INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 06 Issue 12 December 2023

DOI: 10.47191/ijmra/v6-i12-77, Impact Factor: 7.022

Page No. 6059-6064

Navigating the Data Security Landscape: Challenges and Solutions in Financial Markets amid Digitalization and Artificial Intelligence

Mithilesh Gupta[1], Urvi Naresh Shah[2]

[1]Assistant Professor at St. Peter Degree College

[2]Assistant Professor at Mount Carmel Junior College

ABSTRACT: Financial markets have the risk of data mishandling or leakage of information. Regarding consumer, privacy breach and information mismanagement affects the overall trust in the system. With faster digitalization and online usage of information, a large section of economic markets require that consumers reveal their individual information constituting a part of regulatory requirements and privacy agreements. Financial systems gather information such as identity, payment passwords, shopping choices, and other similar details that can be shared online. Financial data is prone to misuse and leakage through big data pricing discrimination and over-marketing. Furthermore, the adoption of artificial intelligence/ Machine learning (AI/ML) creates new, distinct cyber risks and expands possibilities for cyber-attacks. AI/ML systems are susceptible to new threats along with the usual cyber threats posed by human error or software malfunctions. Encroachment of personal details and disruption of law by certain organizations make it difficult for individuals to assess the challenges or problems encountered within financial markets. Therefore, the lack of systematic arrangement of the financial system results in financial losses and psychological disruption presenting as mistrust of the government's accountability, impairment of the social balance, and erratic behavior. The present study aims to assess: 1) The scope of data security in financial markets; 2) the Challenges encountered by financial markets in maintaining data security, 3) the Role of Artificial intelligence in data breaches and Current methods (Technical and non-technical) utilized for data security.

KEYWORDS: Data protection, data privacy, financial markets, financial data, personal, AI

I. INTRODUCTION

Data plays a significant role in all types of business markets with the growing popularity of digitalization and globalization. Individuals often share their details unintentionally and intentionally while using the internet or their smartphones [1, 2]. With the international localization of internet servers, it is challenging to restrict data collection within national borders or under a specific jurisdiction. The initial landmark of framing data security guidelines in the European Economic Area (EEA) came into being with the establishment of the General Data Protection Regulation (GDPR) in 2018. The role of GDPR is not only limited to its national territories but also involves outside locations in case European data is involved. One such industry that collects large amounts of confidential information is the financial sector. Financial markets have adopted novel Financial Technology (FinTech). Data about payment encompasses information related to ethnicity, racial origin, religious customs, health life, and other political life.

Different types of FinTech business markets are dependent on cloud computing, artificial intelligence, and big data. Therefore, the financial sector is a suitable industry to identify the role of GDPR on data security processes. To simplify the data privacy regulations across nations, different policies have been introduced to create stricter regulations [3]. To implement various practices in financial markets, the difference between data privacy, data security, system security, and information privacy needs recognition. The present article aims to investigate data protection in financial markets.

A. DATA PRIVACY

Data privacy denotes a systematic utilization of data generally offered to organizations and corporations for certain specific purposes. To fulfill business needs, data is gathered through the customers. The main aspect of such a privacy approach includes providing detailed information to the customers that is acceptable to them. For example, the Australian Federal Government has strict rules for organizations that restrict sharing complete information to customers about data privacy. In financial markets, data collection aims to assign a unique identity to the customers called Personally Identifiable Information (PII) [4].

DATA SECURITY

Data security denotes the availability, confidentiality, and unification of data [5]. Data security refers to the accessibility, and utilization of data by only authorized individuals. This means that data is available and accessible. The security plan includes a systematic collection of information, maintenance of its safety, and disruption of the details that are no longer relevant. Therefore, data security and data privacy are interrelated where the former represents the protection laid out for the collected information, and the latter denotes the way of data collection for customer identification [6].

