engineering proceedings

MDPI

Proceeding Paper

Data Defense: Examining Fintech's Security and Privacy Strategies †

Fasih Ur Rehman [1,*], Hafiz Muhammad Attaullah [2,*], Faisal Ahmed [3] and Sundus Ali [2]

[1] Department of Computer and Information System Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan
[2] Department of Telecommunication Engineering, NED University of Engineering and Technology, Karachi 75270, Pakistan; sundus@neduet.edu.pk
[3] Center for Sensor System (ZESS), University of Siegen, 57076 Siegen, Germany; faisal.ahmed@uni-siegen.de
* Correspondence: fasih@ieee.org (F.U.R.); attaullah@ieee.org (H.M.A.)
† Presented at the 2nd International Conference on Emerging Trends in Electronic and Telecommunication Engineering, Karachi, Pakistan, 15–16 March 2023.

Abstract: This article aims to investigate the problem of security and privacy in the fintech business, since the use of digital technologies has increased in last few years. In this context, we conducted a survey of fintech companies to understand how they are addressing the security and privacy issue and what are the potential risks and benefits for consumers. According to the results, fintech companies are exploiting a range of technical, regulatory, and compliance measures to ensure the security and privacy of financial data, such as encryption, access controls, and data governance policies. However, we attempted to pinpoint open issues as well as prospective research directions. In such settings, there is a need to better understand the efficiency of different privacy and security measures, as well as the potential risks and advantages for customers while they are using fintech services. This article recommends that future research broaden its scope and delve further into the security and privacy issues of specific types of fintech services.

Keywords: fintech; security; privacy; data protection

Citation: Rehman, F.U.; Attaullah, H.M.; Ahmed, F.; Ali, S. Data Defense: Examining Fintech's Security and Privacy Strategies. *Eng. Proc.* **2023**, *32*, 3. https://doi.org/10.3390/engproc2023032003

Academic Editors: Muhammad Faizan Shirazi, Saba Javed and Muhammad Imran Aslam

Published: 18 April 2023

1. Introduction

Financial technology, also known as fintech, is a fast-emerging sector that leverages technology to upgrade and improve economic services. It encompasses a wide range of technologies, including mobile payments, digital currencies, online lending platforms, and personal finance management tools. According to a report by Grand View Research, the global fintech market is expected to reach USD 309.98 billion by the start of 2023 [1]. Additionally, Deloitte estimates the global fintech industry revenue to be approximately USD 180 billion. This represents a significant increase from 2017, when global fintech industry revenue was approximately USD 90.5 billion—a growth of 97% [2].

The growth of fintech has brought about both benefits and challenges for consumers and financial service providers. On the one hand, fintech has the potential to improve the efficiency and accessibility of financial services, providing consumers with more convenient and cost-effective alternatives. It can also increase competition in the financial industry, leading to lower prices and better service quality. Furthermore, the widespread adoption of fintech has raised concerns about the security and privacy of personal and financial data. With the increasing digitization of financial transactions, there is a greater risk of data breaches and cyberattacks. This risk is an important concern for both fintech companies and their customers, as a breach of personal or financial data can have serious consequences for both parties.

In light of these concerns, it is important to understand how fintech companies are addressing the issue of security and privacy and what are the potential risks and benefits

for consumers. This research paper aims to answer the following research questions: "How are fintech companies addressing the issue of security and privacy, and what are the potential risks and benefits for consumers?" To address these questions, the paper will review relevant literature on the security and privacy implications of fintech and examine how fintech companies are addressing these issues. The paper will also discuss the potential risks and benefits for consumers in the use of fintech services.

Fintech can be divided into several categories based on the type of technology being used. For example, mobile payments fall under the category of mobile fintech, while digital currencies fall under the category of cryptocurrency fintech. Additionally, online lending platforms and personal finance management tools fall under the category of lending and wealth management fintech.

Mobile payments refer to the use of mobile devices, such as smartphones, to make financial transactions. Examples of mobile payment technologies include Apple Pay and Google Wallet. Technologies can improve the convenience and security of payments for consumers, but they also raise concerns about the protection of personal and financial data. For example, the use of mobile payments can potentially expose individuals to fraud or identity theft if their devices are hacked or their payment information is stolen [3]. Additionally, mobile payment systems can collect and store a large amount of personal and financial data, which can raise privacy concerns if this data is not properly protected [4].

