





Article

Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers

Faraz Ahmed ¹, Arsalan Hussain ¹, Sajjad Nawaz Khan ², Arsalan Haneef Malik ^{1,*}, Muhammad Asim ³,
Sadique Ahmad ³ and Mohammed El-Affendi ³

¹ College of Business Management, Institute of Business Management, Karachi 75300, Pakistan; std_31408@iobm.edu.pk (F.A.); arsalan.hussain@iobm.edu.pk (A.H.)

² Department of Business Administration, Iqra University, Main Campus, Karachi 75500, Pakistan; sajjadnawazkhan@gmail.com

³ EIAS Data Science Lab, CCIS, Prince Sultan University, Riyadh 11586, Saudi Arabia; masim@psu.edu.sa (M.A.); ahmad01.shah@ieee.org (S.A.); affendi@psu.edu.sa (M.E.-A.)

* Correspondence: arsalan.haneef@live.com

Abstract: The digital economy's rise has fueled the growth of digital banking, but concerns linger about customer protection. While offering advantages like financial inclusion, this shift disrupts traditional banking experiences and introduces potential risks. Customer safety in this new landscape is paramount, as dissatisfied users may switch providers and institutions risk reputational damage. To remain competitive, financial institutions must prioritize a secure experience that aligns with customer expectations. This study investigates five key factors influencing customer protection in Pakistan's digital financial services. Analysis reveals all factors positively impact customer protection, with information security holding the most weight. These findings highlight the need for robust information security measures as a critical driver for the Pakistani digital banking industry's success.

Keywords: digital risk; financial inclusion; customer protection; risk management; digital banking



Citation: Ahmed, Faraz, Arsalan Hussain, Sajjad Nawaz Khan, Arsalan Haneef Malik, Muhammad Asim, Sadique Ahmad, and Mohammed El-Affendi. 2024. Digital Risk and Financial Inclusion: Balance between Auxiliary Innovation and Protecting Digital Banking Customers. *Risks* 12: 133. <https://doi.org/10.3390/risks12080133>

Academic Editors: Salvador Cruz Rambaud and Angelos Dassios

Received: 18 April 2024

Revised: 17 July 2024

Accepted: 13 August 2024

Published: 22 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

During the last two decades, financial inclusion (FI) has appeared as a cornerstone strategy for poverty alleviation and economic development (Ozili 2020). This focus on FI is driven by various factors, including technological advancements, government initiatives, and private-sector innovation. Growing evidence suggests that FI, when combined with technological advancements, effectively reduces poverty and stimulates economic growth (Diener and Špaček 2021). The primary goal of FI is to enhance access to financial products and services such as savings and checking accounts, insurance, loans, and investment opportunities. By providing people with greater economic opportunities and financial security, FI helps to alleviate poverty and promote fuller participation in the economy (Mhlanga 2021). Recognizing its potential, FI has become a priority for governments, international organizations, and development institutions aiming to foster economic growth and reduce inequality (Ozili 2018).

In this regard, numerous steps have been taken by policymakers to enhance FI. In this new age of technology, the implementation of digital financial services, including mobile banking and digital wallets, has been instrumental in increasing access to financial services, particularly in underdeveloped areas (Naumenkova et al. 2019). Additionally, governments have initiated financial literacy programs to educate people on utilizing financial services and making informed financial decisions. Furthermore, private-sector financial institutions play a significant role in improving access to credit through initiatives like microfinance and low-interest loans, enabling low-income individuals and small businesses to secure the funds necessary for growth (Ozili 2018).

Researchers suggest that integrating technology can significantly boost FI. Existing studies demonstrate the significant impact of technological advancements on FI. The availability of mobile phones, the Internet, and other advanced gadgets has facilitated easier access to financial services, even in remote and underserved areas, leading to a reduction in financial exclusion (Broby 2021). Digital technologies have also driven the digital transformation of the banking industry, prompting changes in its services and products. This transformation has shifted traditional processes towards more streamlined digital systems, thereby reshaping the banking sector (Diener and Špaček 2021).

In line with the objective of digital transformation and the promotion of financial inclusion (FI) (Noreen et al. 2023), authorities are embracing the entry of digital banks as a much-needed catalyst for competition and innovation within the banking industry. The widespread adoption of digital banking worldwide has been greatly influenced by digital technologies, which have empowered these banks to introduce new and innovative services for their customers. To facilitate the growth of digital banking, several authorities have established specific licensing regimes (Choi 2020). Digital banks are emerging as a welcome infusion of competition and innovation within the banking industry, leveraging digital technologies to provide novel services to customers. Operating as deposit-taking financial institutions, digital banks employ a digital-first or digital-only business model to deliver their goods and services. Offering faster, more convenient, and often more cost-effective services than traditional banks, digital banks bridge the gap between the financially privileged and the underserved, granting equal access to financial opportunities and bolstering economic growth through increased financial inclusion (Naumenkova et al. 2019). Financial inclusion is a key driver of economic growth, with digital banks leading the charge to make it a reality (Diener and Špaček 2021).

Moreover, digital banks frequently enjoy lower operating costs compared to their traditional counterparts, enabling them to provide more competitive products and services, such as higher interest rates on savings accounts or lower fees. In essence, digital banks offer enhanced accessibility, convenience, and cost-effectiveness, rendering them increasingly crucial in the financial sector (Shin et al. 2020).

The existing literature on FI and digital financial services has mostly focused on the positive side of technological advancement in the financial industry; however, the other side of the coin tells a different story, where the advent of new financial technologies, when inadequately regulated, may also hurt customers by increasing the financial risk (Moloi and Iredele 2020). FI through digital banking has the potential to empower millions of unbanked individuals, but it also poses significant risk management challenges.

Although digital technology has made remarkable progress in providing financial services, specifically in developing countries, some scholars, such as Njoroge (2016), Kikulwe et al. (2014), and Mugambi et al. (2014), believe that digital customer protection remains a significant concern. Villasenor et al. (2015) have noted that the lack of transparency and instances of fraud involving mobile money operators as well as telecom companies have deterred some individuals from participating in the mobile money sector and using digital financial services. Additionally, the absence of interoperability among different digital payment platforms has raised concerns regarding the privacy and security of confidential information shared across fragmented versions of digital payment platforms (Mazer and McKee 2017). Furthermore, the use of key technologies, such as short message service (SMS) and unstructured supplementary service data (USSD), on mobile phones has known security vulnerabilities that could be exploited to intercept digital banking transactions.

The World Bank (2012) has also suggested that protecting consumers' data while using digital financial services and providing users with adequate information and recourse mechanisms to resolve disputes are crucial for customer protection. The Alliance for Financial Inclusion (Alliance for Financial Inclusion (AFI) 2014) has similarly emphasized the importance of safeguarding consumers from transaction risk and ensuring that they understand mobile money and digital financial products, which could enhance their trust and confidence in digital financial systems, leading to higher adoption and usage (Budiyono and Sukamulja 2023).

The impact of digital banks on customer protection is complex, with both positive and negative elements. Digital banks offer increased convenience and reduce physical interactions, but they may have limitations in protecting customers from the various types of risks associated with digital banks (Choi 2020). Factors associated with digital banks can put customers at risk and erode trust in digital banking services. It is important for digital banks to address challenges and prioritize customer protection to build trust and promote the adoption of digital banking. As digital banks expand FI by reeling in previously unbanked individuals and businesses, the following question arises: what measures are in place to ensure that the risks are managed effectively? Therefore, there is a need to understand the intensity of the risk factors that are associated with digital banks.

Despite overwhelming research work on digital financial services and FI, clarity is required on the impact of digital banks on customer protection (Naumenkova et al. 2019). One aspect that needs to be taken care of is customer protection. Digital banks are expanding access to financial services, but with this opportunity comes the need for effective risk management to protect both customers and institutions (Chen et al. 2021).

To the best of our knowledge, there are fewer studies focusing on this negative consequence of technological advancements in the finance industry and the inclusiveness of digital financial services. Our study aims to add to this strand of literature and examine the impact of digital banks on customer protection. Furthermore, this study explains the intensity of risk indicators that influence customer protection while using digital financial services. It aims to provide a more complete picture on the impact of digital finance advancements on customer protection. Our study is motivated by the need to promote prudent FI and to regulate digital financial markets. Despite the growing importance of digital financial service security in Pakistan, there is a lack of research on the specific digital risk factors that impact customer protection. To address this gap, this study proposes a framework that outlines five risk factors that can influence customer protection in Pakistan digital bank platforms. The factors identified include authentication mechanisms, data privacy details, encryption mechanisms, information provided, and responsiveness. The model was developed based on a comprehensive review of previous research on related areas (Muhtasim et al. 2022).

