Privacy-Preservation and Data-Sharing Security Issues in Banking Applications

Nikoloz Katsitadze
University of Georgia
Tbilisi, Georgia
e-mail: n.katsitadze@ug.edu.ge

Adeyinka Olanrewaju Ajagbe
University of Georgia
Tbilisi, Georgia
e-mail: ajagbe.adeyinka@yahoo.com

https://doi.org/10.62343/csit.2024.5

***Abstract* — The digital transformation of the banking sector has brought forth unprecedented convenience for users but has also exposed financial institutions to a myriad of cyber threats. Maintaining user data security and privacy has become critical as digital banking develops. This research conducts a comprehensive analysis of security incidents in prominent digital banking institutions. Common patterns and distinctive features surrounding the preservation of user data privacy are identified through a cross-examination of these cases.**

The study unveils recurring themes and unique characteristics in these security incidents, and a subsequent cross-case analysis underscores that security breaches often implicate the three integral components of institutions: People, Processes, and Systems.

This research contributes to the ongoing discourse surrounding digital banking security by providing valuable insights into prevalent vulnerabilities. Moreover, it proposes avenues for the formulation of robust security strategies, accompanied by recommendations for further research. As digital banking continues to play a crucial role in financial transactions, the findings aim to inform future practices that prioritize the protection of user data and the integrity of digital banking systems.

***Keywords* — Privacy-preservation, data-sharing security issues, banking applications, *digital transformation*.**

I. INTRODUCTION

Financial services have rapidly evolved and moved from the era of historical brick-and-mortar institutions to digital finance. This change has led to a change in the way individuals and businesses manage their finances. With the increasing transition to online platforms, ensuring the confidentiality of the users' information is paramount. Modern banking applications offer convenient services such as funds transfer, bill payment, accounts management, finance management, etc. thereby transforming the financial space into a seamless and user-friendly experience.

The advent and convenience of digital banking via applications have birthed lots of security challenges. Cyber threats, ranging from phishing attacks to sophisticated malware, data breaches because of unsecured applications, and non-adherence to regulatory framework and privacy policies, pose a constant risk to user data and financial assets. The importance of robust security measures is magnified as financial transactions are being consummated via networks, emphasizing the need for encryption, secure authentication mechanisms, and proactive threat detection.

II. PRIVACY CONCERNS AND REGULATORY FRAMEWORK

Privacy is integral to banking applications as they handle sensitive user information, including personal details and financial histories. The regulatory landscape, marked by stringent data protection laws and financial regulations, necessitates a robust framework for ensuring user privacy. Compliance with regulations such as GDPR (for countries in the European Union-EU), CCPA, and financial industry standards is not only a legal obligation but also a means of building user trust.

Security breaches and privacy lapses can have severe consequences for banking institutions. Users entrust their financial well-being to these applications, making trust a currency as valuable as the transactions themselves. A secure and privacy-respecting banking application not only safeguards users but also contributes to the institution's reputation and customer loyalty.

While stringent security measures are imperative, achieving a balance with a seamless user experience is equally crucial. Cumbersome security processes may deter users, highlighting the importance of implementing solutions that are both robust and user-friendly. Multi-factor authentication, biometric verification, and continuous monitoring are examples of technologies that enhance security without compromising usability.

III. RATIONALE FOR THE STUDY

The rationale for this study is rooted in the points highlighted below:

I. Increased focus on data privacy: Data privacy has become a primary concern for financial institutions due to increased awareness from regulatory bodies, general awareness, and cyber-attacks.

II. Balancing data sharing and security: Open banking raises concerns about the amount of data to be shared with other parties, and it is important to balance the importance of providing relevant data for services and reducing unwanted data sharing.

III. Transparency in data usage: Open banking necessitates transparency in how customer data is utilized, stored, and shared. Financial institutions and third-party providers must be honest about their practices, policies, and security measures in place to secure customer data.

IV. RESEARCH OBJECTIVES

For the case of this research, the objectives and scope of this project are outlined below.