B. INFORMATION PRIVACY

Information privacy means the inclination of individuals to have some authority over data related to them [7]. Broadly, there are four main areas where the issue of information privacy occurs: privacy, accuracy, property, and accessibility (PAPA). According to Phillips (2014), privacy consists of four aspects: Personal data privacy, privacy of person, personal communication, and personal behavior. In the digital age, the majority of communication occurs through the Internet and mobile phones, hence this has led to the unification of personal data privacy and personal communication privacy within the information privacy spectrum [7].

C. SYSTEM SECURITY

System security can be defined as a process that prevents attacks from external sources. In the banking and financial markets, secured systems achieve desirable outcomes when they regulate functions without disruptions [8].

D. CHALLENGES

At a microscopic level, mishandling of personal details, or disclosure of organizational information constitutes the personal information and disrupts the systematic processes of the financial markets. In case of severe circumstances, such activities impose risk on financial security with regards to a specific organization, that may threaten the economy as a whole in certain situations [9]. Similarly, encroachment of personal details and disruption of law by certain organizations make it difficult for individuals to assess the challenges or problems encountered within financial markets. Therefore, the lack of systematic arrangement of the financial system results in financial losses and psychological disruption presenting as mistrust of the government's accountability, impairment of the social balance, and erratic behavior.

Lack of economic stability affects how the population sees consumers and other financial organizations [10]. Regarding consumer, privacy breach and information mismanagement affects the overall trust in the system. With faster digitalization and online usage of information, a large section of economic markets require that consumers reveal their individual information constituting a part of regulatory requirements and privacy agreements. Financial systems gather information such as identity, payment passwords, shopping choices, and other similar details that can be shared online. Financial data is prone to misuse and leakage through big data pricing discrimination and over-marketing.

Financial markets have the risk of data mishandling or leakage of information. For example, senior individuals can be bribed to sell personal information illegally or receive support from hackers resulting in data leakage. This eventually contributes to financial loss as the market may have less than predicted. Additionally, data contamination is probable. In digital transactions, the occurrence of copying and data tampering of unlabelled information is highly possible. If the information is damaged, the model outcome will have different results than expected. Such inadequacy may contribute to additional clean-up costs required by financial institutions, and compromise the financial market decision-making [11].

II. AIMS AND OBJECTIVES

To address the challenges and current situation of data protection in financial markets, it is critical to assess the existing situation and define the questions.

Therefore, with the present study, we aim to assess:

- The scope of data security in financial markets
- Challenges encountered by financial markets in maintaining data security
- Role of Artificial intelligence in data breach
- Current methods (Technical and non-technical) utilized for data security
- Future perspective and the way forward to combat the problem of data security in financial markets.

III. CURRENT SITUATION

Privacy and security information of various financial companies have been evaluated in recent times. According to a survey [12] including the German population, the results denoted that the adoption of FinTech and identification of data security was dependent on the user-design interface and trust placed by consumers. In another study [13], a framework was provided to create a robust construct for FinTech companies based on strong sound security methods. Researchers have stressed the specificity and utilization of data processing by FinTech organizations. According to a study [14], data is used for the identification of an individual, and metadata is useful for the data processor. Based on a large collection of information from a German e-commerce website involving 2.5 lakh purchases, the author mentioned an immense opportunity for data collection [15]. Needless to say, such information exhibits an opportunity to assess the credibility of information. For example, a study [16] investigated the privacy reports of German financial organizations (FinTech) before and after the adoption of GDPR to evaluate the approach toward policy recommendations. However, most of the preliminary information does not specifically pay attention to the privacy statements of these companies when it comes to privacy regulatory laws and GDPR adoption. It was identified that the standardized approach for adopting privacy statements can be implemented through text analysis.

