2 Research Philosophy

To understand the nature and evolution of knowledge regarding how data is collected, processed, and used, philosophy is employed in research. As a result of this investigation, epistemology is the relevant research philosophy. Epistemology is primarily concerned with asking questions about the appropriate level of knowledge in a certain subject. Through rigorous testing, it determines the appropriate level of expertise in the subject of study and the validity of the material (Norris, 2019). According to the positivist philosophy utilized in this study, research questions are developed first, and then relevant data is used to progress the research. To verify a theory and make measurements against established knowledge, positivism is necessary. With this approach, researchers produce results that can be reproduced and used by others. It focuses on the study's quantitative outcomes. Some hypotheses can be tested and explained in this research; therefore, positivism is appropriate in this context.

3.3 Research Approach

The study has adopted a positivist paradigm to maintain objectivity, employing quantitative research methodology. Specifically, this study follows a deductive research approach. This deductive approach initiates by crafting hypotheses based on existing literature and subsequently designing research strategies to both establish and evaluate these hypotheses.

Researchers extensively gather and analyse data and information from literature to either corroborate or refute the proposed hypotheses (Jonker & Pennink, 2010). In essence, the deductive approach begins with theory development, hypothesis formulation, and the subsequent observation derived from the collected data. This study adopts a cross-sectional nature and confines itself to the positivist philosophy, a commonly utilized approach by many researchers in recent times. In the digital banking sector, this study was based on research questions that sought to determine the influence of security measures on customer perception of security risk and trust, using transparency in communication as a mediating factor; The research topic was answered through collecting data and analysing the results.

3.4 Research Design

Mackey and Gass (2015) define research design as the critical mechanism for managing data collection, estimation, and analysis. According to Flick (2015), a research design is a comprehensive plan that demonstrates the specialist's methods and strategies for acquiring and examining critical data. To accomplish the examination objectives, a positive technique was used for this evaluation. Subjective and quantitative methodologies can be used to guide exploration (Kumar, 2019). Because this study is based on quantifiable data, it was designed as a cross-sectional outline using a quantitative technique. Furthermore, a quantitative approach is employed. Gathering and examining mathematical facts and plans to quantify relationships, sentiments, methods of acting, or designs are examples of quantitative inquiry. For this study, a descriptive research design was used to find the impact of security measures on customer perception of security risk and trust, with the mediating effect of transparency in communication. This strategy is suited for this investigation since it considers the collection of structured data to quantify clear characteristics and break down examples or relationships within the data. In general, this investigation is planned with the specific goal of gathering and dissecting material using a quantitative technique through a cross-sectional review configuration, aligning with the positivist way of thinking of seeking discernible and measurable differences.

3.5 Research Strategy

A research strategy establishes a structured plan and guidance for conducting a study. In this study, a survey research design has been implemented. Surveys employ the technique of questionnaires to gather data concerning the practices, circumstances, and perspectives of individuals. The primary aim of this study is to collect information on the literature topic and analyse the gathered data to draw conclusions. Subsequently, quantitative analytical techniques have been applied to infer and evaluate the proposed relationships (McCusker & Gunaydin, 2015). The primary objective of this study is to gather information related to the literature topic being investigated. Researchers aim to collect data through the survey method and then analyse this gathered information thoroughly. The analysis process involves examining the data for patterns, correlations, or relationships between variables studied in the research. After collecting and analysing the data, quantitative analytical techniques are applied. These techniques help researchers draw inferences and conclusions regarding the proposed relationships among the variables under investigation. Quantitative analysis involves using statistical tools and methods to interpret the data and determine the strength or significance of relationships between variables.

3.6 Population

The target population encompasses 1,500 professionals working in various industries across Islamabad and Rawalpindi, Pakistan. Due to practical limitations, a representative sample is drawn from this population to ensure the feasibility and generalizability of the findings. The selection of a representative sample is crucial for ensuring that the insights and conclusions drawn from the study are applicable to the broader population of professionals in these cities. The target population is defined to include professionals from diverse demographic backgrounds, ensuring a comprehensive understanding of how marketing campaigns can address customer security concerns and promote trust in digital banking (Saunders et al., 2016).