This study presents a new perspective on the factors that affect customer protection in the digital banking industry in Pakistan, particularly focusing on digital risk factors. The findings of this study could be valuable for digital bank policymakers, as they shed light on the key risk factors that need to be improved to enhance platform security and encourage greater consumer adoption. In this study, we seek answers to the questions about the intensity of risk factors affecting customer protection while carrying out transactions with digital banks. This study aims to fill the gap in the literature on the understanding of various types of risks associated with digital banks and intensity of these risks on customer protection. The study adds to the literature on customer protection in the context of the evolution of digital banks by taking a practice view of the situation of digital financial services in Pakistan. Our findings have practical implications for risk managers, banking practitioners, digital banking customers, and policymakers. This study applies structural equation modeling (SEM) by using SmartPLS for data analysis.

2. Literature Review

2.1. Financial Inclusion (FI)

FI gained significant attention in the 1970s, when the World Bank began promoting access to financial services as a means to reduce poverty. In 1997, the United Nations established the Microfinance Summit, which aimed to expand access to financial services to low-income populations. In the early 2000s, FI became a key topic of discussion among policymakers and international organizations, as it was recognized as a crucial tool for economic development and poverty reduction. In 2005, the G8 leaders established the Global Partnership for FI, which aimed to promote FI in developing countries (Ozili 2020).

Similarly, in 2005, UNCDF also made a strategic shift to focus its interventions on FI more broadly. The new approach was supporting a market development approach to make

financial sectors more inclusive. It was designed to create enabling environments for a wide range of retail financial service providers and to address gaps in the policy, legal, and regulatory constraints that prevent a financial sector from being inclusive.

The United Nations Development Programme defines FI as the provision of various formal financial services to customers, ranging from basic credit and savings services to more advanced services, such as insurance and pensions (Wang'oo 2013). The definition by Leeladhar (2006) speaks of FI as the process where banking services are delivered in a manner that they become affordable to many sections of disadvantaged groups, especially low-income earners. Thorat (2008) also came up with a definition of FI where FI is defined as how financial services are provided at an affordable rate by formal financial institutions to disadvantaged groups. Another definition of FI was provided by Sarma (2008), where FI was defined as the art of making sure that there is ease of access, availability, and usage of formal financial services to all the people in an economy. Arun and Kamath (2015) also highlighted that FI should be viewed as a situation where people have access to financial services and products of good quality that are affordable and convenient with dignity for all clients. According to a United Nations Report, FI is the sustainable provision of affordable financial services that bring the poor into the formal economy (Ozili 2020).

2.2. Technological Advancements in the Financial Sector

In recent years, technological advancements have played a significant role in promoting FI. Mobile banking, digital wallets, digital banks, and other fintech innovations have made it easier and more affordable to access financial services, particularly for those living in remote or underserved areas. Overall, the history of FI shows a gradual recognition of the importance of providing access to financial services to all individuals, regardless of their income level or location. There is another school of thought that believes that financial innovation and technology can increase financial inclusion because they can bypass existing structural and infrastructural problems in order to reach the poor, thus contributing to the realization of the Sustainable Development Goals (Saqib et al. 2023). Financial innovation and technology have the potential to increase FI by overcoming some of the structural and infrastructural problems that have historically excluded the poor from accessing financial services (Al-Mudimigh and Anshari 2020). Financial innovation is the process of creating new financial instruments, technologies, products, and services to improve the delivery of financial services.

In a study, Ouma et al. (2017) showed that financial innovations and technological advancements, like the availability and usage of mobile phones, were used to offer financial services that promote savings at the household level and improved amounts saved, while Kwenda and Chinoda (2019) showed that mobile phone innovation improved FI in 49 countries. In Southeast Asia, Al-Mudimigh and Anshari (2020) observed that the region had many Internet users and high number of fintech companies, which helped to improve the level of FI, especially for the unbanked population.

Since this study is focusing on the enhancement of financial services via digital financial services, it adopts the school of thought that believes that financial innovation and technological advancement can increase FI. In line with focusing on technological advancements and promoting FI, authorities are also welcoming digital banks. Over the past decade, the world has seen a rise in digital banks. Digital banks have been on the rise as digital technologies transform financial services around the world. Another objective of setting up digital banks is to provide credit access to unserved and underserved population. Furthermore, digital banks also provide affordable/cost-effective digital financial services. As part of the government's objective to set up digital banks, they aim to encourage the application of financial technology and innovation in the banking sector, foster new sets of customer experiences, and develop digital eco-systems.

Technology advancements in the financial industry have largely been discussed from a positive perspective in the literature on FI and digital financial services. In contrast, the introduction of new financial technologies can also lead to an increase in financial risk for

customers when inadequately regulated (Moloi and Iredele 2020). Millions of unbanked people can be empowered through FI through digital banking, but there are also significant risks associated with it.

2.3. Digital Banks

Globally, digital banks now number more than 100 and range from fully digital retail banks to marketplace banks to those that provide 'banking-as-a-service'. Among the prominent names in the field of fully licensed and independently operated digital banks are Rakuten Bank, Sony Bank, and Jibun Bank, all of which are based in Japan. It includes Banco Original and Nubank from Brazil, Tandem, Atom Bank, Starling Bank, Monzo, and Revolut from the United Kingdom. Germany's N26 and SolarisBank. Among them are WeBank and MyBank in China. Timo from Vietnam. In addition to Volt from Australia, Pepper and Judo Bank from Israel are examples. Digital banks have grown on the back of falling trust in the traditional banking sector after the global financial crisis, advances in technology, and increasing demand from customers for lower cost, more convenient, and customer-friendly financial services (Choi 2020).

Digital banks, also known as online banks or neobanks, have become increasingly popular in recent years. These banks operate entirely online, without any physical branches, and offer their services through mobile apps and websites. The concept of online banking was first introduced in the 1980s and 1990s, when traditional banks began offering electronic banking services to their customers. These services included online account access, bill payments, and money transfers. The first online-only banks, such as Ally Bank in the US and First Direct in the UK, were launched in the early 2000s. These banks offered competitive interest rates and low fees and were able to attract customers who were dissatisfied with traditional banks. The popularity of digital banks increased in the 2010s, with the launch of new online-only banks like Simple, Chime, and N26. These banks offered a more streamlined and user-friendly banking experience and used technology to provide personalized financial advice to their customers. In recent times, digital banks are becoming more mainstream, with traditional banks launching their own digital banking services to compete with the online-only banks. Many digital banks are also expanding their offerings beyond basic banking services, such as offering investment products and insurance (Choi 2020).

Overall, the history of digital banks shows how technology has revolutionized the banking industry and how consumers are increasingly turning to digital banking services for their financial needs. A digital bank, also known as an online bank or neobank, is a financial institution that provides banking services exclusively through digital channels such as mobile apps and online portals. Unlike traditional banks that have brick-and-mortar branches, digital banks do not have physical branches and operate entirely through digital platforms (Murinde et al. 2022).

According to the European Central Bank, "Digital banks refer to financial institutions that provide banking services primarily via digital channels, such as mobile apps or online portals, rather than through physical branches". The Financial Stability Oversight Council (FSOC) in the United States defines digital banks as "financial institutions that conduct substantially all of their activities through the internet or other electronic channels with no physical presence".

While there is no standard definition of a digital bank, on this topic we borrow the definition from the Bank for International Settlements (BIS): digital banks are deposit-taking institutions that are members of a deposit insurance scheme, which deliver banking services primarily through electronic channels instead of physical branches.

2.4. Digital Risk and Customer Protection

Digital risk refers to the potential harm or negative impact that can arise from the use of digital technologies, including the Internet, social media, and mobile devices. These risks can include cyberattacks, data breaches, identity theft, fraud, and other forms of online crime (Quach et al. 2022).

Customer protection, on the other hand, refers to the measures that are put in place to safeguard the interests of consumers when using digital technologies. These can include regulations, policies, and practices designed to protect customer privacy, prevent fraud and other forms of online crime, and ensure that consumers have access to secure and reliable digital services (Nizioł 2021).

In his Restricted Access/Limited Control (RALC) theory, Moor (1997) emphasized the need for strict controls to ensure privacy and prevent unauthorized access to personal information. Bongomin and Ntayi (2020) argued that RALC provides a suitable framework for implementing online privacy policies that address privacy concerns related to digital transactions. Marano (2019) explained that digital customer protection is necessary to safeguard financial product users, including those dealing with digital financial intermediaries. According to Mazer and McKee (2017), digital customer protection is a critical component of an inclusive financial system that promotes transparency and fairness to build confidence in formal financial services and providers. To measure digital customer protection variables, Bongomin and Ntayi (2020) adapted items from previous studies by Malady (2016); Mazer and McKee (2017); and Park and Mercado (2021).

