Proceedings of Business and Economic Studies, 2025, Volume 8, Issue 2
http://ojs.bbwpublisher.com/index.php/PBES
Online ISSN: 2209-265X
Print ISSN: 2209-2641

Financial Data Security Management in the Era of Big Data

Yanling Liu, Yun Li*

Hainan Vocational University of Science and Technology, Haikou 570100, Hainan, China

**Author to whom correspondence should be addressed.*

Abstract: In the era of big data, the financial industry is undergoing profound changes. By integrating multiple data sources such as transaction records, customer interactions, market trends, and regulatory requirements, big data technology has significantly improved the decision-making efficiency, customer insight, and risk management capabilities of financial institutions. The financial industry has become a pioneer in the application of big data technology, which is widely used in scenarios such as fraud detection, risk management, customer service optimization, and smart transactions. However, financial data security management also faces many challenges, including data breaches, privacy protection, compliance requirements, the complexity of emerging technologies, and the balance between data access and security. This article explores the major challenges of financial data security management, coping strategies, and the evolution of the regulatory environment, and it looks ahead to future trends, highlighting the important role of artificial intelligence and machine learning in financial data security.

Keywords: Big data; Artificial intelligence; Data security; Privacy protection

Online publication: April 28, 2025

1. Introduction

Big data refers to large amounts of structured and unstructured data generated at high speed from a variety of sources. In finance, this includes transaction records, customer interactions, market trends, and regulatory requirements. The integration of big data analytics with financial services improves decision-making processes, enhances customer insight, and develops more effective risk management strategies. Big data is transforming the financial industry, offering great potential to shape future research and applications [1]. It has three key characteristics: large scale, high dimension, and complex structure, and it is pushing the boundaries of fundamental questions in various areas of finance, including corporate finance, market microstructure and asset pricing.

The financial sector has become one of the fastest growing adopters of big data technology, with banking, insurance, securities, and investment services leading the way [2]. Big data analytics in the financial sector covers a wide range of applications, such as fraud detection, risk management, customer service optimization, and smart trading. The combination of big data with artificial intelligence (AI) has further transformed the industry

by changing the way data and information are generated, processed, and incorporated into the decision-making process [3].

In summary, big data has become a key asset in the financial sector, enabling more efficient contracting and risk-sharing among corporate stakeholders. As the field continues to evolve, researchers and professionals must combine expertise in the financial sector with state-of-the-art data analytics skills to take full advantage of the opportunities offered by big data and analytics tools. However, challenges remain, including data security, privacy concerns, and the need for advanced system architecture to handle the massive data and critical latency requirements in financial analytics [4].

2. Challenges for financial data security management

In the era of big data, financial data security management is faced with unprecedented complex challenges. As financial institutions increasingly rely on huge data sets for decision-making and operations, issues such as data breaches, privacy protection, compliance requirements, the complexity of emerging technologies, and the balance between data access and security are becoming more prominent. These challenges not only threaten the normal operations of financial institutions but can also have a serious impact on customer trust and industry reputation.

2.1. Data breaches and privacy

Financial institutions handle large amounts of sensitive information, including customers' personally identifiable information, transaction records, and financial data, which are highly attractive to cybercriminals. Big data platforms often store huge amounts of high-value information, which makes them prime targets for hackers [5]. Moreover, the highly interconnected nature of the financial data ecosystem further increases the possibility of unauthorized access, leading to a significant rise in the risk of privacy violations.

The complexity of managing personal information in the big data environment requires financial institutions to adopt strong data protection measures to uphold individual privacy rights and ensure ethical practices. However, as the volume of data continues to grow and the flow of data accelerates, traditional security measures have struggled to meet the demand. Financial institutions need to adopt more advanced technical means, such as encryption and multi-factor authentication, to deal with the threat of data breaches.

2.2. Compliance requirements

Financial institutions must also contend with increasingly stringent compliance requirements. Regulatory frameworks across the globe, such as the General Data Protection Regulation (GDPR) and the Gramm-Leach-Bliley Act (GLBA), have set higher standards for data protection [6]. These regulations require financial institutions to comply with strict legal requirements during data collection, storage, and processing to ensure the security of customer data.

However, navigating these complex regulatory frameworks is not easy task, especially among financial institutions operating in multiple jurisdictions. Legal requirements can vary across countries and regions, making it necessary for financial institutions to devote significant resources to ensuring compliance. This includes establishing comprehensive compliance strategies such as regular audits, staff training, and the implementation of best practices to ensure that data processing practices meet legal requirements.