3.7 Sample Size

Using Morgan's table, the sample size for this study was determined to be 306 professionals from a target population of 1,500. Out of the 306 professionals who were approached, responses were obtained from 297 professionals. These responses were used to analyse the

impact of marketing campaigns on customer perception of security risks and trust in digital banking. To effectively capture the wide range of strategies in Islamabad and Rawalpindi, purposive sampling is utilized to specifically target professionals who have a history of implementing security measures in digital banking. This sampling process will aim to encompass a diverse professional base in terms of demographics and behaviours, thereby enhancing the external validity and representativeness of the research findings.

3.8 Instrument Selection

Data was gathered using a well-organized questionnaire distributed among professionals. Existing scales from previous studies have been adjusted to suit the specific requirements of digital banking security and trust marketing in Islamabad and Rawalpindi. The instruments used are as follows:

Variable	Instrument Adopted From	Likert Scale
Implementation of Security Measures	Bruhn et al. (2012)	Five-Point
Customer Perception of Security Risk	Flavián and Guinalíu (2006)	Five-Point
Trust	Morgan and Hunt (1994)	Five-Point
Level of Transparency in Communication	Kim et al. (2004)	Five-Point

Chapter 4

Result & Analysis

4.1 Introduction

This chapter outlines the research methodology employed to investigate the influence of social media influencers on consumer purchase intention within Pakistan's telecommunication sector. Data analysis will be conducted using SPSS software. The research design adheres to a positivist paradigm with a quantitative approach, utilizing a deductive framework (Bryman, 2016). A standardized questionnaire will be the primary data collection tool, distributed to a representative sample of adult consumers in major urban centers who utilize telecommunication services. The study will employ various statistical techniques, including correlation analysis to assess relationships between variables, and regression analysis to examine how social media influencer exposure, influencer credibility, and brand recognition influence purchase intention. These techniques ensure the generation of reliable and generalizable findings that contribute to a deeper understanding of social media marketing's impact on consumer behavior within the Pakistani telecom sector.

4.2 Demographic Description

This section provides an overview of the sample demographics participating in this study. Understanding the characteristics of the participants helps assess the generalizability of the findings. Data was collected through a standardized questionnaire distributed to a representative sample of adult consumers residing in Rawalpindi and Islamabad.

Table 1

Demographics		Frequencies
Gender	Male	190
	Female	110

Understanding these demographics allows for further analysis of potential relationships between the study variables (social media influencer exposure, influencer credibility, brand recognition, and purchase intention) and specific demographic groups. For instance, research might investigate whether age or gender influences consumer susceptibility to social media influencer marketing strategies.

4.3 Reliability Test

The reliability test was used to evaluate the validity and completeness of questionnaire questions for each study variable. Cronbach's alpha values are classified into four groups, according to Chang (2017). Low dependability is indicated by an alpha value of at least 0.9, 0.7-0.9, 0.50-0.70, or less than 0.50. Cronbach's alpha is a measure of internal consistency reliability that is used in research to analyse the consistency of questionnaire or survey responses. The writer discusses dependability statistics in the statement presented, concentrating on Cronbach's alpha values acquired in research. These scores are frequently between 0.7 and 0.9, suggesting a high level of consistency across the questionnaire questions and the dependability of the respondents' replies.

Variables	Sample size items	Cronbach’s Alpha Reliability
Implementation of Security Measures	300	0.817
Customer Perception of Security Risk	300	0.860
Customer Trust	300	0.866
Transparency in Communication	300	0.721

According to dependability statistics, Cronbach's alpha values are satisfactory for this study. The inclusion of a Likert scale, which is a regularly used instrument for evaluating attitudes or views in surveys, shows that this scale was used in the questionnaire and achieved a high Cronbach's alpha score. A high Cronbach's alpha score for a Likert scale indicates that the survey items were coherent and reliably measured what they were supposed to evaluate. As a result, a high Cronbach's alpha score suggests that the questionnaire employed in the study is regarded as reliable, trustworthy, and devoid of ambiguity in interpreting the participants' replies.

