J. COMBIN. MATH. COMBIN. COMPUT. 127b (2025) 8419--8432

Journal of Combinatorial Mathematics and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Artificial Intelligence-based Financial Big Data Information Security and Local Risk Prevention and Control

Minyi Zheng[1,✉]

[1] College of Economics and Information, Zhejiang Tongji Vocational College of Science and Technology, Hangzhou, Zhejiang, 311231, China

ABSTRACT

As a new product of artificial intelligence, big data is widely used in daily life. Due to its appearance, people's lives are more convenient and efficient, but at the same time, there are certain security risks, namely the leakage of private information, especially the financial information problem brought about by financial informatization has a more serious leakage problem. In order to effectively reduce the problems caused by the leakage of financial information privacy, this paper attempted to establish a model of related protection measures for financial big data information security by establishing a three-dimensional encrypted information model of big data or by using differential privacy method and using their own. The three-dimensional encrypted information model of big data overcame the defect that financial information is easy to be broken, while the differential privacy model overcame the defect of inaccurate protection of financial information, both of which can play a better protective role in different applications. The experimental results showed that in the process of accessing financial data information, with the increase of access frequency, the number of sensitive locations changes from 40 to 46. This also meat that a non-sensitive position becomes a sensitive position, which blurs the original sensitive position and achieves the effect of protecting the real sensitive position.

Keywords: Artificial Intelligence, Big Data Era, Financial Information Security, Differential Privacy Model

1. Introduction

Artificial Intelligence refers to letting machines imitate the way humans think and learn, and then intelligently process all kinds of language, images, audio, video and other information. Its foundation covers linguistics, mathematics, psychology, neuroscience, cybernetics and other disciplines, and involves various technologies and algorithms such as natural language processing, computer vision,

✉ Corresponding author.
E-mail address: 13575798396@163.com (M. Zheng).
Received 25 March 2024; Revised 05 June 2024; Accepted 15 December 2024; Published Online 16 April 2025.
DOI: 10.61091/jcmcc127b-460

machine learning, deep learning, etc. [1-2]. Currently, AI has achieved a wide range of applications in various fields such as healthcare, manufacturing, transportation, education, and finance [3-4].

Financial information security risk control refers to the management process of identifying, evaluating, supervising, and controlling all types of potential risks that may be encountered in the process of capital operation in order to minimize all types of risks in the business activities of financial institutions [5-6]. This process is implemented to safeguard the interests of financial institutions from being jeopardized. As a key link in the financial industry, financial information security risk control has a significant impact on the stability of the financial market and the operation of financial institutions [7-9].

Artificial Intelligence utilizes technological advantages to bring intelligent risk control, intelligent investment and other functions to Internet finance, providing efficient financial services for a large number of long-tail customers and promoting the implementation of financial inclusion. However, AI may cause information security risks in the collection, transmission, storage and analysis of Internet financial data [10-11]. On the other hand, AI technology can also be applied to the field of information security of Internet finance, innovate the information security technology of Internet finance, and help improve the level of information security of Internet finance [12-13]. In the era of artificial intelligence, a large number of financial products and services such as payment and settlement, crowdfunding financing, online lending P2P, product sales, financial consulting and other financial products and services are realized through the network, so that the degree of information asymmetry between the consumers and providers of financial products and services is greatly reduced [14-15]. Fast human-computer interaction is carried out based on natural language understanding that includes speech recognition, semantic understanding, and intent recognition, which can accurately analyze scenarios and quickly identify responses. Providing authenticity of transaction behavior and credibility of credit through big data analysis, customer identification and classification based on data mining become the main means of risk management, and dynamic, real-time monitoring rather than retrospective evaluation after the fact will become a regular part of risk management. Various cloud platforms built based on distributed resource management, virtualization and other technologies provide cloud storage, cloud computing services and financial-level disaster recovery capabilities for Internet finance [16-18].