The impact of digital banks on customer protection has been unclear despite overwhelming research on digital financial services and FI (Naumenkova et al. 2019). The protection of customers is an important aspect to consider. With the growth of digital banks, customers can access more financial services, but they are also exposed to risks (Chen et al. 2021).

Data access is restricted to authorized users through authentication mechanisms. Authentication methods could include passwords, two-factor authentication, or biometrics. It would be possible for anyone to gain access to sensitive information without them. Encryption mechanisms, on the other hand, make data unreadable to anyone who intercepts them. The process protects the financial information, personal information, or even private messages of customers. Customer data need to be explained to them in detail, including what data are being collected about them and how they are being used. It is important to have clear data privacy policies to build trust with customers and to allow them to make informed choices (Sun et al. 2018). Moreover, customers need to be able to contact someone who can help them quickly and effectively if they have a security concern. Customers could be supported by a responsive customer service team or security incidents could be reported according to a clear process. Finally, customers should know what risks they may face and how to avoid them (Mazer and McKee 2017). An example could be information on how to identify phishing attempts, how to create strong passwords, or how to avoid common scams. In order to protect customers, banks in Pakistan must implement all of these measures. Data breaches can be reduced through this approach, and customers in Pakistan's market are empowered to take control of their own data.

2.5. Theoretical Background

There are several theoretical frameworks that underpin the concept of FI, including the economic development theory, the financial sector development theory, and the social exclusion theory. These theories provide different perspectives on the drivers of FI and the roles that financial services play in promoting economic growth and reducing poverty.

According to Beck (2021), financial sector development is a critical driver of economic growth, and access to financial services is a key component of financial sector development. Digital banks, as financial institutions that offer banking services through digital channels, can expand access to financial services for underserved populations, including low-income households, women, and rural communities. Financial sector development theory suggests that the adoption of digital banking can lead to the development of a more inclusive financial system by expanding access to financial services for underserved and marginalized populations, including low-income households, women, and rural communities. Digital banking can also increase financial sector efficiency by reducing transaction costs and improving service delivery, leading to increased financial sector development and economic growth.

In addition to the above theories, agency theory suggests that FI initiatives must consider the incentives and motivations of different stakeholders, including financial service providers, regulators, and consumers, in order to effectively address associated risks (Akighir et al. 2022). Agency theory is a well-established economic theory that explains the relationship between principals (such as shareholders or owners) and agents (such as managers or employees) in an organization. This theory is relevant to understanding digital risks, which refer to the risks associated with the use of digital technologies, including cyber threats, data breaches, and other types of digital fraud. According to agency theory, conflicts of interest can arise between principals and agents due to differences in their objectives and incentives. For example, principals may prioritize long-term growth and profitability, while agents may focus on short-term gains or personal interests (Jensen and Meckling 2019). This divergence of interests can create information asymmetry and lead to agency problems, such as moral hazard and adverse selection.

Digital risks can exacerbate agency problems in several ways. For instance, the increasing reliance on digital technologies can create new vulnerabilities and expose banks to cyber threats and data breaches. This can result in significant financial losses, reputational damage, and legal liabilities, which can undermine the long-term interests of principals. Moreover, digital risks can create incentives for agents to engage in opportunistic behavior or shirking, such as by intentionally exploiting digital vulnerabilities or neglecting cybersecurity measures. This can lead to moral hazard and adverse selection problems, as agents may prioritize their own interests over those of the principals. To mitigate agency problems associated with digital risks, principals can adopt various measures, including improved governance mechanisms, better alignment of incentives, and effective risk management strategies (Chen et al. 2021). For example, banks can implement robust cybersecurity policies, invest in cybersecurity training for employees, and establish clear accountability frameworks for managing digital risks.

Risk Management Theory

Risk management theory plays a crucial role in the context of FI, as it enables the development and delivery of financial products and services that are tailored to the needs of underserved and marginalized communities. FI seeks to provide access to affordable financial products and services to those who are traditionally excluded from the formal financial sector, such as low-income households, women, youth, and small businesses. Effective risk management is essential for the sustainability of FI efforts, as it helps to ensure that these products and services are delivered in a responsible and transparent manner. This involves identifying and managing risks associated with the delivery of financial services, such as credit risk, operational risk, market risk, and liquidity risk (Ozili 2018).

Risk management theory also explains that digital risks are an increasingly critical aspect of risk management in today's digital age. Effective risk management requires a proactive approach that involves identifying potential risks, taking measures to mitigate them, monitoring for new threats, and communicating about cybersecurity risks. By adopting these strategies, organizations can better protect themselves against digital risks and ensure the security as well as integrity of their digital infrastructure (Moeller 2007).

Risk management theory and agency theory are based on the fact that risk management can help mitigate agency problems by reducing information asymmetry and aligning the interests of principals and agents. By identifying and managing risks, organizations can ensure that they have adequate information with which to make informed decisions and reduce the chances of opportunistic behavior by agents. For example, effective risk management practices can help organizations identify and address cyber threats, data breaches, and other types of digital fraud, which are increasingly becoming concerns for principals.

Moreover, risk management can help reduce agency costs by providing incentives for agents to act in the best interests of an organization. For instance, if risk management is integrated into performance evaluation and compensation systems, agents may be motivated to engage in risk-reducing behavior and avoid excessive risk-taking, which

can benefit the long-term interests of principals. Risk management theory and agency theory are closely related and can be interlinked to improve organizational performance as well as reduce agency problems. By integrating risk management into their governance and management practices, organizations can improve transparency, align incentives, and mitigate the adverse impact of uncertainty on their stakeholders.

Similarly, according to Moor's (1991, 1997) theory of privacy, known as "Restricted Access/Limited Control" (RALC), the establishment of private contexts or zones to limit others from accessing personal information requires strict control. To protect information in a given situation, privacy policies should restrict others from accessing that information, which in turn limits the control individuals have over their information. By adopting RALC, an online privacy policy can comprehensively address a broad range of privacy concerns related to digital transactions. Therefore, implementing RALC's digital customer protection can create an environment conducive to transactions over mobile money platforms and promote FI.

There is a controversy in the existing literature: the extreme FI problem. Extreme FI occurs whenever access to the formal financial sector is granted to all individuals irrespective of their riskiness and income level. Extreme FI opens the door to everyone, so that everybody can access the formal financial sector. Extreme FI also grants financial access to convicts, criminals, hackers, and fraudsters, too. Most FI studies suggest that access to finance should be granted to everybody and all barriers to financial access should be removed—policymakers consider this to be extreme, at least in practice. Policymakers prefer the removal of some, not all, barriers to FI (Ozili 2020). Digitalization and automation in financial services are major factors that must be addressed. Customers trust banks as a one-stop-shop for their requirements because security and client protection are vital to them; however, in this digital banking era, the challenge is how far digital banking can be applied while maintaining the security of consumer transactions and the safety of customers (Kitsios et al. 2021).

Jayalath and Premaratne (2021) looked into the obstacles to digital transformation in Sri Lanka's banking industry. They said that the banking and financial sector is one of Sri Lanka's most competitive businesses, and, as a result, the industry is facing hurdles in terms of digital growth. It was discovered that, in addition to other business development strategies, all established financial institutions are prioritizing digital transformations to achieve market diversification by developing new business opportunities while considering the generation effect with the help of emerging technologies (Jayalath and Premaratne 2021). According to the survey, most institutions' digital transformation projects have been hampered by a lack of a clear digital strategy, a failure to identify adequate process re-engineering needs, and a failure to pick the optimum technology to offer digital business solutions. Defining a comprehensive digital strategy with strong leadership, transforming existing processes to be compatible with digital products and services, utilizing the most appropriate and cost-effective technology, customer engagement (Fatma and Khan 2023), and customer service are just a few of the key factors that have a significant impact on delivering successful digital business solutions combining digital technology (Jayalath and Premaratne 2021).

Yudi Kornelis (2022) investigated and studied the advancements and legal issues of customer protection in digital banking in Indonesia. It was discovered that digital banking and digital banking services have evolved and will continue to play an essential part in the future creation of a digital ecosystem. An "innovative and secure business; a prudent and sustainable digital banking business; adequate risk management aspects; governance and IT capability requirements for digital bank directors; customer protection of personal data and the risk of data leakage; and the contribution of digital banks to the development of the digital financial ecosystem" are among the challenges in implementing digital banking.

According to the Consultative Group to Assist the Poor, mobile money service providers can increase the adoption of their services by offering comprehensive fraud awareness and prevention programs to sensitize consumers, staff, and agents on fraud trends and prevention measures. Similarly, Mazer and McKee (2017) discovered that revealing loan

terms and conditions to borrowers using KopaCash, a mobile money service provided by Jumo, in Kenya resulted in lower default rates among borrowers.