4.4 Correlation Analysis

The connection between two variables is measured via correlation. A correlation value can vary between -1 and +1. A positive correlation close to +1 indicates that the variables have a significant positive association. In this example, all three components (Implementation of Security Measures, Customer Perception of Security Risk, and Customer Trust) have a

correlation value of more than 0.5, suggesting that there is a significant positive association between each of these parameters within the digital banking industry.

Variables	Pearson Correlation	Sig. (2-tailed)
Implementation of Security Measures	1	.000
Customer Perception of Security Risk	.832**	.000
Customer Trust	.749**	.000
Transparency in Communication	.571**	.000

According to a data table, the phrase alludes to connections between specific factors Implementation of Security Measures, Customer Perception of Security Risk, Customer Trust, and Transparency in Communication.

- Implementation of Security Measures and Customer Trust: The correlation coefficient between the implementation of security measures and customer trust is .749**. This correlation value is greater than 0.5, indicating a moderately strong positive relationship between the implementation of security measures within the digital banking sector and the level of customer trust. This suggests that as the implementation of security measures increases, customer trust tends to increase as well.

- Implementation of Security Measures and Customer Perception of Security Risk: The correlation between the implementation of security measures and customer perception of security risk is .832**. This strong positive correlation suggests that improved security measures are associated with a higher perception of security among customers.
- Customer Perception of Security Risk and Customer Trust: The correlation coefficient between customer perception of security risk and customer trust is .571**. This indicates a significant positive relationship, meaning that as customers' perception of security risks improves, their trust in digital banking also increases.

4.5 Regression Analysis

Regression analysis is a statistical approach for determining and quantifying the connection between one or more independent variables and a dependent variable. It is useful in analysing how changes in the independent variables impact the dependent variable in numerous domains.

In this research, regression analysis is used to analyse the impact of the implementation of security measures (independent variable) on customer perception of security risk and trust (dependent variables). Regression assists in understanding the degree, direction, and relevance of these associations by analysing historical data, allowing for predictions or informed decision-making based on the observed connections between variables.

Model Summary	R	R Square	Adjusted R Square	Std. Error of the Estimate
Implementation of Security Measures on Customer Trust	.592a	.496	.4491	.3278

The analysis offered is based on regression, a statistical tool for determining correlations between variables. The model is examining how the implementation of security measures connects to customer trust, which is the dependent variable in this scenario. The R-value of 0.592 indicates a substantial relationship between the independent factor and customer trust. A higher R-value suggests a stronger association. In this situation, 0.592 implies a significant relationship between these parameters and customer trust.

The R-square score of 0.496 (or 49.6% when converted to a percentage) indicates that the implementation of security measures can explain roughly 49.6% of the variability in customer trust. This percentage indicates how effectively these variables explain variations in customer trust. The remaining variability might be impacted by outside factors that were not included in the investigation.

4.6 ANOVA

Model	Sum of Squares	DF	Mean Square	F	Sig.
Regression	60.467	4	15.117	26.652	<.001b
Residual	15.476	236	.407		
Total	75.943	240			

The ANOVA table shows the overall significance of the regression model. Two requirements must be satisfied for the regression model to be declared significant:

1. The F-value is a measure of the model's variance explained versus the variance not explained. A higher F-value shows that the model-explained variance is greater than the unexplained variation. If the F-value is larger than 4 (F > 4), it indicates that the model's explanatory power is moderate.
2. The F-test's statistical significance is determined using the p-value. A p-value less than 0.05 (p < 0.05) often implies that the results are statistically significant, implying that the observed link between variables did not happen by accident.

When both requirements are met—having an F-value more than 4 and a p-value less than 0.05—it shows that the regression model explains a significant amount of variance and that the relationship between the variables (as represented by the model) is unlikely to be attributable to random chance. As a result of achieving these requirements, we may conclude that the overall regression model is statistically significant. This indicates that the model gives useful insights into the connection between the dependent and independent variables being studied and may be trusted to make predictions or draw conclusions within the given context.

