Proceedings of the 7th International Conference on Economic Management and Green Development
DOI: 10.54254/2754-1169/41/20232034

Data Security Issues and Countermeasure Suggestions for Financial Big Data: A Literature Review

Ningbo Chen[1,a,*]

[1]*Department of physics, Boya College, Macau University of Science and Technology, Macau, 999078, China*
a. 2009853gk011031@student.must.edu.mo
**corresponding author*

Abstract: Financial Big Data is a contentious topic that needs to be addressed because it is having an increasingly negative impact on people's everyday lives, work habits, and thought patterns. The leakage of financial big data is just one of the issues that financial big data is now dealing with. As a result, the study focus of this work is on the data security problems and solutions related to financial big data. This paper summarizes four main categories of data security issues related to financial big data: attacks on financial big data, data leaks related to financial big data, issues with the reliability of financial big data, and issues with access control related to financial big data. Based on these four problem categories, it searches the literature and organizes the suggested solutions as follows: pay attention to the development of financial data security systems in a big data environment, strengthen education and training, increase the da-ta security awareness of various roles, optimize the processing of big data, and strengthen the storage security of big data by strict user access control. This paper's thought and research also reveal that while financial big data does provide data security issues, it also serves as the primary means of addressing the issue itself. Less research has been done on using financial big data as a countermeasure in and of itself. In the future, we should focus on financial big data itself and explore ways to use financial big data as a countermeasure to data security problems.

Keywords: financial big data, data security issues, countermeasures

1. Introduction

In terms of acquisition, storage, management, and analysis, big data is a type of data gathering that is so massive that it substantially exceeds the capabilities of conventional database software tools. It has four key characteristics: enormous data size, quick data flow, a variety of data types, and poor value density [1]. As the big data era begins, all types of data are rising geometrically, and big data study and application are slowly but surely affecting every aspect of human society. The huge amount of data brings serious challenges to management and also provides great value for utilization. Big data research and applications are slowly permeating every aspect of human society and have a growing impact on everyday routines, work practices, and thought processes.

Undoubtedly a key actor in this data storm is the banking sector, which is one of the most data-intensive industries. The current use of big data in the financial industry has brought a more positive impact, and in the future, a definite development trend is the fusion of big data with the financial

DOI: 10.54254/2754-1169/41/20232034

sector. The notion of financial big data is a new one that has emerged as a result of the combination of big data with the financial sector. Financial big data consists of a variety of derivative data, customer data, operational data, regulatory data, and financial transaction data. Its enormous use value is clear to all. However, with the further deepening of financial data, financial data security issues will become more prominent, such as financial big data being attacked, financial big data being leaked, and a series of problems. If not handled properly will lead to catastrophic consequences [2].

The fusion of networks and reality is becoming more and more visible in the age of big data. In the age of big data, data security concerns are more prominent. And in the financial sector, it is more significant. In this article, we concentrate on the data security concerns brought on by financial big data and provide the appropriate remedies.

The data security issues arising from financial big data summarized in this paper can provide guidance and reference for financial institutions, help them develop effective data security management strategies and measures, guarantee the security and controllability of financial big data, and reduce the adverse consequences caused by related data security issues. This paper provides a comprehensive and systematic summary and analysis of the data security issues of financial big data, summarizes the existing research results and experiences, and provides a basis and direction for future research.

2. The Current Situation of the Use of Financial Big Data

Nowadays, financial big data is used to a high degree in the financial field, and it is widely used mainly in the banking and securities industries.

2.1. Use of Financial Big Data in the Banking Industry

The banking industry should use financial big data to drive its business operations, such as using financial big data for real-time marketing and business development, etc. There are four main areas in which financial big data can be used. First, financial data can be used for customer profiling, second, accurate marketing based on customer profiling, then financial data can be used to assist banks in risk control, and finally, financial data can help banks optimize their operations [3].