2.6. Framework and Hypotheses

Past research has shown that risk management plays a significant role in shaping customer protection while using digital financial services, but these studies have examined risk management as a general concept without identifying specific security factors unique to Pakistan's digital banks. Consequently, the present study has proposed a risk indicator framework that includes an authentication mechanism, encryption mechanisms, data privacy details, responsiveness, and information provided, with each factor considered as a separate variable in the research.

2.6.1. Authentication Mechanism

Authentication is a crucial process that ensures a user's identity is verified, and that the activity being carried out is performed by a legitimate individual, thus minimizing the risk of identity theft. For instance, users are often required to verify their identity by entering a one-time password (OTP) to complete payment transactions. Authentication plays a vital role in shaping a user's experience, and thus their decision to adopt digital wallets (Cheah et al. 2021). As trust is a crucial factor, it is essential for digital wallet providers to regulate relevant aspects, such as authentication, to ensure that customers feel confident and secure when using their services.

Therefore, the following hypothesis is proposed:

Hypothesis 1 (H1). *Customer protection in digital banks is greatly enhanced by strong authentication mechanisms.*

2.6.2. Data Privacy Details

The restricted access/limited control (RALC) theory of privacy by Moor (1991, 1997) posits that, in setting-up contexts or zones of privacy to limit or restrict others from access to one's personal information, strict control should be implemented. The privacy policies that protect information in a particular situation by normatively restricting others from accessing that information provide individuals with limited controls. The adoption of RALC helps to frame an online privacy policy that is sufficiently comprehensive in scope to address a wide range of privacy concerns that arise in connection with digital transactions. Thus, the adoption of digital customer protection stipulated under RALC can create a conducive environment for transactions over the digital financial services platform to promote FI. Ozili (2018) observes that the wide use of digital technologies in areas such as digital financial services increases the pervasiveness and scale of cyberattacks that pose a significant threat to the security and privacy of customers' data on digital channels. Similarly, customers' awareness that their data is prone to cyberattacks has made them lose trust in digital channels to perform their transactions.

Privacy details refer to the information collected from customers by digital services, including private information used for registration purposes and authentication mechanisms. Several previous studies have found that the ability of digital banks to maintain customer privacy significantly impacts customer satisfaction and protection.

In today's digital age, customers are increasingly aware of the importance of protecting their personal data. Digital banks that prioritize privacy and data protection through measures such as strong encryption, multifactor authentication, and regular security audits can attract and retain customers who value the security of their information (Wewege et al. 2020). Therefore, the following hypothesis is proposed:

Hypothesis 2 (H2). *Customer protection in digital banks is significantly enhanced by privacy and data protection.*

2.6.3. Encryption Mechanisms

The process of encrypting data involves specific steps and procedures with which to safeguard information and prevent unauthorized access from third parties or hackers. This is carried out by converting data into a gibberish form that can only be decrypted using a unique key or mechanism that corresponds to the encryption method used. Encryption mechanisms are crucial in protecting financial institutions' server systems from breaches by hackers. By ensuring the security of electronic payments, encryption mechanisms play a significant role in increasing consumer confidence in conducting transactions online (Muhtasim et al. 2022).

Therefore, the following hypothesis is proposed:

Hypothesis 3 (H3). *Customer protection in digital banks is significantly enhanced by a properly implemented encryption mechanism.*

2.6.4. Information Provided

According to Ozili (2018), the widespread adoption of digital technologies like mobile money has led to an increase in the prevalence and magnitude of cyberattacks, which pose a substantial risk to the security and privacy of customer data on digital platforms. Consequently, customers have become increasingly aware of the vulnerability of their data to cyberattacks, leading to a loss of trust in digital channels for conducting transactions.

Digital wallet services can enhance customers' knowledge about security by providing relevant information. When digital wallet users are informed of security procedures, they may feel more assured about the safety of a system. Conversely, if customers are unaware of security measures, they may not trust a digital wallet service. Furthermore, having knowledge about digital payment services has a positive and significant effect on customers' continued use of digital wallets; therefore, the security information shared by digital wallet services can help customers become more knowledgeable about security and boost their confidence in the system (Akhila Pai 2018). Therefore, the following hypothesis is proposed:

Hypothesis 4 (H4). *Customer protection in digital banks is significantly enhanced by the information provided.*

2.6.5. Responsiveness

Toor et al. (2016) state that being responsive to customers, displaying a willingness to assist them, and offering prompt services are all elements of responsiveness. These factors ultimately contribute to achieving customer satisfaction, which leads to customer protection.

According to the Consultative Group to Assist the Poor, mobile money providers can significantly increase the uptake of their services by offering comprehensive fraud awareness and prevention programs to sensitize consumers, staff, and agents on fraud trends and prevention measures. A study by Mazer and McKee (2017) found that disclosing loan terms and conditions to borrowers using KopaCash, offered by Jumo mobile money, in Kenya resulted in reduced defaults among the borrowers.

Therefore, the following hypothesis is proposed:

Hypothesis 5 (H5). *Customer protection in digital banks is significantly enhanced by responsiveness.*

The conceptual framework is summarized in Chart 1:

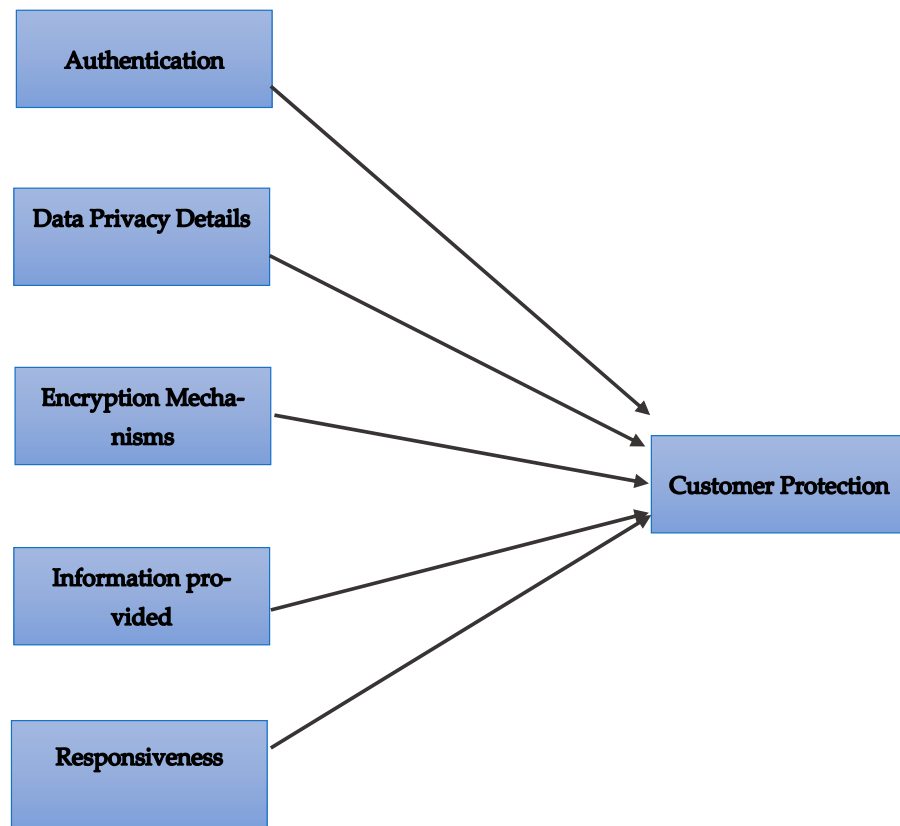


Chart 1. Conceptual framework.

3. Data and Methodology

3.1. Research Design and Unit of Analysis

The research design can be defined as a plan of procedure to conduct the study, data collection, and analysis of variables stated in the research problems. In this research, a cross-sectional survey method, along with a quantitative approach, was used to gather responses from selected participants. Moreover, the unit of analysis means the object that is being studied in the research. The subject can be an individual, household, or organization. The present study has used organizations (banks existing in Pakistan) as the unit of analysis. The aim was to investigate how various risk parameters affect customer protection in the context of using digital financial services. The study commenced by searching for literature in popular databases such as Scopus, Google scholar, etc. In total, 1012 relevant research papers were reviewed. After applying the PRISMA search strategy (preferred reporting elements for systematic reviews and meta-analyses), 37 literature sources were selected.

In order to categorize and organize the findings and results, we reviewed the results, identified duplicates, and used inclusion as well as exclusion criteria. We generated tables of research papers ($n = 37$) based on their classification, allowing us to organize them. Manually comparing and contrasting search lists was performed. By referring to the inclusion/exclusion criteria, we were able to eliminate studies that did not fit our review's objectives from the search and also discard repeated search items. Our search criteria were determined based on an analysis of the study objectives and a brainstorming session with peers to find the best words to describe the search. We set the search parameters at a high level and used generic best-fit phrases, which led us to a number of sources. It was understood that if the initial search did not yield significant results, a narrower syntax would be commissioned. We achieved the most relevant search by implementing a specific syntax, after which we narrowed it to digital financial services and customer protection.