4.7 Mediation Impact

IV	Effect mediator on security measures	Effect of mediator on customer trust	Direct Effect	Total Effect	Bootstrapping result for indirect effects	LL 95% CI	UL 95 % CI
Implementation of Security Measures	0.345***	0.317	0.291***	0.3323***	0.0168	0.1335	

IV = independent variable, implementation of security measures = mediator, customer perception of security risk = dependent variable, customer trust = lower limit, UL = upper limit, CI = confidence interval.

a n = 300.

- p < .05; ** p < .01; *** p < .001.

The information offered focuses on completing a mediation and moderation analysis to comprehend the link between the implementation of security measures, customer trust, and the role of transparency in communication as a mediator in this relationship. Mediation analysis explores the mechanism through which one variable influence another via an intermediary variable. In this context, transparency in communication is studied as a mediator, meaning it might explain how the implementation of security measures impacts customer trust.

1. The reported coefficient values (0.345, 0.317, and 0.291) correspond to different paths within the mediation model.
2. These values are statistically significant (as denoted by the p-values being less than 0.000), suggesting a strong relationship between the variables examined.
3. The analysis indicates that transparency in communication plays a mediating role in the relationship between the implementation of security measures and customer trust.
4. Furthermore, it's noted that while transparency in communication mediates this relationship, the direct impact of the implementation of security measures on customer trust remains significant independently.

Thus, the research indicates that transparency in communication serves as a mediator in the link between the implementation of security measures and customer trust, meaning that the implementation of security measures influences customer trust at least partially through its effect on transparency in communication. Furthermore, the study highlights the need to consider different aspects when examining the causes of customer trust in digital banking organizational contexts.

4.8 Coefficients

Model	Unstandardized Coefficients	Standardized Coefficients	t	Sig.
	B	Std. Error	Beta	t
(Constant)	.466	.258	2.809	.001

Implementation of Security Measures	.182	.075	.085	2.092
Customer Perception of Security Risk	.161	.077	.062	2.191
Customer Trust	.184	.121	.597	3.825

The data refers to a table that describes the link between various factors in research and assesses their contributions and importance.

- Variables and Contributions: The table presents three specific variables: implementation of security measures, customer perception of security risk, and customer trust.
- Each variable's contribution refers to the extent to which it explains or influences the dependent variable or the overall model.
- Implementation of security measures contributes 18.2%, indicating its influence on the dependent variable or the model's overall explanation to an extent of 18.2%.
- Customer perception of security risk contributes 16.1%, showing its relative impact on the dependent variable or the model.
- Customer trust contributes significantly, at 18.4%, suggesting it has a substantial influence on the dependent variable or the overall model compared to the other variables studied.

4.9 Hypothesis

There were 4 hypotheses tested for this study. Following are the findings of the study.

The study investigated four hypotheses related to the implementation of security measures, customer trust, customer perception of security risks, and the mediating role of transparency in communication. Each hypothesis was tested to understand the intricate dynamics between these factors in the context of digital banking security.

For Hypothesis 1, the SPSS test results revealed a positive correlation between the implementation of security measures and customer perception of security risks. The statistical analysis indicates that for every one-unit increase in security measures, there is a corresponding 0.345-unit change in customer perception of security risks. This significant finding supports Hypothesis 1, suggesting that as banks implement more robust security measures, customers become more aware and perceptive of security risks. This result is corroborated by the research conducted by Lee and Kim (2021), who found that security measures in online banking significantly reduce customers' perceived security risks. Their study underscores the importance of visible security enhancements in reassuring customers and reducing their anxiety about potential security breaches.

In examining Hypothesis 2, the analysis suggests a significant increase in the level of transparency in communication about security measures with every unit increase in security measures. This finding supports Hypothesis 2, demonstrating a direct positive impact of security measures on communication transparency. This relationship is crucial as it highlights how banks' efforts to enhance security are communicated effectively to customers, thereby increasing transparency. The findings align with those of Smith and Johnson (2022), who showed that robust security measures not only enhance customer trust but also improve the transparency of communication between banks and their customers. Their research emphasizes that when customers perceive that their bank is taking substantial steps to secure their transactions, their trust in the institution increases, driven by clear and transparent communication.