Recent studies have shown that Big Data Analytics (BDA) can pose serious implications related to data privacy and security (DPS) [17]. A study assessed how DPS investment can impact the economic stability of firms that are dependent on big data analytics (BDA) and those that are without BDA investment (non-BDA firms). The study followed a difference-in-difference methodology and application of propensity score related to >1000 DPS performed by 228 US organizations and whose stocks were offered publicly from 2004-2018 on US financial markets. The findings of the results revealed that investing in DPS diminishes any organization's risk of leakage of data. Furthermore, the risk of a data breach is greater for non-BDA firms compared to BDA firms. Therefore, it is reported that DPS investment minimizes the firm risk, and the role of information technology is greatly dependent on the other aspects of BDA. It is noticeable that the risk of a data breach is greater for non-BDA firms as they are exposed to systematic risk. This research highlights the role of security-led investment in improving financial market stability by minimizing the scope of risk [18]. Additionally, it denotes that DPS can act as a risk-changer [19].

Financial firms that include DPS strategies within their technology set-up tend to improve their market proposition by avoiding financial risks. Authentic data security solutions such as decentralized identifiers, encryption, and random identifiers can safeguard the user's information from hacking attempts and harmful exposure. Other studies have revealed that data breaches can be avoided by safely securing customer credentials, through channelizing the customer experience via a two-factor authentication process [18]. Apart from this approach, before the collection of customer data, the privacy firms should ensure that users have information regarding the reason for their data collection and understand the process of why data collection is important [20].

IV. AI AND DATA BREACH

The adoption of artificial intelligence/ Machine learning (AI/ML) creates new, distinct cyber risks and expands possibilities for cyber-attacks. AI/ML systems are susceptible to new threats along with the usual cyber threats posed by human error or software malfunctions. To take advantage of the intrinsic limits of AI/ML algorithms, these threats concentrate on data manipulation at some point in the AI/ML lifecycle. This kind of manipulation makes it possible for hackers to avoid detection and causes AI/ML to extract data or make incorrect decisions. Because of their intricacy and the possible consequences for finance-related organizations, machine learning models demand ongoing supervision to ensure that attacks of this kind are accurately identified and immediately addressed. By including unique examples in the training database of an ML algorithm, data poisoning attacks attempt to influence the algorithm during training. The AI learns to categorize or recognize data inappropriately due to these attacks. According to Liu et al. [21], data poisoning is another way to develop Trojan models, which conceal malicious activities that require specific inputs to be activated. Attacks using data poisoning need superior access to training and model input. After it is done correctly, infected models might go undetected until the malicious activity doesn't interfere with routine diagnostic tests [22].

Authorities in the financial sector are worried about AI/ML cybersecurity. AI/ML cyber threats have the potential to erode public confidence in the financial industry and its integrity. The ability of the finance industry to appropriately analyze, price, and handle risks might be compromised by corrupted structures, which could result in the accumulation of unnoticed systemic risks [22]. Additionally, training data sets containing private and confidential financial data might be obtained by attackers. The banking industry may decide to include AI/ML-specific cyber threats within the legal boundaries of cybersecurity standards. It should be mandatory for service providers and consumers of AI/ML algorithms in the finance industry to implement mitigation procedures as part of a larger cybersecurity structure [22]. These include methods to safeguard model and data confidentiality, effective security for training data sets, and detection and tracking systems.

Large-scale data privacy issues are prevalent and have existed before AI and ML became widely used. tools have been created to support the safeguarding of data participants' anonymity and private information. Globally, structures for legal data policies are being established to deal with these issues. Nonetheless, new privacy concerns are brought up by how well AI/ML models work to stop the loss of information from the data used for training [22]. By using inferences, AI/ML, for instance, can reveal anonymized data (i.e., determining identities from behavioral structures). Likewise, after using the data, AI/ML may recall details about people in the sample set, or the results of AI/ML may either explicitly or implicitly reveal private information. Tools are created to solve these problems and improve the security of AI/ML models in protecting private information. However, efforts are required, as well as a suitable revision to the regulation and law that mandates increased privacy regulations for AI/ML systems and associated databases, along with pertinent anti-money laundering and counterterrorism financing requirements [22].