3.2. Instrumentation, Measures of Variables

The measurement scales of the present study were obtained from previous published research. The variables of authentication mechanism, encryption mechanisms, data privacy details, and information provided were measured using items that were adapted and modified from [Muhtasim et al. \(2022\)](#), and the variable of responsiveness was measured using the items that were obtained and modified from [Kaur et al. \(2021\)](#). Additionally, customer protection was measured using items obtained and modified from [Bongomin and Ntayi \(2020\)](#). The detailed dimensions of these variables, along with their references, have been provided in [Table A1 \(Appendix A\)](#).

3.3. Data Collection Procedure

To collect data with which to examine the impact of various risk factors on customer protection while using digital financial services, we created a survey. The survey consisted of 36 statements. The first section of the questionnaire was related to a respondents' age, gender, and occupation. The respondents were asked to respond to the 36 statements using a five-point Likert scale, in which "5" = strongly agree, "4" = agree, "3" = neutral, "2" = disagree, and "1" = strongly disagree.

A structured survey was conducted to gather data from customers of various banks. The survey was conducted from the first quarter of 2023 to the first quarter of 2024. The sample consisted of customers in Pakistan who used digital banking services. The survey yielded 250 valid responses, which, as per [Hinkin's \(1995\)](#) recommendation, is an optimal sample size for performing structural equation modeling. Hinkin suggested that the item-to-response ratio should range from 1:4 to 1:10 for each scale analyzed, which translates to 120–300 responses ([Deb and Lomo-David 2014](#); [Hinkin 1995](#)).

To analyze the data collected, the researchers used Microsoft Excel to calculate descriptive frequencies of the participant demographics. Afterwards, the present study employed SmartPLS (partial least square), a structural equation modeling tool, to examine the relationship between the variables (fair treatment of customers, transparency, privacy and data protection, security, complaints handling and dispute resolution, and responsible business practices) and their impact on customer protection when using digital financial services in Pakistan.

4. Data Analysis and Findings

The primary aim of this section is to showcase the outcomes derived from the analysis of the data. The analysis encompasses descriptive and inferential statistics. Descriptive analysis was carried out to portray the demographic characteristics of the current study. Furthermore, this section delves into the findings obtained through SmartPLS path modeling, wherein the measurement model was utilized to examine cross-loadings, convergent validity, internal consistency reliability, and discriminant validity. Likewise, a structural model was developed to ascertain the influence of path coefficients, R-squared values, the individual variable effect size, and the predictive relevance model. Finally, the hypotheses were tested, and the results were subjected to PLS-SEM analysis to uncover the mediating effect of social media use, which was then reported as a component of the structural model. [Table 1](#) shows details of the questionnaire distributed and the response rate received.

Table 1. Response rate of questionnaires.

Type of Questionnaire	Response Rate
Distributed	500
Returned	245
Incomplete	20
Returned and usable	225
Response rate percentage	47%
Usable response rate	45%

4.1. Demographics Analysis

This section encompasses demographic characteristics, such as gender, age, and educational level, pertaining to digital banks. With respect to gender, the data reveal that males accounted for 62 percent of the total responses, whereas females constituted 38 percent. Hence, the majority of respondents were male. The descriptive analysis further illustrates that 50 percent of the total respondents fell within the age range of 35–45 years, while 35 percent were aged between 25 and 35 years, and 15 percent were aged between 44 and 55 years. Regarding educational attainment, individuals with a bachelor’s degree comprised 56 percent of the respondents, while those with a master’s degree constituted 35 percent. Lastly, respondents with post-master’s-level education represented 9 percent of the total respondents.

4.2. Descriptive Analysis of Latent Construct

The following descriptive statistics were computed based on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The statistics include the mean, minimum, maximum, and standard deviation values. The descriptive statistics reveal that the mean values range from 3.5 to 3.9, while the standard deviation values range from 0.8 to 1.1, as shown in Table 2. Additionally, the results of Cronbach’s alpha align with the standard criteria for reliability. An average reliability is considered to be at least 0.65, whereas a reliability score of 0.70 or higher indicates a higher level of instrument reliability.

Table 2. Descriptive Analysis of Latent Construct.

	Min	Max	Mean	SD	Cronbach’s Alpha
Authentication	1	5	3.540	0.858	0.890
Data privacy	1	5	3.527	0.875	0.709
Encryption mechanisms	1	5	3.988	1.033	0.808
Information provided	1	5	3.727	1.114	0.734
Responsiveness	1	5	3.780	1.096	0.851
Customer protection	1	5	3.864	0.948	0.866

4.3. Assessment of Measurement Model

The current study investigated the validity and internal consistency reliability of the model used to assess the outer model, which is also referred to as the measurement model. This model is depicted in Figure 1.

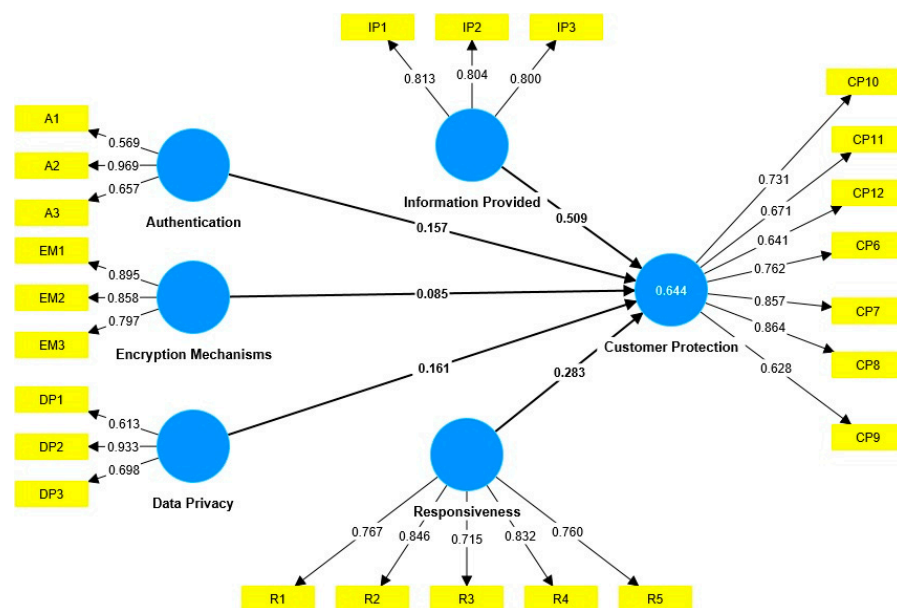


Figure 1. The PLS algorithm of the measurement model.

4.3.1. Internal Consistency Reliability and Convergent Validity

The internal consistency reliability of the model was assessed using composite reliability (CR). The table presented below demonstrates that all values exceed 0.50, thereby satisfying the criteria outlined by [Hair et al. \(2014\)](#). Additionally, [Ringle et al. \(2020\)](#) define convergent validity as “the extent to which a latent construct accounts for the variance in its indicators”. Furthermore, [Table 3](#) reveals that each construct achieves at least 50% of the variance (i.e., AVE is equal to or greater than 0.50), surpassing the threshold value specified by [Ringle et al. \(2020\)](#).

Table 3. Reliability and validity results.

Construct	Items	Loadings	Composite Reliability (CR)	Average Variance Extracted (AVE)
Authentication	A1	0.569	0.890	0.565
	A2	0.969		
	A3	0.657		
Data privacy	DP1	0.613	0.709	0.578
	DP2	0.933		
	DP3	0.698		
Encryption mechanisms	EM1	0.895	0.808	0.724
	EM2	0.858		
	EM3	0.797		
Information provided	IP1	0.813	0.734	0.649
	IP2	0.804		
	IP3	0.800		
Responsiveness	R1	0.767	0.851	0.617
	R2	0.846		
	R3	0.715		
	R4	0.832		
	R5	0.760		
Customer protection	CP10	0.731	0.866	0.550
	CP11	0.671		
	CP12	0.641		
	CP6	0.762		
	CP7	0.857		
	CP8	0.864		
	CP9	0.628		

4.3.2. Discriminate Validity

[Kline’s \(2023\)](#) criteria were employed to assess the validity of the constructs, which include two commonly utilized parameters, namely HTMT.85 and HTMT.90, with predetermined cutoff points. The HTMT values were evaluated based on these thresholds. [Table 4](#) displays values that are below the specified threshold values.

Table 4. Heterotrait–monotrait ratio of correlations (HTMT).