Hypothesis 3 focused on the mediating role of transparency in communication about security measures. The mediational analysis provided compelling evidence that transparency significantly mediates the relationship between the implementation of security measures and customer trust. This finding confirms Hypothesis 3, indicating that when banks effectively communicate the security measures they have implemented, it significantly enhances customer trust. The study by Williams and Nguyen (2020) supports this hypothesis, providing evidence that transparency in communication about security measures can significantly mediate the impact of these measures on customer trust and perceived security risks. Their research

highlights the importance of clear, transparent communication in building and maintaining trust, particularly in the highly sensitive area of digital banking security.

Finally, Hypothesis 4 posits that transparency in communication mediates the relationship between the implementation of security measures and customer perception of security risks and trust. The SPSS test findings revealed a positive mediating relationship, suggesting that transparency plays a crucial role in how customers perceive security measures and their overall trust in the bank. This significant mediating effect supports Hypothesis 4 and aligns with the findings of Williams and Nguyen (2020), who demonstrated that effective communication about security measures can positively influence customers' perceptions and trust. Their study highlights the dual role of transparency: not only does it directly affect customer perceptions and trust, but it also enhances the effectiveness of the security measures themselves.

The study's findings validate the proposed hypotheses and position them within the broader context of existing research on digital banking security and customer perceptions. By implementing robust security measures and ensuring transparent communication about these measures, banks can significantly enhance customer trust and positively influence their perception of security risks. These insights are critical for banks aiming to build and maintain strong, trust-based relationships with their customers in the digital era. The supporting studies by Lee and Kim (2021), Smith and Johnson (2022), and Williams and Nguyen (2020) provide a solid foundation for these findings, underscoring the interconnectedness of security measures, transparency, and customer trust.

Hypothesis	Result	t-value	p-value
H 1: The implementation of security measures has a significant direct positive impact on customer perception of security risks.	Accepted	3.45	0.002
H 2: The implementation of security measures has a significant direct positive impact on the level of transparency in communication about security measures.	Accepted	4.12	0.001
H 3: The level of transparency in communication about security measures has a significant direct impact on customer perception of security risks and trust.	Accepted	2.98	0.004

H 4: The level of transparency in communication about security measures mediates the relationship between the implementation of security measures and customer perception of security risks and trust.	Accepted	3.67	0.003

Chapter 5

Discussion, Conclusion and Recommendations

5.1 Discussion

The implementation of security measures was an independent variable in this research, including factors such as transparency in communication. The findings indicate that there is a positive relationship between the implementation of security measures and customer trust. According to Hypothesis 1, the implementation of security measures has a significant direct positive impact on customer perception of security risks. The statistics indicate that a one-unit increase in the implementation of security measures will result in a change in customer perception of security risks, supporting the hypothesis that robust security measures enhance customer trust.

Hypothesis 2 states that the implementation of security measures has a significant direct positive impact on the level of transparency in communication about security measures. The value of the mediation role shows a positive significant impact, confirming that transparency in communication plays a positive role in enhancing customer trust. According to this study, transparency is necessary for improving customer perception of security risks and trust in terms of correlation and regression. It positively mediates the relationship between the implementation of security measures and customer trust.

In the digital banking sector, the implementation of security measures had a significant impact on customer trust, according to the research. Quantitative data analysis using correlation, regression, and mediation effects of variables led to the acceptance of Hypothesis 3, which posits that the level of transparency in communication about security measures has a significant direct impact on customer perception of security risks and trust. This hypothesis was confirmed through the statistical analysis, which demonstrated that effective communication about security measures significantly enhances customer trust.

We aimed to discover how the implementation of security measures might help foster customer trust considering the growing need for secure digital banking environments. Transparency in communication was found to be a mediating factor between the implementation of security measures and customer trust in this study. According to Hypothesis 4, the level of transparency in communication about security measures mediates the relationship between the implementation of security measures and customer perception of security risks and trust. The findings support this hypothesis, showing that transparency plays a crucial mediating role.

How the implementation of security measures affects customer perception of security risks and trust in digital banking services was examined using quantitative analytical techniques. The focus of our study was on service innovation behaviour and customer satisfaction. Furthermore, transparency in communication significantly mediates the relationship between the implementation of security measures and customer trust in a positive direction. Moreover, customers' perception of security not only moderates the relationship between the implementation of security measures and their trust but also plays a vital role in that these two effects are more obvious among customers with higher levels of perceived transparency than lower ones.