Intelligent risk control carries out timely and effective identification and early warning of personal credit risk, integrates enterprise business information, compliance, and relationship genealogy to improve the enterprise credit rating status, reduces the cost of risk control, improves the efficiency of credit collection, and realizes the full automation and intelligence of pre-loan audit, loan monitoring and post-loan management, improves the breadth and precision of personal credit collection, and improves the credit system of small and micro enterprises [19-20].

The mainstream research direction of artificial intelligence technology in the field of finance mainly includes investment portfolio, risk prediction, operational efficiency improvement, and customer service, and researchers mainly use the literature review method, quantitative and qualitative data analysis method to conduct related research. Literature [21] reviewed the research literature on AI integration in finance, and the research topics mainly include portfolio construction and investment behavior prediction, as well as financial distress analysis, etc. The research provides an important reference for further research on AI in finance. Literature [22] affirms the positive role played by AI in the field of e-commerce and finance, including improving operational efficiency, reducing operating costs and assisting in the development of new customers, etc., and believes that there is a need for in-depth investigation in the areas of financial fraud detection, portfolio management, and so on. Literature [23] provides an in-depth overview of the meaning and underlying logic of artificial intelligence technology, discusses its practice in the supervision of the financial system, as well as the advantages and disadvantages, and makes a positive contribution to the construction of informationization and intelligence in the financial field. Literature [24] describes the fact that banks and other financial institutions are investing in and developing AI technology, and discusses the advantages and disadvantages of AI technology, including creating a crisis of confidence in financial consumer investors and assisting in financial regulation. Literature [25] systematically reviews research on sustainable finance enabled by machine learning and big data technologies, covering topics such as green finance, sustainable finance, investment governance, and climate finance, and gives recommendations based on the analysis, including the development of unified financial sustainability policies and frameworks to deal with the problem of corporate greenwashing, as well as the adoption of advanced technologies such as artificial intelligence to facilitate sustainable finance. Literature [26] reviewed the effect of practicing AI and machine learning technologies in the financial field, and found that the application of AI and ML in the areas of stock price prediction, bankruptcy prediction, and anti-money laundering showed an upward trend, and the study provided effective guidance for practitioners in the financial field in the use of AI and machine learning technologies.

Research around financial risk management covers, risk research prediction and assessment quantification, risk occurrence mechanisms and impacts, and how to avoid and control financial risks. Many researchers have conducted extensive studies on the above topics from the dimensions of information technology tools, financial risk management prediction methods, and financial institutional systems. Literature [27] reviewed the research on the application of machine learning in bank risk management, and based on the results of the study, it was learned that machine learning technology is mainly applied to credit risk, market risk and liquidity risk management, which is still in the primary stage of development in the field of bank risk management, and there is still a huge space for development. Literature [28] proposes an analytical prediction model based on deep learning technology to achieve the prediction of high-risk financial behaviors of financial traders, and confirms the reliability of the proposed model through numerical evaluation tests, which can be used to improve the financial risk management capability of financial institutions. Literature [29] conceptualized a Multi-Criteria Decision Making (MCDM) strategy to achieve prediction of credit risk and bankruptcy risk by considering multiple KPIs and evaluated the imbalance classifiers in financial imbalance databases, and pointed out that TOPSIS, which combines six evaluation criteria, performs best in evaluating the imbalance classifiers. Literature [30] emphasizes the important role of digital financial literacy in helping investors avoid financial risks and fraud risks, and provides an in-depth analysis of digital financial education strategies for investors' digital financial literacy as well as financial literacy assessment tools developed by G20 countries. Literature [31] reveals that children's financial investment behaviors are correlated with parental behaviors and the environment, in which the amount of children's upbringing financial investment is significantly correlated with portfolio volatility, which confirms that financial risk-taking is determined by the environment. Literature [32] tries to build an equilibrium risk-sharing model in countries with different levels of financial development, and analyzes that financially developed countries bear more financial risks because their financial intermediaries have stronger financing capabilities, and during the global financial crisis, the RMB as an appreciated reserve currency has strong risk-hedging capabilities.