- Identify and analyze the privacy and data sharing security issues in both open banking and digital banking.
- Compare the security and privacy challenges faced by financial institutions in implementing these two banking models, by Identifying patterns, similarities, and differences, and providing a comprehensive view of their respective strengths and weaknesses.
- Recommend solutions to address the identified security and privacy issues in open banking and digital banking.
- Provide insights and recommendations into how financial institutions can strike a balance between data sharing for innovative services and maintaining customer privacy.

Help people comprehend the significance of data privacy in relation to banking technology changes and laws, like the General Data Protection Regulation (GDPR).

V. SCOPE AND LIMITATIONS OF THE RESEARCH

Scope of the Study:

- Comparison of privacy and data sharing security issues in open banking and digital banking.
- An examination of the privacy and security issues that financial organizations encounter when putting these two banking models into practice.
- The identification of viable remedies to security and privacy concerns in digital and open banking.
- Exploration of the balance between data sharing for innovative services and maintaining customer privacy

Limitations of the Study:

- Limited Access to Internal Information
- Reliance on Historical Data
- Assumption of Accurate Public Information
- Methodological shortcomings
- User-Specific Context

VI. RESEARCH METHODOLOGY

This study will be built upon the application of qualitative research methodology. To support the perceptions, information from libraries and the internet will be used as a secondary data collecting type in this study.

One essential component of the process is the instances to be used. The cases will center on privacy and security, and the best ways to protect them in financial applications. This methodology attempts to produce an inventive, context-rich inquiry that leads to a thorough understanding of Privacy-Preservation and Data-Sharing Security Issues in Banking Applications by utilizing the strengths of the case study method.

Case Study Research Design: The cases used for this project provide ample information on the Privacy-Preservation and Data-Sharing Security Issues in Banking Applications, security, and policy concerns, and many more. The importance of privacy preservation cannot be over-emphasized, as its relationship ensuring the security of users' data.

Techniques for Gathering Data: Examining various data breach scenarios can reveal trends and similarities throughout firms, along with the opportunities and problems they encountered.

Approaches to Data Analysis: Upon completion of the study, a cross-case analysis will be conducted to determine whether existing security vulnerabilities are similar or different, and to determine the best ways to protect users' privacy when using banking applications.

VII. COMPARATIVA ANALYSIS

Upon cross-examination of the cases of Westpac, Bank of Ireland, Cash App, Flagstar Bank, UniCredit, and JPChase Morgan and Co., we uncovered common patterns, as well as distinctive features concerning the security issues bordering the preservation of the privacy of users' data that occurred during the incidences highlighted in this research work.

Common Themes:

- Personal Identifiable Information (PII) Exposure: In all the cases reviewed, significant amounts of personally identifiable information (PII) were exposed, ranging from names, addresses, phone numbers, and email addresses, investment portfolios, etc. This raised concerns about the potential for identity theft and other malicious activities.
- Data Privacy and Protection: Every example highlights how important it is to have strong security measures in place to safeguard personal data. The dangers of gathering and keeping a lot of personal data were made clear by the hacks.
- Reputational Damage: The breaches caused harm to the organizations' reputations, which persists to some extent even now.
- Lack of encryption for sensitive data: Sensitive data as personally identifiable information (PII), should be encrypted. This would, as much as possible, ensure that bad actors, even if they get access to it, may not be able to make any use of it.
- Failure to Use multi-factor authentication (MFA): MFA is a security feature that provides an additional degree of protection. The security breaches made clear how crucial it is to use multi-factor authentication (MFA) to stop unwanted access even in the case that credentials are compromised.
- Financial losses to the companies and the customers involved: In all the cases reviewed, there were financial implications in the form of loss of funds to the customers and fines incurred by the companies.

Distinctive Features:

- Type of Data Stolen: In the Bank of Ireland case, the data revealed was not to bad actors. The internal issues in the system made the wrong customer’s details appear when a user logs into their banking application, which has the potential for fraud to occur. All the other cases, however, had some form of users’ private information exposed.
- Insider Threats: The Cash App and Desjardins' cases stood out as those that emanated from the inside, as against the others which were attempts from external parties. These kinds of threats are the hardest to identify.