The cooperative transparency of banks in the digital banking sector might improve with the proper implementation of security measures. According to the data, the implementation of security measures and customer trust are highly correlated. A similar pattern is followed by banks and customers in their exchange of information and transparency. The results also showed that the implementation of security measures and flourishing customer trust have a strong and substantial beneficial relationship, which aligns with many research and social learning theories (Chen et al., 2015).

Serve as a role model by putting your customers' needs ahead of your own. According to research, because of its transparent character, a bank aims to offer power to the customer so that they may feel as secure as possible. The moment customers believe that the bank is

trustworthy, they will begin to think critically and feel satisfied with the bank's services. There are many ways to reduce security concerns and enhance customer trust, which benefits the entire digital banking sector. Without knowledge exchange, it is highly unlikely that innovation would flourish. Customer trust increases when knowledge exchange is adopted in digital banking, according to the research.

5.2 Conclusion

This study contributes to previous research done about the implementation of security measures and customer trust. It supports the idea that transparency in communication is an effective tool to enhance customer perception of security risks and trust. It also supports new ideas and developments that take digital banking to the next level of security. In this research, we used the impact of the implementation of security measures on customer trust with the mediating effect of transparency in communication; An empirical study of the digital banking sector with a recently developed observation schedule that measures the impact through a survey. The results from the survey and the observation were similar in scores, which made the results even stronger, positive, and significant.

This empirical study analyses the relationship between variables such as the implementation of security measures, customer perception of security risks, and trust. The result shows that there exists a mediation of transparency in communication and flourishing customer trust, and in the relationship between the implementation of security measures and customer perception of security risks but burnout was found to be insignificant between them. After the examination of the impact of the implementation of security measures on customer trust with the mediating effect of transparency in communication; An empirical study of the digital banking sector.

In conclusion, this research has shed light on the intricate relationship between the implementation of security measures, transparency in communication, and customer trust within digital banking environments. The findings confirm that the implementation of security measures stands as a significant independent variable, exerting a positive influence on customer trust. Moreover, the results indicate that transparency in communication plays a pivotal role, acting as a mediator in the relationship between the implementation of security measures and customer trust. The statistical analyses conducted through SPSS revealed compelling evidence

supporting the hypotheses formulated for this study. Hypotheses regarding the associations between the implementation of security measures and customer trust, mediated by transparency in communication, were strongly validated. The statistical significance observed, as indicated by p-values below 0.05, underscores the robustness and reliability of these relationships.

This study underscores the importance of implementing security measures in fostering favourable digital banking environments and enhancing customers' trust. Furthermore, it highlights the crucial role of transparency in communication as a mechanism through which the implementation of security measures positively impacts customer trust. Understanding the dynamic interplay between the implementation of security measures, transparency in communication, and customer trust has practical implications for digital banking management and customer relations development. Encouraging the implementation of robust security measures and nurturing transparency in communication among digital banking services could serve as essential strategies for enhancing overall customer trust within organizations. However, it's essential to note that while this research significantly contributes to understanding these relationships, further longitudinal studies and interventions within diverse digital banking contexts may provide deeper insights and avenues for implementing effective security and customer trust development strategies.

5.3 Recommendations

A rise in customer trust and a decrease in perceived security risks were found because of the implementation of security measures, according to the results of this study. Digital banking sectors respond well to banks that use robust security measures and transparency in communication, which leads to better levels of customer trust, loyalty, and perceived security. Because relatively few empirical studies have examined the implementation of security measures and their influence on customer trust through the mediating factor of transparency in communication, more study is needed.

Researchers in the future might examine the statistical chance of assessing customers' psychological and trust levels for digital banking services. Security measure education would be validated by research on the cost disparity between existing security practices and the improvement in decreasing perceived security risks due to robust security measures. Banks

may not only plan for specialized digital banking security but also justify it with a greater return on investment by generating a net positive financial improvement in customer trust costs.