V. TECHNICAL APPROACH TO DATA PROTECTION

A. Information security management in banking and financial services

When utilizing cloud computing architecture infrastructure, the finance industry takes the following precautions for data safety and confidentiality [23].

1) Identity Access Management: Using credentials and other attributes, this process aids in the authentication of users and services. The terms "User Identity" (also known as a Unique Network ID and Password) and "Characteristics" refer to the specified way that cloud services are to be operated. It is crucial to identify consumers who have access to data within the finance industry when private data about customers and their financial habits is accessible via cloud architecture. By classifying users according to their positions and duties, an IDM system assists in safeguarding their access levels [23].

2) Controlling Access and Logging Mechanism: The framework of cloud service provider models is intricate. Integration of this intricate architecture with a controlled access interface necessitates a structure for implementation and a policy-neutral access specification. The Single Sign-On (SSO) is a technique used in finance and banking to provide users access across numerous apps while controlling access [23]. These access methods verify a user's one-time identity using their "Single User ID / Network ID" and a password that complies with security regulations. The process of collecting and keeping track of user activity logs for cloud infrastructure maintenance, operation, and access is known as user activity or access logging monitoring. Monitoring user activity on cloud infrastructure aids in keeping track of all the modifications made to data and apps [23].

3) Governance and Compliance: Information safety procedures, organizational structure, and leadership comprise cloud security governance. Authorities must enforce compliance for their operations to take place. Governance and compliance guarantee that the system is strategically aligned with the demands of the business, employees, and customers. In the finance and banking sectors, the section on governance and compliance contributes to the altogether structure for working, measuring, communicating, and overseeing the security of cloud architecture [24].

4) Secure Data Removal: When a goal is accomplished, financial and banking organizations gather pertinent data and securely destroy it. Erasing data is an operational task that must be completed to maintain space for storing new data. Secure removal of information is essential when storing data on the cloud and allowing users to access it, to prevent future fraud or misuse. When using cloud infrastructure that is managed by an outside entity, it is crucial to guarantee that data is erased and verify that it is unable to be recuperated. If the information is not removed, it may be accessed later on and used dishonestly to establish fake profiles and identities for clients to carry out fraud. Financial crimes and additional problems with building trust in cloud infrastructure will result from this. Removing data securely contributes to data security maintenance [24].

B. NON-TECHNICAL APPROACHES TO DATA PRIVACY

When it comes to taking steps to address privacy issues, non-technical methods like guidelines and protocols can be highly successful along with comprehending the advantages and drawbacks of technical alternatives for data privacy in new markets. For example, government organizations in the United States are often constrained by written rules and regulations that specify acceptable uses of information [25]. Limits on privacy are typically stricter in Europe. There are legal limitations on collecting, storing, processing, and disclosing private information under the General Data Protection Regulations. Additionally, the GDPR mandates adherence to seven data protection and transparency principles, even in cases where using personal details is deemed permissible. There is a fine of up to 4% of worldwide revenue or 20 million Euros for noncompliance with the GDPR. The goal of these hefty fines is to encourage proactive data privacy practices by encouraging adherence to the GDPR. Businesses in the private sector also commonly implement policies that help staff members respect the privacy of customers [26].

Sector-driven regulations regarding data protection and privacy establish general guidelines for how and when details may be obtained, stored, safeguarded, retrieved, used, and erased, even though these policies differ amongst businesses. Some typical methods involve data reduction, use limits, disclosing requirements and restrictions, and deidentification [27]. These procedures aid in keeping organizations in check and adhering to the guidelines. According to Bowman et al. [28], other accountability mechanisms can be employed to identify any discrepancies in these rules and procedures, including audit logging and access restrictions. Yet, these rules and procedures must be based on local notions of privacy to guarantee that they are appropriately calibrated to the particular setting. Several eminent scholars have contended that the data privacy "Silicon Valley paradigm" is unsuitable for growing market environments [29]. This implies that numerous data-sharing customs that are acceptable in the United States might be considered privacy infractions in the Global South.