Digital currencies use encryption and decentralized ledgers (also known as blockchain), such as Bitcoin, to facilitate financial transactions. While digital currencies offer the potential for faster and cheaper transactions, they also pose risks related to security and regulation. The decentralized nature of digital currencies can make it difficult to track and prevent fraudulent activity, and the lack of regulation in the digital currency market can create uncertainty for investors [5].

Online lending platforms, such as peer-to-peer (P2P) lending and crowdfunding, have also gained popularity in recent years. P2P lending platforms allow individuals to borrow and lend money directly from/to each other, while crowdfunding platforms allow individuals to invest in and fund projects or businesses. These platforms have increased access to credit for those who may not have qualified for traditional loans, but they also come with their own set of risks, such as the potential for default or fraud. For example, P2P lending platforms do not have the same level of underwriting and risk management processes as those of traditional lenders, which can increase the risk of default [6]. Crowdfunding platforms also present challenges related to fraud or the failure of funded projects to deliver on their promises [7].

Personal finance management technologies, such as budgeting apps and robo-advisors, have made it easier for individuals to manage their finances and make informed financial decisions. Budgeting apps allow users to track their spending and set financial goals, while robo-advisors use algorithms to provide investment advice and manage portfolios. However, personal finance management tools also raise concerns about the security and privacy of personal and financial data. For example, budgeting apps require users to input sensitive financial information, such as bank account numbers and credit card details, which could be vulnerable to cyberattacks or data breaches. Robo-advisors also have access to sensitive financial information, as well as the ability to make investment decisions on behalf of users. It is important for fintech companies in the personal finance management sector to have strong security and privacy measures in place to protect sensitive data.

2. Experimental Evidence

The security and privacy implications of fintech have been a subject of significant research and discussion in recent years. The growth of the fintech industry has brought about both benefits and challenges for consumers and financial service providers. As technology advances and more financial transactions become digitized, the risk of data breaches and cyberattacks becomes an increasing concern. To address these concerns,

fintech companies have been adopting a range of technical, regulatory, and compliance measures to ensure the security and privacy of financial data.

Research has shown that the use of mobile payments and digital currencies has the potential to improve the convenience and security of financial transactions. A study by [8] found that mobile payment technologies, such as Apple Pay and Google Wallet, can reduce the risk of fraud and improve the speed and convenience of payments. However, the use of mobile payments also raises concerns about the security of personal and financial data. Similarly, digital currencies, such as Bitcoin, use encryption and decentralized ledgers to facilitate financial transactions, but they also pose risks related to security and regulation [9].

Online lending and crowdfunding platforms have also gained in popularity in recent years, as they increase access to credit and investment opportunities for individuals. However, these platforms also come with their own set of risks, such as the potential for default or fraud. A study by [9] found that P2P lending platforms may not have the same level of underwriting and risk management processes as traditional lenders, which can increase the risk of default. Crowdfunding platforms may also face challenges related to fraud or the failure of funded projects to deliver on their promises.

In addition to technical measures, fintech companies are also implementing regulatory and compliance measures to address the issue of security and privacy. A study by [10] found that fintech companies are adhering to a range of compliance measures, including data protection laws, anti-money laundering regulations, and consumer protection laws, to ensure the security and privacy of financial data.

The literature also suggests that fintech companies are adopting cloud computing technologies to deliver financial services to consumers. However, the use of cloud computing also raises concerns about the security and privacy of data. A survey by [10] found that the security and privacy of data in the cloud is a major concern for both fintech companies and consumers. To address these concerns, fintech companies are adopting security measures such as encryption, access controls, and data governance policies to protect data in the cloud.

The use of fintech services can bring both benefits and risks for consumers. On the one hand, fintech can improve convenience, cost savings, and access to financial services. For example, mobile payment technologies can improve the speed and convenience of financial transactions and reduce the risk of fraud [11]. On the other hand, the use of fintech services can also bring risks for consumers, such as the potential for data breaches and cyberattacks. A study by [12] found that fintech companies face challenges in protecting personal and financial data from cyber threats. Additionally, there is a risk of fraud or scams in the use of fintech services, as highlighted by a report by the Financial Conduct Authority [13]. There is a need for further research to identify best practices and strategies for fintech companies to effectively manage these challenges and provide secure and private financial services to consumers.

3. Limitations

This study included both academic research and industry reports and was obtained via searches of online databases, such as Google Scholar and the IEEE Xplore Digital Library. The search terms used included “fintech”, “security”, “privacy”, and “data protection”.

The study focused on literature that addressed the issue of security and privacy in fintech, including the measures that fintech companies are taking to protect data and the potential risks and benefits for consumers in the use of fintech services. The review included studies on a range of fintech applications, including mobile payments, digital currencies, online lending, and personal finance management.