In the past, the protection of financial information mostly relied on external detection, rather than strengthening the security of the system itself. By referring to the three-dimensional encryption model and the differential privacy model, self-prevention can prevent the risk of financial information being leaked. In this paper, the financial information protection strategy based on the three-dimensional encryption model and the differential privacy mechanism was used to reduce the risk of financial information leakage. The innovations are: (1) Although information security issues have been common, most people focus on personal information security issues, and few people focus on financial information security issues; (2) For the problem of financial information leakage, the differential privacy model and the three-dimensional storage encryption method are not only widely used and accurate in calculating data, but also can maximize the risk of financial information leakage.

2. Artificial Intelligence Algorithms and Financial Information Privacy Protection Methods

2.1. AI Algorithm of PageRank

At present, most of the development of artificial intelligence is to earn more benefits, some are achieved by improving work efficiency, and some are by collecting user information, so as to use their personal information for their own personal gain without their knowledge. Figure 1 showed the general process of artificial intelligence collecting user information.

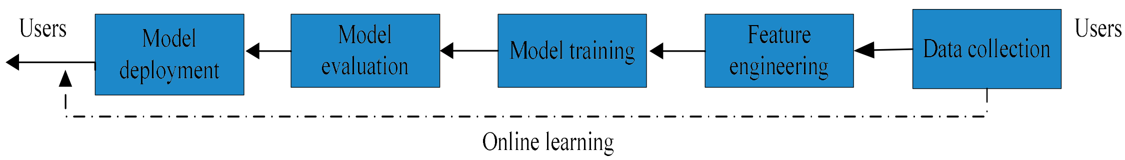

Fig. 1. The process of artificial intelligence collecting user information

Due to the continuous improvement of the algorithm, the Page Rank algorithm is divided into the traditional Page rank algorithm and the Enhanced-RatioRank algorithm which is improved on the traditional Pagerank algorithm. The traditional PageRank algorithm mainly evaluates the importance of some specific web pages relative to other web pages in the search engine. The mathematical formula of the traditional PageRank algorithm is as follows:

$$PR(u) = (1-d) + d \sum_{v \in B(u)} \frac{PR(v)}{N_v} \tag{1}$$

The matrix form is as follows:

$$P = (1-d)e + d\, A^T P \tag{2}$$

In the formula, d, B(u), and N_v represent the damping coefficient, the set of links to the web page u, and the out-degree of the web page v respectively. The existence of the damping coefficient is to reduce the probability of clicking on the link.

Weighted PageRank can finally get the Enhanced-RatioRank algorithm by combining VOL (Visits of Links). The mathematical formula of the algorithm is as follows:

$$WPR_{vol}(u) = (1-d) + d \sum_{v \in B(u)} \frac{V_u W^{in}_{(v,u)} WPR_{vol}(v)}{TL(v)} \tag{3}$$

In the formula, $W^{in}_{v,u}$, V_u, TL(v) respectively refer to the link-in weight factor, the number of clicks on the link from page v to page u, and the number of clicks on all links related to page v. In order to remove the problem of topic drift in the Weighted PageRank algorithm, the RatioRank algorithm is obtained through improvement. The mathematical formula of the algorithm is as follows:

$$RR(u) = (1-d) + d \sum_{v \in B(u)} \frac{(V_u x W^{in}_{v,u} + y W^{out}_{v,u} RR(v))}{} \tag{4}$$

Among them, u and v respectively represent the weight ratio of the chain in weight factor and the chain out weight factor, u、$v \in [0,1]$ and $u + v = 1(u > v)$.

It has been proved by many experiments that on the basis of the algorithm of formula (4), when the page sorting effect reaches the best state, u=0.76, y=0.24. The mathematical formula of the algorithm is as follows:

$$ER(u) = (1-d) + \sum_{v \in B(u)} \frac{Vu0.76W^{in}_{v,u} + 0.24W^{out}_{v,u} ER(v)}{TL(v)} \tag{5}$$

Among them, the calculation formulas of $W^{in}_{(v,u)}$ and $W^{out}_{(v,u)}$ are as follows:

$$W^{in}_{(v,u)} = \frac{I_u}{P \in O(v)} I_p \tag{6}$$

$$W^{out}_{v,u} = \frac{O_u}{P \in O(v)} O_p \tag{7}$$

Among them, I_u is the in-degree of web page u, O_u is the out-degree of web page U, and O(v) is the set of outgoing web pages of web page v.