Numerous legislative reactions have resulted from the quick development of AI and ML. Some jurisdictions, like De Nederlandsche Bank and the Monetary Authority of Singapore, have approached the problems more comprehensively, while others have concluded that the laws currently in place and the standards for good governance are adequate to deal with the issue of data privacy. Authorities have typically concentrated on managing risks, internal controls, improved model and data controls, and AI/ML governing structures through new or updated regulations [29]. To tackle these obstacles, regulatory measures and cooperative endeavors are necessary. Building precise minimum requirements and rules for the industry along with a greater emphasis on obtaining the requisite technical skills are essential components of an appropriate policy framework. Collaboration between the banking industry, economic supervisors, and other parties is important for preventing work duplication and mitigating potential risks associated with the implementation of AI/ML systems in the world of banking. To foster AI/ML development and prevent regulatory gaps, many prominent jurisdictions are in the process of establishing clearly defined national AI plans [29].

VI. CONCLUSION

The present article describes the difficulties financial institutions face in protecting their data. Strict procedures are desperately required, even in the face of innovative laws, regulations, and policies. It is clear from the body of research that financial institutions recognize the importance of data protection and its growing necessity. The data protection regulators make an effort to reveal the caliber of data security measures implemented for financial institutions to foster openness and user-friendliness. Furthermore, to comprehend how financial policies correspond with privacy claims, they must adhere to the GDPR's laws and protocols. For example, users could actively give up parts of their data privacy in exchange for better prices or more usage rights, and conversely pay more to maintain greater data privacy. More transparency also leads to more trust and reputation gains for companies. Simple-to-use menus, for instance, might assist consumers in stopping businesses from disclosing personal data to specific third parties when it isn't strictly required for the fulfillment of a contract. In this case, technological advancements may make it possible for FinTechs and customers to implement in tandem. Lastly, data processing should be standardized and stored as tabular data. Standardization would, however, necessitate cooperation between FinTech companies and perhaps new legislative initiatives. Now that the EU and other nations have enacted a privacy law linked to the GDPR, legislators, and policymakers can understand the implications and unintended consequences of the law. This could open the door for the GDPR to be readjusted in the future or provide more useful advice on how to draft privacy statements that will guarantee compliance with all relevant legal requirements. Our research highlights the role of efficient privacy policies in protecting consumer data and future considerations to mitigate the issue of mishandling of data in financial sectors

REFERENCES

1) Lindgreen, E. R. (2018). Privacy from an economic perspective. The Handbook of Privacy Studies: An Interdisciplinary Introduction (pp. 181–208). Amsterdam: Amsterdam University Press
2) World Bank. (2021). World Development Report 2021: Data for Better Lives. Washington, D.C.: World Bank.
3) Fara Soubouti, Data Privacy and the Financial Services Industry: A Federal Approach to Consumer Protection, 24 N.C. BANKING INST. 527 (2020).
4) Sophia et al., (2014) A survey of Cryptographic approaches to securing BigData Analytics in Cloud, Sophia, p1-p2, 978-1-4799-6233- 4/14,@IEEE, 2014
5) France Belanger Privacy in the Digital Age: A review of Information privacy research in Information systems, MIS Quarterly, Vol. 35, No.4, pp 1017-1041/December 2011
6) An overview of the security concern in enterprise cloud computing, Anthony Bisong et. al., International Journal of network security & its applications (IJNSA), Vol.3, No.1, January 2011, P.36
7) Data-Intensive Applications, challenges, techniques and technologies: A survey on Big Data, C.L. Phillip Chen, C.-Y. Zhang / Information Sciences, 275, (2014). p 314 – p 347