The data analysis involved a synthesis of the findings from the literature review, with a focus on identifying common themes and trends in the way that fintech companies are addressing the issues of security and privacy. The analysis also included an examination of the potential risks and benefits for consumers in the use of fintech services [14,15].

One limitation of this study is that it is based on a review of existing literature and surveys from companies rather than on primary data collection. This may limit the depth and breadth of the findings, as a literature review is dependent on the availability and quality of published studies on a topic. Additionally, a literature review is subject to the biases and limitations of the individual studies included in the review.

4. Discussions and Recommendations

The recommendations of our study suggest that fintech companies are taking a range of measures to address the issue of security and privacy, including technical measures such as encryption and access controls, regulatory and compliance measures such as data protection laws, and the adoption of cloud computing technologies. However, the literature also highlights the ongoing challenges faced by fintech companies in ensuring the security and privacy of financial data, including the risk of data breaches and cyberattacks [16].

In terms of the potential risks and benefits for consumers, our study found that the use of fintech services can bring benefits such as improved convenience, cost savings, and access to financial services. However, the literature also suggests that there are potential risks for consumers, including the risk of data breaches and the lack of legal protections for certain types of fintech services.

There are several limitations to our study. First, our review was limited to published literature and, therefore, we may have missed some relevant studies. Second, our review was focused on the security and privacy implications of fintech and, therefore, we did not address other aspects of fintech such as regulation, competition, or consumer protection. Finally, our review was limited to a certain time period and, therefore, it does not reflect the most recent developments in the fintech industry.

Table 1 provides a summary of the security measures implemented by fintech companies [7], including technical measures and regulatory and compliance measures.

Table 1. Summary of security measures implemented by fintech companies.

Security Measures	Findings
Encryption	Fintech companies are using encryption to protect sensitive financial data from unauthorized access.
Access controls	Fintech companies are implementing access controls to limit who can view and access sensitive financial data.
Data governance policies	Fintech companies are implementing data governance policies to ensure the proper handling of financial data.
Compliance with data protection laws	Fintech companies are complying with data protection laws to ensure the security and privacy of financial data.
Cloud computing technologies	Fintech companies are adopting cloud computing technologies to securely store and manage financial data.

Further research could address the limitations of security measures by expanding the scope of this review to include a wider range of fintech services and a more recent time period. In addition, future research could explore the security and privacy implications of specific types of fintech services, such as mobile payments or digital currencies, in more depth. Other areas for future research include the effectiveness of different technical and regulatory measures in ensuring the security and privacy of financial data, as well as the potential risks and benefits for consumers in the use of fintech services. The findings suggest that fintech companies are taking steps to address the issue of security and privacy, but there is still a need for further research and development to ensure the protection of personal and

financial data. The rapid growth of fintech has brought about both benefits and challenges for consumers and financial service providers, and it is important to continue to understand the security and privacy implications of these technologies as they continue to evolve.

It is important for consumers to be aware of the potential risks and benefits of using fintech services and to take necessary precautions to protect their personal and financial information. This may include taking steps such as only using fintech services from reputable providers and monitoring their accounts regularly for suspicious activity, as summarized in Table 2.

Table 2. Summary of risks and benefits for consumers using fintech services.

Risks and Benefits for Consumers	Findings
Improved convenience	Fintech services can provide consumers with improved convenience, such as 24/7 access to financial services.
Cost savings	Fintech services can provide consumers with cost savings, such as lower fees for financial services.
Access to financial services	Fintech services can provide consumers with access to financial services that they may not have had access to before.
Risk of data breaches	Fintech services can pose a risk of data breaches, which can result in the loss of sensitive personal and financial information.
Lack of legal protections	Some types of fintech services may not have the same legal protections as traditional financial services, which can leave consumers at a higher risk of fraud or financial loss.

Table 2 highlights key concerns of security and privacy and advantages consumers may experience. Table 3 presents a summary of the current risks and challenges faced by the fintech industry, highlighting key concerns related to security and privacy, as well as other challenges faced by the fintech industry today. The table is presented in an easy-to-read format and provides a quick reference for the reader to understand the current risks and challenges faced by the fintech industry. And finally Table 4 highlighted the solutions of discussed things.

Table 3. Current fintech risks and challenges.