2.2. Use of Financial Big Data in the Securities Industry

Financial big data is also widely used in the securities industry, mainly for stock price prediction, customer relationship management, investment analysis, and market environment analysis (see Figure 1). Among them, the use of financial big data for stock price prediction is relatively early, with some investment companies in the UK applying it to real trading in 2011 and achieving some results. Customer relationship management using big data technology mainly involves segmenting customers based on customer information and their various securities transactions, identifying valuable customers and focusing on them, as well as using financial big data to predict possible customer churn and take measures to reduce the churn rate. In the area of investment analysis, financial data is used to analyze the securities investment behavior of customers and provide them with appropriate investment services. In addition, we can also analyze the market environment by monitoring the investments of individual investors to determine the investment climate.

DOI: 10.54254/2754-1169/41/20232034

Figure 1: The use of financial big data in the financial sector.(Source: https://baijiahao.baidu.com/s?id=1681241206715022241&wfr=spider&for=pc.)

3. Data Security Issue of Financial Big Data

Large amounts of financial property information on people and institutions are included in financial data, making the issue of data security for this type of big data extremely crucial. According to the literature that has been published thus far, attacks on financial big data, financial big data leaks, issues with the reliability of financial big data, and issues with access control over financial big data are the four major aspects of data security issues resulting from financial big data that have the biggest impact.

3.1. The Concentration of Financial Big Data Is More Likely to Become the Target of Attack in the Network

In today's big data environment, financial big data has become a big target that is more likely to be noticed. In one sense, the concentration of financial big data means the collection of more massive and sensitive data, and these data are extremely important in the financial field, which makes these data have a high value, so these data will attract many cyber attackers. In one sense, the concentration of financial big data also means that if hackers successfully invade, they will be able to obtain more and more valuable information about finance, which will greatly reduce the cost of hacking and increase the benefit of hackers [2].

3.2. Financial Big Data Leakage

The advancement of the times,a large amount of sensitive financial information is stored in the terminals carried by customers, including their various online banking accounts, passwords, and other key financial data information. The leakage of personal information will promote an increase in the frequency of bank card theft, fraud, extortion, and even threats to personal safety [2].

3.3. Problems in the Trustworthiness of Financial Big Data

Due to issues with data collection, storage, and processing, financial organizations may have inconsistent data. For instance, data for the same consumer may be inconsistent across various systems. Financial institutions may have poor data quality due to problems in the data collection and cleaning process, such as missing data and data errors [4]. Employees of financial institutions may

DOI: 10.54254/2754-1169/41/20232034

mishandle or omit data due to operational errors or negligence. All of these scenarios could compromise the reliability of financial big data.

3.4. Problems in Access Control of Financial Big Data

Big data access control is challenging since it is challenging to foresee the actual authority of each function [5]. Security administrators might not have the necessary industry knowledge to accurately specify the scope of data that users can access, which could make it difficult for financial staff to access the financial data they need. Some financial staff may even be able to access financial data that they are not authorized to access, leading to a certain amount of financial data leakage. A certain amount of financial data leakage may result from this.

4. Countermeasures for Data Security Issues of Financial Big Data

4.1. Pay Attention to the Construction of Financial Data Security Systems in the Big Data Environment

Planning the development of a financial data application requires that the severity of the financial data security situation be effectively recognized from a strategic height, that data be distinguished based on value or degree of confidentiality, that the primary protection objects be clarified, and that the monitoring and management of sensitive and important data be strengthened. [6]. Increase the publicity of the financial data security situation, clarify the key protection areas of financial data, accelerate the research of financial data security technology in the big data environment, cultivate professional talents of data security, and establish and improve the financial data security system [7].

4.2. Strengthen Education and Training to Enhance the Data Security Awareness of Different Roles

Coordinate with all institutions and individuals in the financial market chain to jointly promote data security standards in the financial market and strengthen industry self-monitoring; strengthen communication with regulators, enhance their financial data security standards with the help of public services, and strengthen compliance management; take the initiative to strengthen communication with customers in financial data security and financial data use, and enhance users' data security awareness [8].

4.3. Optimize the Processing Process of Big Data

Ensure that data sources are reliable, data collection methods are compliant, and data cleaning and pre-processing are accurate [9]. Data collection and cleaning are the basis for ensuring the credibility of financial big data, and if there are problems in this step, subsequent analysis and applications will be useless. Establish a secure data storage system to ensure that data are not tampered with, leaked, or lost. Financial big data often contains sensitive information, so data security is an issue that cannot be ignored. And to better supervise and train employees' behavior in data processing.