- Third-Party Vulnerabilities: Westpac's case was because the third-party company, PayID was compromised, which by extension affected them.
- Incorrect Customer Information Management System Update: The flaw that existed in the customer information system of the Bank of Ireland made a different customer's information appear on the bank's mobile application when a customer logged into it.
- Access Control policy lapses: Still in Westpac's case, even if the ex-staff had access to the system, access to personal information such as an investment portfolio should require levels of access to view and authorization to download.
- Regulatory Impact: The Bank of Ireland case violated data privacy policies, which helped the European Union implement the General Data Protection Regulation (GDPR). They were heavily fined for the lapses as well.

Cross-case analysis. A review of all these cases brings us to the understanding of the following:

- All institutions are made of three components: People, Processes, and Systems.
- A great deal of breaches are because of the people (i.e. human errors). However, it is important to build systems that are easy to use and ensure that robust training policies are in place to ensure that this is curbed or reduced to the barest minimum. Most times, it is these lapses that bad actors (aka hackers) prey on to gain access to the system.
- All the security issues/ threats can either emanate internally or externally.
- Internally, the threats that emanated were from a disgruntled staff that had access to the system, while the other case was that of an ex-staff that still had access to the banking system, even after leaving the system.
- The external threats in this review were via phishing attempts, which enabled bad actors to

VIII. SUMMARY

This research examined security issues in digital banking, analyzing cases from Westpac, Bank of Ireland, Cash App, Flagstar Bank, UniCredit, and JPChase Morgan and Co. Common themes included PII exposure, data privacy concerns, reputational damage, lack of encryption, failure to implement MFA, and financial losses. Distinctive features included the type of data stolen, insider threats, third-party vulnerabilities, access control policy lapses, and regulatory impact.

Cross-Case Analysis Findings:

- Components of Breaches: Breaches often involve the three components of institutions: People, Processes, and Systems. Human errors are significant contributors, emphasizing the importance of user-friendly systems and robust training policies.
- Internal and External Threats: Breaches may originate internally (disgruntled staff, ex-employees with access) or externally (phishing attempts). A multi-layered security strategy is vital, involving access control, encryption, internal audits, human resource management, and continuous employee training.

CONCLUSION

Safeguarding digital banking requires a comprehensive approach. The identified security issues underscore the critical need for institutions to address vulnerabilities in their people, processes, and systems. A multi-layered security strategy, including access control, encryption, and continuous training, is crucial. Rapid incident response plans and learning from past mistakes are essential for minimizing the impact of data breaches. As the digital banking space evolves, maintaining a cyber-aware office environment is paramount to ensuring the security and privacy of customer transactions.

REFERENCES

1. Ahirrao, S. (2023, May 2). What are the Major Security and Privacy Challenges in Open Banking? Ardent Privacy. https://www.ardentprivacy.ai/blog/what-are-the-major-security-and-privacy-challenges-in-open-banking/
2. Arabia, S. (2023, August 30). 5 winning strategies for digital transformation journey of banks. https://www.linkedin.com/pulse/5-winning-strategies-digital-transformation-journey-banks/
3. Biggest Data Breaches in US History (Updated 2024) | UpGuard. (n.d.). https://www.upguard.com/blog/biggest-data-breaches-us#:~:text=The%20data%20breach%20of%20Yahoo,over%20the%20next%20three%20years.
4. Burgess, M. (2020, March 24). What is GDPR? The summary guide to GDPR compliance in the UK. WIRED UK. https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018
5. Challenges and opportunities of digitising the customer relationship. (n.d.). https://blog.cenareo.com/en/digitising-the-customer-relationship
6. Chaurasia, N. (2023, December 5). The 10 Biggest Data Breaches of the 21st Century: Lessons in Cybersecurity. Sprintzeal.com. https://www.sprintzeal.com/blog/biggest-data-breaches
7. Coventry, S. (2023, November 6). Security Measures for Protecting Mobile Banking Users. https://www.poundsterlinglive.com/central-news-feed/148-opinion-news-feed/19470-mobile-banking-protection-11-key-security-measures
8. Data Privacy in Digital Banking | Meniga. (n.d.). https://www.meniga.com/blog/data-privacy-in-digital-banking/
9. Degrees, S. (2023, August 10). Five Biggest Data Breaches in Financial Service History: Lessons to Be Learnt. Six Degrees. https://www.6dg.co.uk/blog/biggest-data-breaches-financial-services/
10. DPC (Ireland) - IN-20-7-2. (n.d.). GDPRhub. https://gdprhub.eu/index.php?title=DPC_(Ireland)_-_IN-20-7-2
11. Fintechly (2021, July 4). Digital or Open Banking. Finextra Research. https://www.finextra.com/blogposting/20470/digital-or-open-banking
12. Fintechly (2022, June 22). Discover How Fintech's Shaping the Future of Banking. Fintechly. https://fintechly.com/financing/how-fintech-is-shaping-the-future-of-banking/
13. Frankenfield, J. (2020, November 11). General Data Protection Regulation (GDPR) Definition and Meaning. Investopedia. https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp
14. GDPR Data Protection: Definitions and Practical Measures. (2023, September 27). Cloudian.