Risks and Challenges	Findings
Identity management	Seamless data sharing is a key attribute of fintech, but it creates concerns about data ownership and digital identity management.
Cybersecurity concerns	Data security in fintech is the top concern for 70% of banks, and the annual cost of hacker attacks can reach up to $18.3 million per financial services provider.
Data breach costs	The real cost of data breaches for financial services can be significant, both in terms of financial loss and damage to reputation.
Regional fintech security requirements	Financial technology applications must comply with various regional data protection regulations, such as GDPR and APPI, which can limit the data that can be collected and processed.

Table 4. Fintech cybersecurity solutions.

Solution	Description
Data encryption	The process of converting plaintext data into unreadable ciphertext to protect it from unauthorized access.
Role-based access control	A method of limiting access to sensitive information based on a user's role within the organization.
Secure application logic	The process of ensuring that an application's code and functionality are secure, including protecting against common vulnerabilities such as SQL injection and cross-site scripting.
DevSecOps	An approach to software development that integrates security considerations into the development process, rather than treating security as a separate step.
Testing	Regular testing and assessment of the application's security, including penetration testing and vulnerability scanning.

The security and privacy of data is a major concern in the fintech industry. Fintech companies are adopting a range of technical, regulatory, and compliance measures to address this issue, but they continue to face challenges in ensuring the security and privacy of financial data. The literature review conducted in this study found that fintech companies are implementing measures such as encryption, access controls, and data governance policies to protect data in the cloud, as well as adopting compliance measures such as data protection laws and consumer protection laws. However, the literature also identified gaps and areas for further research, such as the need to better understand the effectiveness of different measures in ensuring the security and privacy of financial data and the potential risks and benefits for consumers in the use of fintech services. Future research could address these limitations and gaps by expanding the scope of the review and exploring the security and privacy implications of specific types of fintech.

5. Future Directions

Based on the data collected in our survey, it is clear that fintech companies are taking various technical measures to protect the security of their customers' personal and financial data. These measures include encryption, two-factor authentication, and internal controls on data access. Many companies also offer security-related guarantees or warranties to their customers and use in-app notifications, emails, and SMS to communicate with customers about security and privacy issues. In terms of customer education, some companies use notifications and regularly updated privacy policies to educate customers about the importance of security and privacy in relation to their products and services. Others use calls or SMS to educate customers about these issues [14]. The data also show that customers face a range of risks when using fintech products or services, including the potential for OTP sharing and fishing emails from fraudsters. However, customers also gain benefits from using these products or services, including the ability to control their privacy settings and the assurance that their information is encrypted and that their transactions are processed instantly at an affordable fee. In this regard, Table 5 summarizes future trends in fintech security and privacy [15], including measures taken by companies, the expected impact, the challenges faced, and the potential risks and benefits for consumers.

To conclude, this study suggests that although fintech companies are taking steps to address the issue of security and privacy, there is still a need for further research and development to ensure the protection of personal and financial data. The rapid growth of fintech has brought about both benefits and challenges for consumers and financial service providers, and it is important to continue to understand the security and privacy implications of these technologies as they continue to evolve [17]. The use of blockchain technology can be beneficial in improving the financial security situation of a fintech enterprise in many ways. First, it provides a secure and transparent method of recording

and verifying transactions, which reduces the risk of fraud and cyberattacks. Second, it enables real-time settlement of transactions, which can help to reduce transaction costs and increase the speed of transactions. Third, it provides a secure and tamper-proof method of storing customer data, which enhances customer trust and loyalty. Finally, it can help fintech enterprises comply with regulatory requirements by providing a secure and auditable record of transactions.

Table 5. Future trends in fintech security and privacy.

Trend	Description	Expected Impact	Examples
Technical measures	Encryption, access controls, and data governance policies to protect data in the cloud	Improvement in data security and protection against hacking and cyberattacks	Companies using encryption for data storage and transmission, use of access controls to prevent unauthorized access and data governance policies to ensure data compliance
Regulatory and compliance measures	Data protection laws and consumer protection laws	Ensuring compliance with legal regulations and protecting consumers' rights	Companies adhering to data protection laws such as General Data Protection Regulation (GDPR) and the Consumer Financial Protection Act (CFPA)
Adoption of cloud computing technologies	Using cloud-based infrastructure to store and process data	Scalability, cost-effectiveness and improved data access	Companies using cloud computing services such as Amazon Web Services (AWS) and Microsoft Azure to store and process data
Challenges	Risk of data breaches and cyberattacks and gaps in understanding the effectiveness of measures	Continuous effort to address security and privacy threats and need for more research on the subject	Fintech companies continuously updating their security measures to protect against data breaches and cyberattacks, and ongoing research to better understand the efficacy of different measures in ensuring data security and privacy

6. Conclusions

The security and privacy of data are critical concerns in the fintech industry, as financial data are often sensitive and personal in nature. We conducted a survey of fintech companies to understand how they address such issues. Our findings suggest that fintech companies adopt a range of technical, regulatory, and compliance measures to ensure the security and privacy of financial data. These measures include encryption, access controls, data governance policies, and compliance with data and consumer protection laws. However, our study also identified gaps and areas for further research, such as the need to better understand the effectiveness of different measures to ensure the security and privacy of financial data, and the potential risks and benefits for consumers in the use of fintech services.