	Authentication	Customer Protection	Data Privacy	Encryption Mechanisms	Information Provided	Responsiveness
Authentication						
Customer protection	0.121					
Data privacy	0.078	0.092				
Encryption mechanisms	0.111	0.305	0.058			
Information provided	0.130	0.902	0.123	0.307		
Responsiveness	0.059	0.726	0.094	0.167	0.094	

4.4. Structural Model

Following the evaluation of the measurement model, the focus shifted towards assessing the structural model. The structural model incorporates path coefficients and t-values to analyze direct and indirect relationships. Moreover, a t-value greater than 1.64 is considered significant in determining the strength of the relationship and is subsequently utilized to make decisions regarding the hypotheses proposed earlier. The structure model of the study is depicted in Figure 2 below.

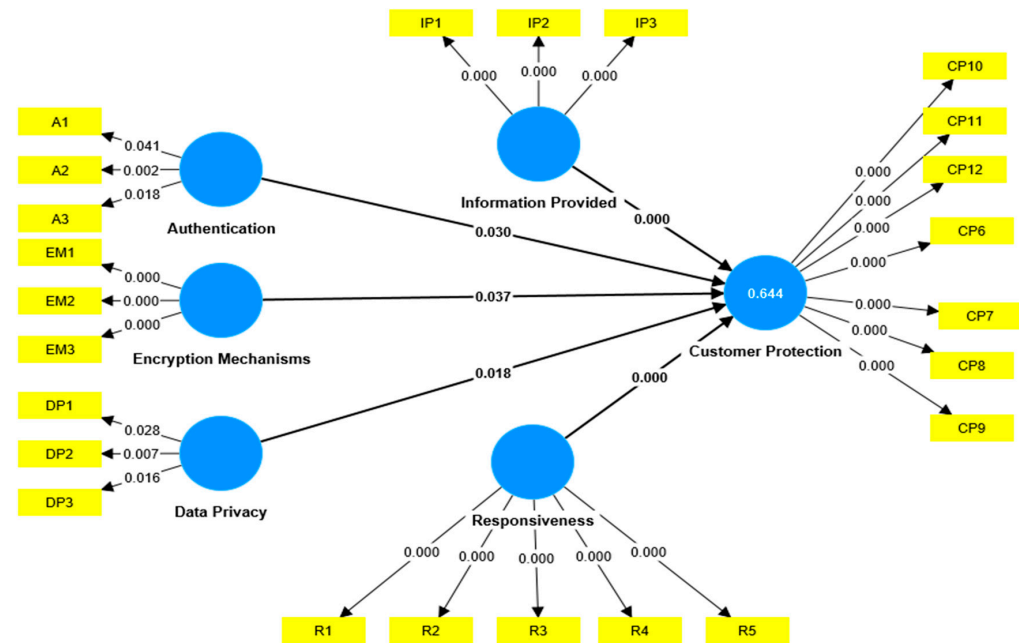


Figure 2. Assessment of the structural model.

4.4.1. Assessment of Structural Model

Table 5 presents the hypotheses that received support in the present study with t-values exceeding 1.64. Consequently, all hypotheses regarding direct relationships were supported in the current study; however, the first direct hypothesis, which examines the direct influence of authentication on customer protection, did not receive support (beta value = 0.157; T = 1.878; and $p < 0.05$). Conversely, the second direct hypothesis, which investigates the impact of data privacy on customer protection, received support (beta = 0.161; T = 2.100; and $p < 0.05$). Similarly, the third direct relationship, focusing on the impact of the encryption mechanism on customer protection, was found to be significant (beta = 0.085; T = 1.786; and $p < 0.05$). The fourth direct relationship, which examines the impact of information provided on customer protection, was also found to be significant (beta = 0.509; T = 7.082; and $p < 0.05$). Lastly, the fifth direct hypothesis, which explores the direct impact of responsiveness on customer protection, was supported (beta = 0.283; T = 4.071; and $p < 0.05$).

Table 5. Hypotheses testing results (direct effect).

	Std. Beta	Std. Error	T-Value	p-Value	Decision	R ²
Authentication → customer protection	0.157	0.083	1.878	0.030	Supported	0.644
Data privacy → customer protection	0.161	0.077	2.100	0.018	Supported	
Encryption mechanisms → customer protection	0.085	0.048	1.786	0.037	Supported	
Information provided → customer protection	0.509	0.072	7.082	0.000	Supported	
Responsiveness → customer protection	0.283	0.070	4.071	0.000	Supported	

4.4.2. Assessment of the Coefficient of Determination (R^2)

To evaluate the predictive accuracy of the research model, the researcher computed the coefficient of determination (R^2). In the present study, the coefficient of determination (R^2) is calculated to be 0.644. This value indicates the extent to which the variance in the endogenous variable is explained by all the exogenous variables. According to the thresholds established by [Hair et al. \(2014\)](#), an R^2 value of 0.75 is considered substantial, 0.50 is considered moderate, and 0.25 is considered weak in terms of predictive accuracy. As depicted in the table above, the values demonstrate a substantial level of predictive accuracy.

5. Discussion and Conclusions

5.1. Discussion

The aim of this study was to offer a fresh perspective on the factors influencing customer protection in the digital banking sector in Pakistan, with a specific emphasis on digital risk factors. The subsequent discussion centers on the hypotheses generated within this study.

The examination of hypotheses indicates that the p -value for the positive influence of a robust authentication mechanism on customer protection when utilizing digital banking services is 0.030, which is below the threshold of 0.05 ([Cheah et al. 2021](#)). Therefore, H1 is supported. Consequently, it can be concluded that the adoption of a strong authentication mechanism by digital banks has a significant positive impact on customer protection ([Cheah et al. 2021](#)). The findings imply that customers are more inclined to utilize digital financial services when the authentication process is robust and secure. Based on the survey results, a secure authentication process is likely to alleviate security concerns among users of digital financial services ([Wewege et al. 2020](#)).

Furthermore, the p -value for the impact of robust data privacy controls on customer protection is below 0.05, specifically 0.018. Consequently, H2 is also supported, indicating that data privacy exerts a significant positive influence on customer protection in the context of digital financial services. This finding underscores the fact that users of digital banking services place great importance on the privacy of their data, which in turn affects the level of customer protection within the digital financial system. In today's digital era, customers possess an increased awareness regarding the significance of safeguarding their personal data ([Wewege et al. 2020](#)). Digital banks that prioritize privacy and data protection through measures such as robust encryption, multi-factor authentication, and regular security audits can attract and retain customers who value the security of their information.

Moreover, the p -value for the correlation between encryption mechanisms and customer protection is 0.037, indicating its significance at a level below 0.05. Hence, H3 is also supported, highlighting the substantial positive impact of encryption mechanisms on customer protection within the realm of digital banking. The survey respondents express their concerns regarding the acceptance or rejection of digital financial services based on the presence of encryption mechanisms. Similarly, participants believe that the implementation of strong encryption mechanisms serves as a preventive measure against the misuse or unauthorized access of user information when utilizing digital financial services ([Muhtasim et al. 2022](#)).

Based on the table presented above, H4 is also substantiated as the p -value for the impact of information provided is 0.000, which is less than 0.05. Thus, it can be inferred that the information provided holds a significant positive influence on customer protection. The findings highlight that the information disseminated by digital financial service providers enables users of digital banking to gain a better understanding of security measures ([Akhila Pai 2018](#)). The provision of additional security information enhances the credibility of online payment systems. Moreover, when consumers are aware of the software performance, they feel more assured about the security of the digital banking system. Consequently, the study concludes that the proposed security factors significantly impact customer protection within digital banks, based on the hypotheses that were tested ([Akhila Pai 2018](#)).

The p -value for the impact of responsiveness on customer protection is 0.000, which is below the significant level of 0.05. Therefore, H5 is supported, indicating that being responsive to customers in digital banks has a significant effect on customer protection. The

findings validate the expectation of digital banking users that financial service providers should demonstrate a willingness to assist them and provide prompt services. These factors ultimately contribute to customer satisfaction, which in turn enhances customer protection (Mazer and McKee 2017).

5.2. Conclusions

The present study has introduced a comprehensive security framework consisting of five factors that impact customer protection when utilizing digital financial services in Pakistan. In conclusion, all of the factors proposed in this research exhibit a significant positive influence on customer protection (Mazer and McKee 2017). The analysis reveals that the information provided holds the greatest significance in influencing customer protection within digital financial services, followed by responsiveness, data privacy, authentication, and encryption mechanisms; therefore, the implementation of enhanced information security management principles is crucial for the progress and development of the digital banking industry in Pakistan (Mazer and McKee 2017; Park and Mercado 2021).