4.4. Strict User Access Control to Strengthen the Security of Big Data Storage

First, we can deploy network access control technology, define distinct permission levels for large data and users, and carefully regulate access rights depending on the level of secrecy of big data and the various demands of users.

Secondly, through the unified authentication registration and permission control technology of single sign-on, the application security of big data can be ensured to a certain extent [10].

DOI: 10.54254/2754-1169/41/20232034

In summary, the existing literature is relatively complete for the countermeasures of data security issues arising from financial big data, but most of the countermeasures are to use external forces to protect financial big data. Financial big data brings data security problems, but it is also an important means to solve the problem itself. Existing technologies based on financial big data can be used to prevent and solve data security problems. For example, data release anonymity technology [11]: The fundamental technique and method for achieving privacy protection for structured data in big data, which is still in the development and enhancement stage, is data release anonymity protection. Watermarking data technologies [12]: Digital watermarking is the process of imperceptibly incorporating identifiable information into the data carrier without obstructing its use. These large financial data-based technology solutions can efficiently avoid and address data security issues.

5. Conclusion

This paper compiled the four major categories of financial big data security issues from the literature: financial big data breaches, financial big data leaks, potential issues with financial big data's reliability, and potential issues with financial big data's access control. And from these four categories of financial big data security problems and literature, four countermeasures are derived to solve these four categories of data security problems. In addition to these four countermeasures, this paper also finds that financial big data does bring data security problems, but it is also an important means to solve the problem itself, and for a significant portion of data security problems, financial big data itself as a means to solve the problem more efficiently. Financial big data's data security issues can be effectively solved by financial organizations using technologies built on top of it.

This paper advances understanding of data security issues related to financial big data among researchers, deepens and broadens research perspectives, and provides a foundation and a direction for some future research on how to handle the increasingly complex data security issues related to financial big data as well as how to use financial big data itself to address data security issues. This kind of research, it can focus on the technologies based on financial big data, which can solve data security problems with lower human and material costs as well as better results.

Future research can explore the establishment of a multi-level data security management system, including network security, physical security, application security, etc., to guarantee the security of financial big data in all aspects.

References

[1] *Zhang, B.: The application of big data technology in the financial field and its regulation. Journal of Beijing Vocational College of Economics and Management (01), 16-23+33 (2020).*
[2] *Lu, S.; Financial big data security risks and countermeasures. Financial technology era (01),68-69 (2015).*
[3] *Zhang, H. J.: Research on the application of big data in the financial field. Think Tank Times 8(34),175+180 (2018).*
[4] *Wang, J. J.: Challenges and considerations of financial data security under the new situation. Financial technology era (08),53-54+58 (2020).*
[5] *Feng, D. G., Zhang M., Li H.: Big data security and privacy protection. Journal of Computer Science (01), 246-258 (2014).*
[6] *Wu, X. Q., Zhang, Z. N.: Research and practical suggestions on data security construction model for financial industry. China financial computer 2(12),86-87 (2022).*
[7] *Dong, L. G.: Building data security system to help efficient application of financial data. Financial Electronic (07),39-40 (2021).*
[8] *Dun, H. C.: Thinking about data security under the marketization environment of data elements. China Financial Computer (09),10-13 (2020).*
[9] *Zhou, W., Liu Z.: Data security issues and countermeasures in the era of intelligence. Digital design (11),10-11 (2017).*
[10] *Zhang, D. E., Zhou, Y.: A few thoughts on data security in the big data environment. Cyberspace security (08),17-20 (2016).*

DOI: 10.54254/2754-1169/41/20232034

[11] Sweeney L.: A model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems 10 (5) ,557-570 (2002).

[12] Pease A., Niles I., Li J.: The suggested upper merged ontology: A large ontology for the semantic web and its applications//Proceedings of the AAAI-2002 Workshop on Ontologies and the Semantic Web. Edmonton, Canada1-4 (2002).