8) Mahalle et al., Data Privacy and System Security for Banking and Financial Services Industry based on Cloud Computing Infrastructure, 2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design
9) Huo, H.; Guo, J.; Yang, X.; Lu, X.; Wu, X.; Li, Z.; Li, M.; Ren, J. An Accelerated Method for Protecting Data Privacy in Financial Scenarios Based on Linear Operation. Appl. Sci. 2023, 13, 1764. https:// doi.org/10.3390/app13031764
10) Tramer, F.; Boneh, D. Slalom: Fast, verifiable and private execution of neural networks in trusted hardware. arXiv 2018, arXiv:1806.03287
11) Sun, Y.; Shi, Y.; Zhang, Z. Finance big data: Management, analysis, and applications. Int. J. Electron. Commer. 2019, 23, 1512270.
12) Stewart, H., & Jürjens, J. (2018). Data security and consumer trust in fintech innovation in Germany. Information and Computer Security, 26(1), 109–128
13) Gai, K., Qiu, M., Sun, X., & Zhao, H. (2017). Security and privacy issues: A survey on fintech. In M. Qiu (Ed.), Smart Computing and Communication (pp. 236–247). Cham: Springer International Publishing
14) Ingram Bogusz, C. (2018). Digital traces, ethics, and insight: Datadriven services in FinTech. In R. Teigland, S. Siri, A. Larsson, A. M. Puertas, & C. Ingram Bogusz (Eds.), The Rise and Development of Fintech: Accounts of Disruption from Sweden and Beyond (pp. 207–222). London: Routledge
15) Berg, T., Burg, V., Gombovi´c, A., & Puri, M. (2020). On the rise of FinTechs: Credit scoring using digital footprints. The Review of Financial Studies, 33(7), 2845–2897
16) Dorfleitner, G., & Hornuf, L. (2019). FinTech and Data Privacy in Germany: An Empirical Analysis with Policy Recommendations. Cham: Springer International Publishing
17) Yueyue Zhang, Effect of data privacy and security investment on the value of big data firms, Decision Support Systems, https://doi.org/10.1016/j.dss.2021.113543
18) Bose, A. Chung, M. Leung, Adoption of identity theft countermeasures and its short-and long-term impact on firm value, MIS Q. 43 (2019) 313–327
19) S. Dewan, F. Ren, Risk and return of information technology initiatives: evidence from electronic commerce announcements, Inf. Syst. Res. 18 (2007) 370–394
20) J. Brill, P. Lee, Preserving privacy while addressing COVID-19, Microsoft (2020). https://blogs.microsoft.com/on-the-issues/2020/04/20/privacy-covid-19-data-co llection/
21) Liu et al., (2018). Fine-Pruning: Defending Against Backdooring Attacks on Deep Neural Networks, Available at: https://arxiv.org/abs/1805.12185
22) El Bachir Boukherouaa (2021). Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance, 24, 1-34
23) Hassan Takabi (2011). Security and privacy challenges in cloud computing environments, , Jmaes Joshi, p.5- p.8, IEE Security and privacy magazine, January 2011
24) Secure use of cloud computing in the finance sector, Good Practices and recommendations, European network for network and information security, p.7-p36, December 2015.
25) Officer, Chief Privacy, and Timothy J Keefer. 2009. “Privacy and Civil Liberties Policy Guidance Memorandum.”
26) Bamberger, Kenneth A, and Deirdre K Mulligan. 2015. Privacy on the ground: driving corporate behavior in the United States and Europe. MIT Press
27) Sedenberg, Elaine M, and Deirdre K Mulligan. 2015. “Public Health as a model for cybersecurity information sharing.” Berkeley Tech. LJ, 30: 16
28) Bowman, Courtney, Ari Gesher, John K Grant, Daniel Slate, and Elissa Lerner. 2015. The architecture of privacy: On engineering technologies that can deliver trustworthy safeguards. ” O’Reilly Media, Inc.”
29) Abebe, Rediet, Kehinde Aruleba, Abeba Birhane, Sara Kingsley, George Obaido, Sekou L Remy, and Swathi Sadagopan. 2021. “Narratives and counternarratives on data sharing in Africa.” 329–341.