In recent years, digital banks have experienced a surge in popularity due to their provision of convenient and cashless digital financial services for daily payments and transactions. However, limited research has been conducted to systematically consider and derive security factors during the development of digital financial payment systems. Without a comprehensive understanding of these security factors, the progress of the digital banking industry may be hindered. This study aims to fill this research gap by exploring and identifying specific security factors that are crucial for digital financial service providers. Notably, these factors have not been previously analyzed in the context of customer protection, making this research contribution unique and valuable. Therefore, this study significantly enhances the theoretical literature surrounding digital banks by shedding light on previously unexplored security factors (Bongomin and Ntayi 2020; Malady 2016; Mazer and McKee 2017; Park and Mercado 2021).

Customer protection is of utmost importance for the thriving digital banking industry (Quach et al. 2022). As the prevalence of hackers and fraudulent activities continues to rise, it is imperative to enhance the security of digital financial services (Ozili 2018). The findings of this research can serve as a valuable resource for digital financial service providers, enabling them to strengthen their system security and prioritize key security factors that contribute to enhanced customer protection within digital banks. Furthermore, this study can provide valuable guidance to future researchers who intend to delve into this field by considering the variables proposed and examined in this study.

While our study has provided valuable insights, it is important to acknowledge its limitations. Despite achieving a satisfactory response rate for our survey, it is crucial to recognize that the respondents represent only a subset of customers in Pakistan. In order to broaden the scope of research and facilitate comprehensive discussions on customer protection in the context of digital financial services in Pakistan, it would be advantageous to attract a more diverse pool of customers from various regions within the country. Furthermore, future research endeavors could explore the factors that influence customer preferences in different countries, such as the level of economic development, literacy, and other relevant sociocultural aspects. Such investigations would be intriguing and offer valuable comparative insights into the digital banking industry across diverse national contexts.

5.3. Policy Implications

The establishment of digital banks is a significant stride towards promoting FI. To ensure the success and security of digital financial services, it is crucial for the promoters of such services, as well as regulators, to focus on reinforcing the existing customer protection laws applicable to digital banking platforms. This necessitates a collaborative approach, involving fintech companies, financial institutions, and regulatory bodies. By collectively strengthening the laws against digital banking fraudsters, a robust framework can be established to deter and penalize those involved in fraudulent activities within the fintech

ecosystem. Additionally, it is essential to establish an efficient mechanism for recourse, compensation, and remedies to benefit the victims of frauds and cybercrimes in digital banking. Implementing stringent laws and imposing appropriate legal consequences on individuals found guilty of digital banking fraud will further contribute to safeguarding the interests of customers and maintaining the integrity of the digital banking industry.

Author Contributions: Conceptualization, F.A. and A.H.; methodology, F.A., A.H. and A.H.M.; software, F.A., A.H. and S.N.K.; validation, M.E.-A., S.A. and M.A.; formal analysis, F.A., A.H.M., A.H. and S.N.K.; investigation, F.A., M.A.; resources, M.A., S.A., M.E.-A. and S.N.K.; data curation, F.A., A.H. and A.H.M.; writing—original draft preparation, F.A., A.H. and A.H.M.; writing review and editing, F.A., A.H.M., A.H. and S.N.K.; visualization, S.N.K.; supervision, M.E.-A.; project administration, A.H., S.N.K. and A.H.M. All authors have read and agreed to the published version of the manuscript.

Funding: The authors would like to thank EIAS Data Science Lab, Prince Sultan University for paying the APC of this article.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the first author.

Acknowledgments: The authors would like to thank Prince Sultan University for their valuable support.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Dimensions and sources.

Variable	ID	Measurement Item	Source
Authentication mechanism	A1	User authentication has a directly proportional relationship with digital e-wallet security.	Muhtasim et al. (2022)
	A2	User authentication helps in ensuring that the genuine cardholder is in charge while completing transactions online.	
	A3	User authentication acts as another measure to keep scammers away.	
Encryption mechanisms	EM1	A good encryption mechanism can prevent user information from being misused or hacked.	Muhtasim et al. (2022)
	EM2	An encryption mechanism acts as a barrier between a customer and third parties with malicious intent to steal customer information.	
	EM3	Encrypted data would have no value when stolen by a hacker because the data are encrypted.	
Data privacy details	DP1	Information taken from a user can cause security issues perceived risk.	Muhtasim et al. (2022)
	DP2	User information is vulnerable.	
	DP3	The more confidential information stored results in a higher user perceived risk.	
Responsiveness	R1	Digital banking provides quick confirmation of the service ordered.	Kaur et al. (2021)
	R2	Digital banking can handle customer complaints directly and immediately.	
	R3	A bank's website provides appropriate information to customers when a problem occurs.	
	R4	Digital banking promptly responds to requests and questions that are made by email or other means.	
	R5	In digital banking, a bank quickly resolves problems that you encounter with digital transactions.	

Table A1. Cont.

Variable	ID	Measurement Item	Source
Information provided	IP1	Information provided by the digital wallet system can help a user to understand more about security.	Muhtasim et al. (2022)
	IP2	Providing more information about security improves the transparency of an online payment system.	
	IP3	Users will feel more assured and at ease if they are provided with more security information.	
Customer protection	CP1	I feel secured to give my data over digital financial service platforms.	Bongomin and Ntayi (2020).
	CP2	I am not worried to use digital banking channels because of their safety.	
	CP3	I believe that the digital banking agents will not expose my personal information to a third party.	
	CP4	I do not have fear that the digital banking agents will wrongly process my transactions.	
	CP5	I feel assured that my money will be refunded if it send to a wrong person.	
	CP6	I believe that the digital banking technology can stop intrusion into my account.	
	CP7	The existing laws are effective to protect digital banks users against fraud.	
	CP8	I believe that the associated risk with digital banks is minimal.	
	CP9	The digital financial service provider gives a lot of security instructions on how to protect my account from fraudsters.	
	CP10	My details are easily identified by a digital bank system if a fraudster uses it.	
	CP11	The digital bank workers have no access to my PIN numbers.	
	CP12	The digital banking service providers have strong internal controls to protect all my transactions.	
	CP13	The digital bank service providers automatically block my PIN when tampered with.	
	CP14	The telecom companies always prevent SIM swaps.	
	CP15	I can easily stop a wrong digital money transaction.	
	CP16	It is easy to get all the useful information about digital banking.	

References

- Akhila Pai, H. 2018. Study on consumer perception towards digital wallets. *IJRAR* 3: 385–91.
- Akighir, David Terfa, Tyagher Margaret, Jacob Terungwa Tyagher, and Tordue Emmanuel Kpoghul. 2022. An Empirical Analysis of the Impact of Agency Banking on Financial Inclusion in Benue State, Nigeria: Implications for Economic Activities. *International Journal of Economics and Finance* 14: 1–75.
- Alliance for Financial Inclusion (AFI). 2014. *Mobile Financial Services Consumer Protection in Mobile Financial Services*. Mobile Financial Services Working Group (MFSWG). Guideline Note No. 13. Kuala Lumpur: Alliance for Financial Inclusion.
- Al-Mudimigh, Abdullah, and Muhammad Anshari. 2020. Financial technology and innovative financial inclusion. In *Financial Technology and Disruptive Innovation in ASEAN*. Hershey: IGI Global, pp. 119–29.
- Arun, Thankom, and Rajalaxmi Kamath. 2015. Financial inclusion: Policies and practices. *IIMB Management Review* 27: 267–87. [[CrossRef](#)]
- Beck, Thorsten. 2021. Digital technology and financial innovation: A literature survey. In *Fostering Fintech For Financial Transformation*. London: CEPR Press.
- Bongomin, George Okello Candiya, and Joseph Mpeera Ntayi. 2020. Mobile money adoption and usage and financial inclusion: Mediating effect of digital consumer protection. *Digital Policy, Regulation and Governance* 22: 157–76. [[CrossRef](#)]
- Broby, Daniel. 2021. Financial technology and the future of banking. *Financial Innovation* 7: 47. [[CrossRef](#)]