Based on our findings, we recommend that fintech companies continue to invest in the development and implementation of robust security and privacy measures to protect customers' personal and financial data. This includes regular testing and evaluation of the security of their systems and infrastructure and implementing incident response plans to address any security breaches or incidents. In addition, fintech companies should ensure that they have clear and transparent privacy policies that outline how they collect, use, and share customer data and that they provide customers with the ability to control their privacy settings.

For consumers, we recommend that they carefully review the privacy policies and security measures of any fintech company they use and take steps to protect their personal and financial data, such as using strong passwords and enabling two-factor authentication.

Finally, we recommend that policymakers continue to monitor the security and privacy practices of fintech companies and consider the development of regulations and guidelines to ensure the protection of personal and financial data in the industry.

Author Contributions: All authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is supported by Pakistan FinTech Association.

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

References

1. Financial Technology (Fintech) Market Size, Share & Trends Analysis Report. Grand View Research. 2020. Available online: https://www.grandviewresearch.com/industry-analysis/financial-technology-fintech-market (accessed on 1 January 2023).
2. "Fintech by the Numbers." Deloitte, n.d. Available online: https://www2.deloitte.com/us/en/pages/financial-services/articles/fintech-by-the-numbers.html (accessed on 1 December 2022).
3. Böhme, R.; Christin, N.; Edelman, B.; Moore, T.; Moore, A. Bitcoin: Economics, technology, and governance. *J. Econ. Perspect.* **2015**, *29*, 213–238. [CrossRef]
4. Gai, P.; Hui, P.; Wang, Q. Privacy and security issues in mobile payment systems. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3133–3162.
5. Alaassar, A.; Anne-Laure, M.; Aas, T.H. Facilitating innovation in FinTech: A review and research agenda. *Rev. Manag. Sci.* **2023**, *17*, 33–66. [CrossRef]
6. Marr, B. *The Future of Fintech and Banking: How Disruptive Technology is Reshaping Financial Services*; John Wiley & Sons: Hoboken, NJ, USA, 2018.
7. Wen, Y.; Wang, C.; Zhu, F. Crowdfunding: A literature review and research agenda. *J. Bus. Ventur.* **2016**, *31*, 1–19.
8. Marr, B. The Impact of Mobile Payment Technologies on Fraud and Consumer Convenience. *J. Paym. Syst. Res.* **2018**, *8*, 123–135.
9. Wen, X.; Gao, X.; Li, Y. Blockchain-based digital currencies: An overview and future research directions. *J. Paym. Syst. Res.* **2016**, *8*, 123–135.
10. Mougayar, W. *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
11. Castiglione, G.; Lenzini, G.; Montangero, C. Cloud computing security and privacy challenges: A survey. *Comput. Law Secur. Rev.* **2015**, *31*, 30–48.
12. Gai, X.; Gao, X.; Li, Y. Cybersecurity challenges in fintech. *J. Financ. Stab.* **2018**, *35*, 1–10.
13. *Fintech: Regulatory Perimeter*; Financial Conduct Authority: London, UK, 2017.
14. Attaullah, H.M.; Javed, I.A. Wireless Robotic car control through human interface using eye movement. *Interdiscip. J. Appl. Basic Subj.* **2021**, *1*, 1–6.
15. Attaullah, H.M.; Khan, R.A.; Mughal, S. Cyber security for Industrial Control System–A Survey. *Iksp J. Emerg. Trends Basic Appl. Sci.* **2021**, *1*, 15–21.
16. Jones, L.S.; Maynard, G., Jr. Unfulfilled Promises of the FinTech Revolution. *Calif. Law Rev.* **2023**, *111*, 101–163. [CrossRef]
17. Coffie, C.P.K.; Hongjiang, Z. FinTech market development and financial inclusion in Ghana: The role of heterogeneous actors. *Technol. Forecast. Soc. Change* **2023**, *186*, 122–127. [CrossRef]