https://cloudian.com/guides/data-protection/gdpr-data-protection/
15. Issues and Challenges Associated with Data Sharing. (2016, April 29). Principles and Obstacles for Sharing Data From Environmental Health Research - NCBI Bookshelf. https://www.ncbi.nlm.nih.gov/books/NBK362423/
16. Khan, H. (2023, October 17). 8 Effective Digital Transformation Strategies in Banking. Wavetec. https://www.wavetec.com/blog/banking/digital-transformation-tips-for-banks/
17. Khon, S., Nizam, A., Tan, D., & Taraporevala, Z. (2022, July 13). Best of both worlds: Balancing digital and physical channels in retail banking. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/best-of-both-worlds-balancing-digital-and-physical-channels-in-retail-banking
18. Koch, R. (2023, September 14). Everything you need to know about GDPR compliance. GDPR.eu. https://gdpr.eu/compliance/
19. Lake, R. (2021, April 5). Increase In Digital Banking Raises Consumer Data Privacy Concerns: How To Protect Yourself. Forbes Advisor. https://www.forbes.com/advisor/banking/digital-banking-consumer-data-privacy-concerns/
20. Leuillier, A. (2023, January 20). What Is the Impact of Digitalization on Customer Service? Vocalcom. https://www.vocalcom.com/blog/impact-digitalization-customer-service/
21. Ovington, T. (2023, May 21). Digital transformation in banking: A complete guide - WalkMe Blog. WalkMe Blog. https://www.walkme.com/blog/digital-transformation-in-banking/
22. Privacy Laws for Apps: How to Protect User Data? (2023, May 23). https://cookie-script.com/blog/privacy-laws-for-apps-how-to-protect-user-data
23. Sadik, N. (2023, April 26). Revolutionizing Customer Relationship Management: The Impact of Digital Transformation and AI. https://www.linkedin.com/pulse/revolutionizing-customer-relationship-management-impact-nassim-sadik/
24. Security, I. (2023, November 13). How can you overcome security challenges in the digital era? www.linkedin.com. https://www.linkedin.com/advice/1/how-can-you-overcome-security-challenges-digital
25. Temple, A. (2023, October 25). Navigating the security challenges of digital commerce. Commercetools. https://commercetools.com/blog/navigating-the-security-challenges-of-digital-commerce
26. The digital customer relationship in financial service - Livework. (2023, September 15). Livework - English. https://liveworkstudio.com/insight/the-digital-customer-relationship-in-financial-service/
27. The Impact of Digital Transformation & Customer Experience. (2023, May 18). https://www.linkedin.com/pulse/impact-digital-transformation-customer-experience/
28. UniCredit 2015 data incident. (2019, October 28). UnicreditGroup.eu. https://www.unicreditgroup.eu/en/press-media/press-releases/2019/unicredit-2015-data-incident.html
29. What is Data Protection and Privacy? (2023, October 27). Cloudian. https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/
30. Wolford, B. (2023, September 14). What is GDPR, the EU's new data protection law? GDPR.eu. https://gdpr.eu/what-is-gdpr/
31. Yin, R. (2014). Case Study Research Design and Methods. Canadian Journal of Program Evaluation, 282.