2.2. Three-Dimensional Encrypted Storage of Big Data Information

The formula for constructing big data information is:

$$\mathrm{SLM}(u_1, v_1) = F_rT_\lambda, Z_3\{ F_rT_\lambda, Z_2\{ F_rT_\lambda, Z_1\{ C(u_1, v_1) \} \times A(u_2, v_2) \} \cdot S(u_3, v_3) \} \tag{8}$$

$$Q(u_1, v_1) = \mathrm{SLM}(u_1, v_1)/\mathrm{SLM}(u_1, v_1) \tag{9}$$

Among them, $F_rT_\lambda\{\ \}$ is the diffraction model; $C(u_1,v_1), A(u_1,v_1), S(u_1,v_1)$ represents the three points in the space represented by the three-dimensional function.

In order to obtain the calculation formula of big data three-dimensional information $R_0(u_0,v_0)$, $R_1(u_1,v_1)$ and $R_2(u_2,v_2)$ was introduced, which represent the first information and the next information respectively. $R_0(u_0,v_0)$ represents the amplitude. At the same time, a plane wave is used as a reference during the calculation. Its formula is as follows:

$$R_0(u_0, v_0) = F_rT_\lambda, zII \left\{ \left\{ F_rT_\lambda, zI \left\{ \exp\left[jQ(u_i, v_i) \right] \times \exp\left[jR_1(u_i, v_i) \right] \right\} \times \exp\left[jR_2(u_n, v_n) \right] \right\} \tag{10}$$

Representing the diffraction transformation as $F_rT_\lambda, zII\{\ \}$, the inverse transformation operation can be realized, and the process is as follows:

$$\mathrm{DeSLM}(u_i, v_i) = IF_rT_\lambda, zI \left\{ IF_rT_\lambda, zII \times \left\{ \exp\left[jR_0(u_0, v_0) \right] \times \exp\left[-jR2(u_n, v_n) \right] \right\} \times \exp\left[-jR1(u_i, v_i) \right] \right\} \tag{11}$$

After a series of inverse Fresnel transforms, the decrypted three-dimensional information $DeCAS(u,v,w)$ can be obtained, that is, the decrypted two-dimensional function set $\{DeC(u_1,v_1), DeA(u_2,v_2), DeS(u_3,v_3)\}$:

$$DeC(u_1, v_1) = IF_rT_\lambda, z1\{DeSLM(u_i, v_i)\} \tag{12}$$

$$DeA(u_2, v_2) = IF_rT_\lambda, z2\{DeSLM(u_i, v_i)\} \tag{13}$$

$$DeS(u_3, v_3) = IF_rT_\lambda, z3\{DeSLM(u_i, v_i)\} \tag{14}$$

2.3. Differential Privacy Method

1) Definition. The basic idea of differential privacy is to maximize the availability of database queries, while maximizing the protection of personal privacy, financial information privacy or other privacy in the database from being leaked. Figure 2 is a schematic diagram of the curve of user privacy leakage risk:

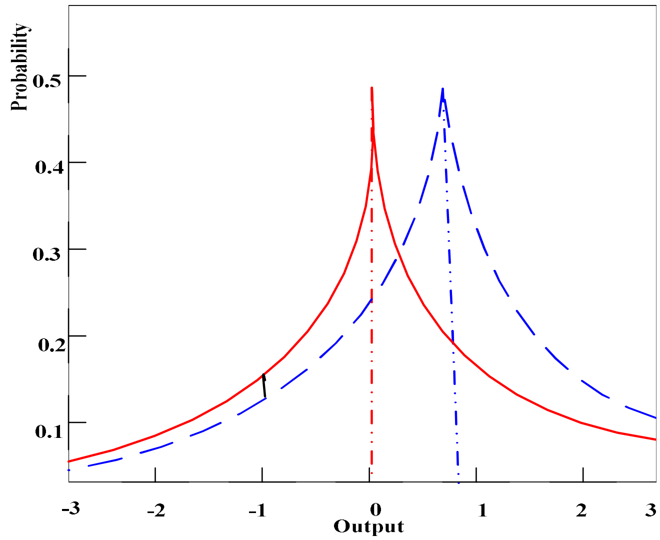

Fig. 2. Privacy Breach Risk Curve

Supposing there is a random algorithm N, C is the set of all possible output results of N, and $\Pr[\ ]$ represents the probability. The specific constraints are as follows:

$$\Pr[N(D) \in C] \le e^{\varepsilon} \Pr[N(d) \in C] \tag{15}$$

Or:

$$\Pr[N(D) \in C] \le e^{\varepsilon} \Pr[N(d) \in C] + \theta \tag{16}$$

$$e^{-\theta} \le \frac{P(N(u) \in C)}{P(N(v) \in C)} \le e^{\theta} \tag{17}$$

Among them θ is the differential privacy budget.

2) Implementation Mechanism. Differential privacy mainly realizes the protection of user privacy information by introducing relevant mechanisms, and then applying this mechanism to noise. In this paper, the Laplacian mechanism is used to debug the size of the noise. At the same time, differential privacy also includes: function sensitivity (global sensitivity, partial sensitivity and smooth sensitivity) and composition properties (sequence composition and parallel composition). Figure 3 illustrates the specific use of these two properties:

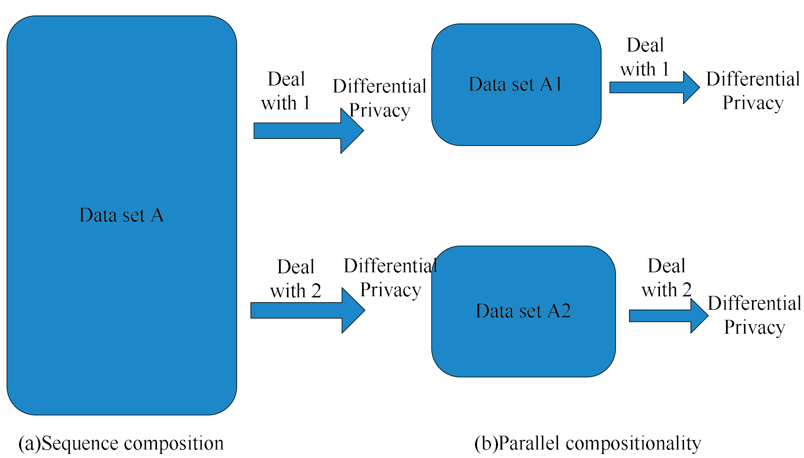

Fig. 3. Sequence and Parallel Compositionality

(1) Global Sensitivity. The global sensitivity is defined as follows:

$$S(f)=\max_{D,D'}\left\|f(D)-f(D')\right\|_1 \tag{18}$$

Among them D is a dataset, R is the return result of the query function, and $\left\|f(D)-f(D')\right\|_1$ is the Manhattan distance between f(D) and f(D').

(2) Local Sensitivity. Roughly the same as the global sensitivity rough function definition, its local sensitivity is defined as follows:

$$LS_f(D)=\max_{D}\left\|f(D)-f(D')\right\|_1 \tag{19}$$

(3) Smooth Sensitivity. For a β >0, the β-smooth sensitivity of a query function f is:

$$S_f^*(D)=\max_{y\in D^n}\left\{LS_f(y)\times e^{-\beta\times d(D,y)}\right\} \tag{20}$$

Among them y is an arbitrary dataset with the same dimension as the given dataset D, and the function d returns the number of distinct elements in datasets D and y.