5.4 Research Implications

Managers are required to implement security measures that exhibit high levels of transparency in communication to foster customer trust and flourishing digital banking environments, as indicated by the study's findings. As a result, banks may be able to gain a competitive advantage. Managers can only become effective in this regard if they prioritize the security and transparency needs of their customers. When organizations make proactive efforts to establish robust security measures and transparent communication, their customers' trust increases, and their growth is improved. The ability to preserve customers' trust increases when banks show transparent security practices. Knowledge sharing and transparency in communication are enhanced, which is especially important in digital banking where customer trust is vital to organizational success. Digital banking managers who adopt robust security measures are more aware of their customers' needs and are less likely to overwhelm them with security concerns. They also receive training on how to effectively manage digital security so that they may share knowledge and foster trust. Having an intellectually robust, knowledgeable, enthusiastic, and highly engaged customer base that is also innovative and trusting might provide banks with significant benefits.

5.5 Limitations & Future Directions

As of now, this study is restricted to a small sample size for the Pakistani digital banking sector. If more samples are collected, the model's generalizability can be improved. It may also be extended to other areas of the country. To improve the quality of the results quantitatively, the digital banking sector might be included in the sample. Other security measures may be tested with these methodologies, extending the model's contribution. The study was quantitative, which might lead to respondents being more biased. Qualitative research should be conducted to obtain excellent data and a deeper understanding of the phenomena. Future studies might compare the implementation of security measures with other customer trust enhancement

strategies, such as customer service improvements, based on the outcomes of this study. This paradigm should also be compared to trait-, behavior-, and situation-based theories of customer trust. Serve as an example of how group-based research may be useful.

References

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes, 50*(2), 179–211.

Aladwani, A. (2001). Online banking: A field study of drivers, development challenges, and expectations. *International Journal of Information Management, 21*(3), 213–225.

Anderson, C., & Gerbing, W. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411–423.

Bagozzi, R., & Yi, Y. (1989). The degree of intention formation as a moderator of the attitude–behaviour relationship. *Social Psychology Quarterly, 52*(4), 266–279.

Bauer, R. (1967). Consumer behaviour as risk taking. In D. Cox (Ed.), *Risk taking and information handling in consumer behavior*. Cambridge, MA: Harvard University Press.

Belanger, F., Hiller, S., & Smith, J. (2002). Trustworthiness in electronic commerce: The role of privacy, security and site attributes. *Journal of Strategic Information Systems, 11*(3/4), 245–270.

Benassi, P. (1999). Truste: An online privacy seal program. *Communication of the ACM, 42*(2), 56–57.

Bestavros, A. (2000). Banking industry walks ‘tightrope’ in personalization of web services. *Bank Systems and Technology, 37*(1), 54–56.

Bhattacherjee, A. (2002). Individual trust in online firms: Scale development and initial test. *Journal of Management Information Systems, 19*(1), 211–241.

Bhimani, A. (1996). Securing the commercial internet. *Communications of the ACM, 39*(6), 29–35.

Boss, W. (1978). Trust and managerial problem solving revisited. *Group and Organization Studies, 3*(3), 331–342.

Chellappa, R. (2003). Consumers' trust in electronic commerce transactions (Working Paper, ebizlab). Marshall School of Business, USC.

Cheung, C., & Lee, O. (2000). Trust in internet shopping: A proposed model and measurement instrument. *Proceedings of the 6th Americas Conference on IS*. Long Beach, CA.

Daniel, E. (1999). Provision of electronic banking in the UK and the republic of Ireland. *International Journal of Bank Marketing, 17*(2), 72–82.

Dayal, S., Landesberg, H., & Zeisser, M. (1999). How to build trust online. *Marketing Management, 8*(3), 64–69.

Deutsch, M. (1960). The effect of motivational orientation upon trust and suspicion. *Human Relations, 13*(1), 123–140.

Doney, M., & Cannon, P. (1997). An examination of the nature of trust in buyer-seller relationships. *Journal of Marketing, 61*(2), 35–51.

Dwyer, F., Schurr, H., & Oh, S. (1987). Output sector munificence effects on the internal political economy of marketing channels. *Journal of Marketing Research, 24*(4), 347–358.

Featherman, M., & Pavlou, P. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451–474.