2.3. Emerging threats and technological complexity

The dynamic nature of big data also presents challenges related to the speed and amount of information. The rapid generation and processing of data require flexible security solutions that can adapt to the ever-changing

threat landscape [7]. In addition, emerging technologies such as artificial intelligence (AI) and machine learning (ML) present both opportunities and challenges in the field of data security. On the one hand, these technologies can enhance threat detection and response capabilities, enabling financial institutions to identify and respond to potential security risks more quickly. On the other hand, the complexity of these technologies could also introduce new vulnerabilities. For example, AI and ML models could be subject to data poisoning attacks or algorithmic bias that could lead to security issues. Therefore, financial institutions need to take extra care when adopting these technologies to ensure that their implementation processes meet security standards [8].

2.4. Balance data access and security

Another major challenge in financial data security management is how to strike a balance between data accessibility and security. Financial institutions need to follow the principle of least privilege by granting users only access to the information [1] required for their role. This principle helps reduce the risk of unauthorized access, but it may face difficulties in practice.

2.5. Human factors

Human factors play a crucial role in financial data security management. Although technological means can significantly improve data security, human error is still one of the leading causes of data breaches. For example, employees may be targeted by phishing attacks due to a lack of security awareness, or sensitive data may be compromised due to operational errors.

3. Manage financial data security strategies

In the context of financial institutions, data security is of Paramount importance due to the sensitivity of the information being handled. Protecting customer data and financial transactions is essential not only for regulatory compliance but also for maintaining customer trust and confidence in the integrity of the institution. As financial services increasingly rely on digital platforms and big data analytics, the potential risks associated with data breaches are escalating, highlighting the need for robust security measures [3,5].

(1) Encryption: Encryption is a key defense mechanism that converts sensitive data into an unreadable format that requires a specific key to access [9,10]. Utilize strong encryption protocols, such as AES or RSA, to ensure that even if the data is intercepted, it remains secure and protected against unauthorized access. The technology is essential to protect stored data and information transmitted over the network.

(2) Multi-factor Authentication (MFA): Multi-factor authentication adds an extra layer of security by requiring multiple forms of verification before granting access to sensitive information. This approach significantly reduces the risk of unauthorized access because it ensures that even if one credential is compromised, the additional verification step remains valid.

Perform regular security audits. Regular security audits are critical to identifying gaps in your organization's data security framework. These audits should be performed by both internal teams and external experts to get a full picture of potential vulnerabilities. Routine assessments help organizations stay vigilant and address security vulnerabilities before they can be exploited.

(3) Staff training: Human error is still a significant factor in data breaches, which makes employee training an important aspect of data security. Regular training programs strengthen an organization's security posture against insider threats by educating employees on best practices, such as identifying phishing attempts and adopting strong password policies [7,11].

(4) Incident response plan: Having a clear incident response plan in place is critical to mitigating the impact

of a data breach. The plan should outline specific steps for detecting, responding to, and recovering from a security incident, ensuring that the organization can act quickly to minimize damage in the event of a breach.

(5) Third-party risk management: Because financial institutions often work with third-party vendors, managing third-party risk is critical. Organizations must ensure that their partners adhere to strict security standards to prevent potential breaches from outside sources. This includes a thorough review process and regular evaluations of third-party security practices.

(6) Compliance: Financial institutions must navigate the complex regulations that govern data security. Ensuring compliance with these regulations not only protects customer data but also reduces legal risk. Institutions should implement policies and frameworks that meet regulatory requirements to maintain compliance and enhance data security [12].

Take advantage of emerging technologies. Leveraging machine learning and artificial intelligence can enhance real-time detection of anomalies and potential security threats. By analyzing patterns in transaction data, these technologies can take proactive measures to protect against fraud and cyber threats [5,13].

4. Regulatory environment

The emergence of fintech and rapid advances in technology have created new regulatory challenges, particularly in the areas of data security and regulatory oversight [14]. Financial institutions must navigate complex regulatory webs while managing the risks associated with the rapid data dissemination and powerful covert nature of modern financial technologies.

The regulatory framework places particular emphasis on the protection of personally identifiable information and sensitive financial data. Banks and financial institutions face serious consequences if important information and data are compromised or lost, making compliance with data protection regulations their top priority [15]. In addition, with the deepening of the process of enterprise informatization, regulatory requirements are also paying more attention to the security of information systems. Financial institutions must establish strong internal control systems to comply with regulatory standards and guard against emerging security risks.

On the compliance side, financial institutions need to address the challenges of technology integration, including maintaining secure data storage and transmission systems, implementing effective risk prevention mechanisms, and ensuring proper integration of systems while maintaining security protocols. In addition, with the increasing internationalization of financial services, financial institutions must comply with the requirements of multiple jurisdictions. In the case of ICBC USA, for example, financial institutions are subject to both domestic and international regulatory standards.

5. Future trends in financial data security

The future of financial data security will be shaped by several transformative trends that reflect changing technology and regulatory requirements.

Increased adoption of AI and ML. AI and ML are becoming an integral part of financial institutions' data security strategies. These technologies enable organizations to analyze large amounts of data in real time, enabling them to quickly detect patterns and anomalies that could indicate a security breach. By leveraging AI-powered tools, financial entities can improve their threat detection capabilities, thereby enhancing their overall security posture against increasingly sophisticated cyber threats.