(4) Laplace Mechanism. Given a dataset G and a query function $f:G\rightarrow R^d$ with a sensitivity of Δf, then the algorithm A(G)=f(G)+X satisfies θ-differential privacy. Among them $X\sim Lap(\frac{\triangle f}{\theta})$, which is the random noise obeying the Laplace distribution of parameter $\frac{\triangle f}{\theta}$.

3. Information Security and Risk Experiment Design and Results

3.1. Financial Information Protection Based on Three-dimensional Encrypted Storage of Big Data Information

1) The process of encryption and decryption. Both encryption and decryption refer to the process of processing information, but decryption is the reverse operation of encryption. For encryption, only the user who has entered the correct password in the process can access the information, and other users can either not see the information at all, or see the information completely garbled. Therefore, the leakage of financial data can be protected to a certain extent by means of encryption. Figure 4 shows the specific process of encryption and decryption:

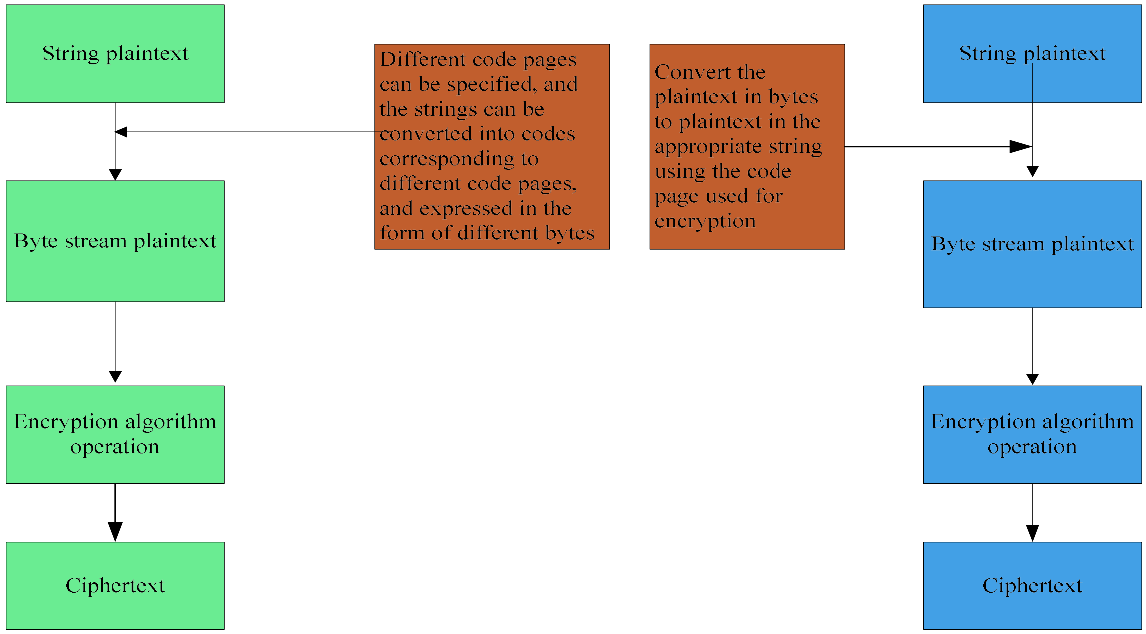

Fig. 4. The process of data encryption and decryption

2) Experimental analysis based on three-dimensional information storage method:

(1) Big data security performance verification. On the basis of the exact same experimental conditions, the two methods were tested for 5 times respectively, and the experimental results of the information security comparison were obtained as shown in Figure 5. By comparison, it can be seen that the security performance of the three-dimensional storage encryption method in the process of storing big data information is always stable at more than 90%. However, the current storage method is always below 80%, and the fluctuation range is obvious.