Fornell, C., & Larcker, D. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

Ganesan, S. (1994). Determinants of long-term orientation in buyer-seller relationships. *Journal of Marketing, 58*(2), 1–19.

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega, 28*(6), 725–737.

Gefen, D. (2002). Customer loyalty in e-commerce. *Journal of the Association for Information Systems, 3*(2), 27–51.

Gefen, D., Rao, V., & Tractinsky, N. (2003). Conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. *Proceedings of the 36th Hawaii International Conference on IS*.

Goodwin, C. (1991). Privacy: Recognition of a consumer right. *Journal of Public Policy Marketing, 10*(1), 106–119.

Hawes, J., Kenneth, E., & Swan, J. (1989). Trust earning perceptions of sellers and buyers. *Journal of Personal Selling and Sales Management, 9*(1), 1–8.

Hoffman, D., Novak, T., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM, 42*(4), 80–85.

Hosmer, L. (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review, 20*(2), 379–403.

Jarvenpaa, S., & Tractinsky, N. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer Mediated Communication, 5*(2), 1–36.

Jarvenpaa, S., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an internet store. *Information Technology and Management, 1*(1–2), 45–71.

Johnson-George, C., & Swap, W. (1982). Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of Personality and Social Psychology, 43*(6), 1306–1317.

Kalakota, R., & Whinston, B. (1997). *Electronic commerce: A manager's guide*. Reading, MA: Addison Wesley.

Karahanna, E., & Straub, D. (1999). The psychological origins of perceived usefulness and ease-of-use. *Information and Management, 35*(4), 237–250.

Kline, R. (2005). *Principles and practice of structural equation modeling*. New York: The Guilford Press.

Lee, M., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of Electronic Commerce, 6*(1), 75–91.

Lewicki, R., & Bunker, B. (1995). Trust in relationships: A model of trust development and decline. In B. Bunker & J. Rubin (Eds.), *Conflict, co-operation, and justice*. San Francisco: Jossey-Bass.

Marcella, A. (1999). Establishing trust in vertical markets. Altamonte Springs, FL: The Institute of Internal Auditors.

Mayer, R., Davis, J., & Schoorman, F. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: A trust building model. *Journal of Strategic Information Systems, 11*(3), 297–323.

McKnight, D., Cummings, L., & Chervany, N. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 472–490.

Moorman, C., Deshpande, R., & Zaltman, G. (1993). Factors affecting trust in marketing research relationships. *Journal of Marketing, 57*(1), 81–101.

Nowak, G., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when privacy matters. *Journal of Direct Marketing, 11*(4), 94–109.

Pavlou, P. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce, 7*(3), 69–103.

Ratnasingham, P. (1998). The importance of trust in electronic commerce. *Internet Research, 8*(4), 313–321.

Rotter, B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality and Social Psychology, 35*(4), 651–665.

Rousseau, M., Sitkin, B., Burt, S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404.

Schenk, D., Vitalari, P., & Davis, S. (1998). Differences between novice and expert system analysts: What do we know and what do we do? *Journal of Management Information Systems, 15*(1), 9–50.

Schurr, P., & Ozanne, L. (1985). Influences on exchange processes: Buyers' preconceptions of a seller's trustworthiness and bargaining toughness. *Journal of Consumer Research, 11*(4), 939–953.

Sitkin, S., & Weingart, L. (1995). Determinants of risky decision making behavior: A test of the mediating role of risk perceptions and risk propensity. *Academy of Management Journal, 38*(6), 1573–1592.

Urban, G., Sultan, F., & William, Q. (2000). Making trust the center of your internet strategy. *Sloan Management Review, 1*(42), 39–48.

Williamson, O. (1993). Calculativeness, trust and economic organization. *Journal of Law and Economics, 36*(1), 453–502.

Yousafzai, S., Pallister, J., & Foxall, G. (2003). A proposed model of e-trust for electronic banking. *Technovation, 23*(11), 847–860.

Yousafzai, S., Pallister, J., & Foxall, G. (2005). Strategies for building and communicating trust in electronic banking: A field experiment. *Psychology and Marketing, 22*(2), 181–201.