Blockchain technology. Blockchain technology is gaining popularity as a means of enhancing the security and integrity of data within the financial system. Its decentralized nature allows for more secure transactions and

reduces the risk of data tampering. As financial institutions explore the potential of blockchain, they aim to create a more transparent and secure environment for data management that fosters customer trust and compliance with regulatory frameworks.

The rise of quantum computing. Quantum computing is both a challenge and an opportunity for financial data security. While it has the potential to disrupt traditional encryption methods, advances in quantum-resistant algorithms are being developed to protect sensitive information. Financial institutions must stay ahead of these technological developments to protect their data from future threats posed by quantum computing power.

6. Conclusion

The rapid development of big data technology has brought unprecedented opportunities to the financial industry but also posed serious challenges. Financial data has become a key asset, but its security management is under pressure from multiple aspects, including data breaches, privacy protection, and compliance. Financial institutions need to remain flexible in a rapidly changing technological and regulatory environment, adopting advanced technological means such as artificial intelligence and machine learning to improve threat detection and response capabilities. In addition, financial institutions must establish comprehensive risk management systems that balance data accessibility with security to ensure the protection of sensitive data. The evolving regulatory environment requires financial institutions to remain compliant across multiple jurisdictions while addressing regulatory challenges posed by emerging technologies such as blockchain and the Internet of Things. In the future, financial data security will be more dependent on technological innovation and globalized regulatory cooperation. By continuously optimizing data governance and security strategies, financial institutions can fully leverage the potential of big data technology to drive the sustainable development of the industry while protecting data security.

Funding

Exploration and Practice of the Application of Blockchain Technology to the Cultivation of Compound Talents under the Background of Free Trade Port (HKJG2023-18)

Disclosure statement

The authors declare no conflict of interest.

References

[1] Goldstein I, Ye M, Spatt C, 2021, Big Data in Finance. The Review of Financial Studies, 34(7): 3213–3225.

[2] Arena F, Pau G, 2020, An Overview of Big Data Analysis. Bulletin of Electrical Engineering and Informatics, 9(4): 1646–1653.

[3] Cao S, Jiang W, Lei L, et al., 2024, Applied AI for Finance and Accounting: Alternative Data and Opportunities. Pacific-Basin Finance Journal, 84, 102307.

[4] Tian X, Han R, Wang L, et al., 2015, Latency Critical Big Data Computing in Finance. The Journal of Finance and Data Science, 1(1): 33–41.

[5] Rubel M, Emran A, Borna R, et al., 2024, AI-Driven Big Data Transformation and Personally Identifiable Information Security in Financial Data: A Systematic Review. Journal of Machine Learning, Data Engineering and Data Science, 1(1): 114–128. https://doi.org/10.70008/jmldeds.v1i01.47

[6] Mhlanga D, 2024, The Role of Big Data in Financial Technology Toward Financial Inclusion. Front Big Data, 7: 1184444. https://doi.org/10.3389/fdata.2024.1184444

[7] Hasan M, Hoque A, Le T, 2023, Big Data-Driven Banking Operations: Opportunities, Challenges, and Data Security Perspectives. FinTech, 2(3): 484–509. https://doi.org/10.3390/fintech2030028

[8] Lin D, 2024, An Analysis of Risk Control in the Financial Sector Using Big Data Technology. Applied and Computational Engineering. 87(1): 167–172.

[9] Ji W, 2023, Research and Analysis of the Security Risk Management Strategy of Big Data Technology in the Financial Industry. Proceedings of the 2023 5th International Conference on Big Data Engineering, 67–72.

[10] Wei R, Yao S, 2021, Enterprise Financial Risk Identification and Information Security Management and Control in Big Data Environment. Mobile Information System, 7188327: 1–6.

[11] Rahmadhani L, Ramadhan M, Rahmani N, 2024, Risk Analysis and Sustainability of Sharia Insurance in Facing the Challenges of the Digital Era. Quantitative Economics and Management Studies, 5(5): 1114–1122.

[12] Chen N, 2023, Data Security Issues and Countermeasure Suggestions for Financial Big Data: A Literature Review. Advances in Economics, Management and Political Sciences, 41: 55–60.

[13] Luo Y, 2021, Financial Data Security Management Method and Edge Computing Platform Based on Intelligent Edge Computing and Big Data. IETE Journal of Research, 69: 5187–5195.

[14] Zhang R, Li J, 2024. Research on Financial Technology Risk Management and Control in the Context of the Big Data Era. Highlights in Business, Economics and Management. 43: 487–493.

[15] Sun C, 2024, Research on Information Security Management and Protection Measures of Financial Enterprises in the Era of Big Data — Take the USA of Industrial and Commercial Bank of China. Journal of Education, Humanities and Social Sciences. 35: 39–44.