- Budiyo, Elizabeth Fiesta Clara Shinta, and Sukmawati Sukamulja. 2023. Digital Customer Protection: Mediator between Mobile Money Usage and Financial Inclusion. *Media Ekonomi dan Manajemen* 38: 205–33. [\[CrossRef\]](#)
- Cheah, Jit Seng, Salmi Mohd Isa, and Shaohua Yang. 2021. The impact of perceived usefulness, perceived value, and perceived security on mobile payment app loyalty through satisfaction: User interface as moderator. *Proceeding National & International Conference* 14: 44.
- Chen, Yanyu, E. Kusuma Kumara, and V. Sivakumar. 2021. Investigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research* 326: 1–22.
- Choi, Youjin. 2020. *Digital Banks: Lessons from Korea*. Washington, DC: World Bank Group.
- Deb, Madhurima, and Ewuuk Lomo-David. 2014. An empirical examination of customers' adoption of m-banking in India. *Marketing Intelligence & Planning* 32: 475–94.
- Diener, Florian, and Miroslav Špaček. 2021. Digital transformation in banking: A managerial perspective on barriers to change. *Sustainability* 13: 2032. [\[CrossRef\]](#)
- Fatma, Mobin, and Imran Khan. 2023. Impact of CSR on customer citizenship behavior: Mediating the role of customer engagement. *Sustainability* 15: 5802. [\[CrossRef\]](#)
- Hair, Joe F., Jr., Marko Sarstedt, Lucas Hopkins, and Volker G. Kuppelwieser. 2014. Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review* 26: 106–21. [\[CrossRef\]](#)
- Hinkin, Timothy R. 1995. A Review of Scale Development Practices in the Study of Organizations. *Journal of Management* 21: 23. [\[CrossRef\]](#)
- Jayalath, J. A. R. C., and S. C. Premaratne. 2021. Analysis of digital transformation challenges to overcome by banks and financial institutions in Sri Lanka. *International Journal of Research Publications* 84: 1–9. [\[CrossRef\]](#)
- Jensen, Michael C., and William H. Meckling. 2019. Theory of the firm: Managerial behavior, agency costs and ownership structure. In *Corporate Governance*. Farnham: Gower, pp. 77–132.
- Kaur, Baljinder, Sood Kiran, Simon Grima, and Ramona Rupeika-Apoga. 2021. Digital banking in Northern India: The risks on customer satisfaction. *Risks* 9: 209. [\[CrossRef\]](#)
- Kikulwe, Enoch M., Elisabeth Fischer, and Matin Qaim. 2014. Mobile money, smallholder farmers, and household welfare in Kenya. *PLoS ONE* 9: e109804. [\[CrossRef\]](#)
- Kitsios, Fotis, Ioannis Giatsidis, and Maria Kamariotou. 2021. Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services. *Journal of Open Innovation: Technology, Market, and Complexity* 7: 204. [\[CrossRef\]](#)
- Kline, Rex B. 2023. *Principles and Practice of Structural Equation Modeling*. New York: Guilford Publications.
- Kornelis, Yudi. 2022. Digital banking consumer protection: Developments & challenges. *Jurnal Komunikasi Hukum (JKH)* 8: 378–94.
- Kwenda, Farai, and Tough Chinoda. 2019. The impact of institutional quality and governance on financial inclusion in Africa: A two-step system generalised method of moments approach. *Journal of Economic and Financial Sciences* 12: 1–9.
- Leeladhar, Vivek. 2006. Taking banking services to the common man-financial inclusion. *Reserve Bank of India Bulletin* 60: 73–77.
- Malady, Louise. 2016. Consumer protection issues for digital financial services in emerging markets. *Banking & Finance Law Review* 31: 389–401.
- Marano, Pierpaolo. 2019. Navigating InsurTech: The digital intermediaries of insurance products and customer protection in the EU. *Maastricht Journal of European and Comparative Law* 26: 294–315. [\[CrossRef\]](#)
- Mazer, Rafe, and Kate McKee. 2017. Consumer protection in digital credit. *CGAP*, 24.
- Mhlanga, David. 2021. Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International Journal of Financial Studies* 9: 39. [\[CrossRef\]](#)
- Moeller, Robert R. 2007. *COSO Enterprise Risk Management: Understanding the NEW integrated ERM Framework*. Hoboken: John Wiley & Sons.
- Moloi, Tankiso, and Oluwamayowa Olalekan Iredele. 2020. Risk management in the digital era: The case of Nigerian banks. In *Digital Transformation in Business and Society: Theory and Cases*. Cham: Palgrave Macmillan, pp. 229–46.
- Moor, James H. 1991. *The Ethics of Privacy Protection*. Champaign: University of Illinois.
- Moor, James H. 1997. Towards a theory of privacy in the information age. *ACM Sigcas Computers and Society* 27: 27–32. [\[CrossRef\]](#)
- Mugambi, Allan, Christopher Njunge, and Samuel C. Yang. 2014. Mobile-money benefits and usage: The case of M-PESA. *IT Professional* 16: 16–21. [\[CrossRef\]](#)
- Muhtasim, Dewan Ahmed, Siok Yee Tan, Md Arif Hassan, Monirul Islam Pavel, and Samiha Susmit. 2022. Customer satisfaction with digital wallet services: An analysis of security factors. *International Journal of Advanced Computer Science and Applications* 13: 195–206. [\[CrossRef\]](#)
- Murinde, Victor, Efthymios Rizopoulos, and Markos Zachariadis. 2022. The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis* 81: 102103. [\[CrossRef\]](#)
- Naumenkova, Svitlana, Svitlana Mishchenko, and Dmytro Dorofiev. 2019. Digital financial inclusion: Evidence from Ukraine. *Investment Management & Financial Innovations* 16: 194.
- Nizioł, Krystyna. 2021. The challenges of consumer protection law connected with the development of artificial intelligence on the example of financial services (chosen legal aspects). *Procedia Computer Science* 192: 4103–11. [\[CrossRef\]](#)
- Njoroge, Patrick. 2016. Financial inclusion in Sub-Saharan Africa. Paper presented at the TICAD VI/Alliance Forum Foundation & Comesa, Nairobi, Kenya, August 26.
- Noreen, Umara, Attayah Shafique, Zaheer Ahmed, and Muhammad Ashfaq. 2023. Banking 4.0: Artificial intelligence (AI) in banking industry & consumer's perspective. *Sustainability* 15: 3682. [\[CrossRef\]](#)
- Ouma, Shem Alfred, Teresa Maureen Odongo, and Maureen Were. 2017. Mobile financial services and financial inclusion: Is it a boon for savings mobilization? *Review of Development Finance* 7: 29–35. [\[CrossRef\]](#)
- Ozili, Peterson K. 2018. Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review* 18: 329–40. [\[CrossRef\]](#)

- Ozili, Peterson K. 2020. Theories of financial inclusion. In *Uncertainty and Challenges in Contemporary Economic Behaviour*. Bradford: Emerald Publishing Limited, pp. 89–115.
- Park, Cyn-Young, and Rogelio V. Mercado. 2021. Financial inclusion: New measurement and cross-country impact assessment 1. In *Financial Inclusion in Asia and beyond*. London: Routledge, pp. 98–128.
- Quach, Sara, Park Thaichon, Kelly D. Martin, Scott Weaven, and Robert W. Palmatier. 2022. Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science* 50: 1299–323. [[CrossRef](#)] [[PubMed](#)]
- Ringle, Christian M., Marko Sarstedt, Rebecca Mitchell, and Siegfried P. Gudergan. 2020. Partial least squares structural equation modeling in HRM research. *The International Journal of Human Resource Management* 31: 1617–43. [[CrossRef](#)]
- Saqib, Najia, Haider Mahmood, Muntasir Murshed, Ivan A. Duran, and Ismail Ben Douissa. 2023. Harnessing digital solutions for sustainable development: A quantile-based framework for designing an SDG framework for green transition. *Environmental Science and Pollution Research* 30: 110851–68. [[CrossRef](#)]
- Sarma, Mandira. 2008. *Index of Financial Inclusion*. Working paper No. 215. New Delhi: Indian Council for Research on International Economic Relations (ICRIER).
- Shin, Jae Woo, Ji Yeon Cho, and Bong Gyou Lee. 2020. Customer perceptions of Korean digital and traditional banks. *International Journal of Bank Marketing* 38: 529–47. [[CrossRef](#)]
- Sun, Jianguo, Qi Zhong, Liang Kou, Wenshan Wang, Qingan Da, and Yun Lin. 2018. A lightweight multi-factor mobile user authentication scheme. Paper presented at IEEE INFOCOM 2018–IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Honolulu, HI, USA, April 15–19; pp. 831–36.
- Thorat, Usha. 2008. *Financial Inclusion and Information Technology*. New Mumbai: eSocialSciences.
- Toor, Areeba, Mudassir Hunain, Talha Hussain, Shoaib Ali, and Adnan Shahid. 2016. The impact of e-banking on customer satisfaction: Evidence from banking sector of Pakistan. *Journal of Business Administration Research* 5: 27–40. [[CrossRef](#)]
- Villasenor, John, Darrell M. West, and Robin J. Lewis. 2015. *The 2015 Brookings Financial and Digital Inclusion Project Report*. Washington, DC: Center for Technology Innovation at Brookings.
- Wang’oo, Elizabeth W. 2013. *The Relationship between Financial Inclusion and Economic Development in Kenya*. Ph.D. thesis, University of Nairobi, Nairobi, Kenya.
- Wewege, Luigi, Jeo Lee, and Michael C. Thomsett. 2020. Disruptions and digital banking trends. *Journal of Applied Finance and Banking* 10: 15–56.
- World Bank. 2012. Information, Communication Technologies, and infoDev (Program). In *Information and Communications for Development 2012: Maximizing Mobile*. Washington, DC: World Bank Publications.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.