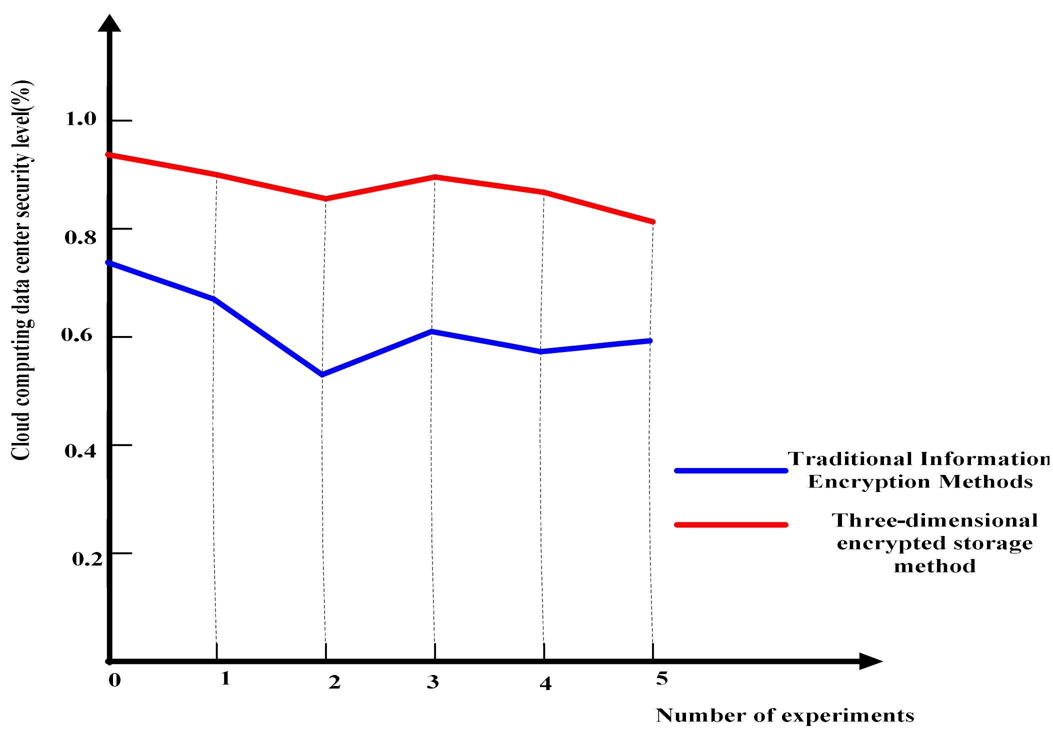

Fig. 5. Comparison of safety test results

(2) Data hiding degree comparison. In the above experiments, the data hiding degree with different number of users was recorded. According to the data comparison results in Table 1, compared with the traditional encryption method, the data hiding degree of the three-dimensional storage encryption method is higher, so it can be seen that this method can be applied to financial information.

From the above security performance and data hiding degree, it can be seen that the three-dimensional storage encryption method can significantly improve the security index of information. Therefore, it can be better applied to the prevention and control of financial information security risks.

Table 1. Comparison of data hiding degree

Number of Users	Current Method Hiding/%	The Hidden Degree of this Method (%)
200	74.46	90.98
400	79.73	93.28
600	80.19	92.67
800	81.08	94.59

3.2. Financial Information Privacy Protection Scheme Based on Differential Privacy Method

This paper mainly uses the timeliness of the algorithm (The time to build the financial information search tree, the time to update the financial information search tree and the amount of data extracted per unit time) and the utility of the algorithm (Data accuracy and data protection) to evaluate the quality of the algorithm, so that the differential privacy method can be used in the privacy protection of financial information. The premise of the algorithm is to set the relevant parameters, such as Table 2 is the experimental parameter settings:

Table 2. Parameter settings

Parameter	Value
k	30 50 70 90 110 130 150 170 190 300 500 1000
θ	0.01 0.015 0.02 0.025 0.03 0.0.35 0.04 0.045 0.1 0.5 0.75 1.0 1.2 1.45 1.65 1.85
Position	1 2 3 4 5
sequence	40 20 25 0 20

1) Timeliness analysis. In order to draw relevant conclusions, the timeliness of this experiment will be from building a financial information search tree. The three aspects of updating the financial port information search tree and the efficiency of extracting financial information data are analyzed, and the corresponding results are obtained in Table 3.

Among them, n represents the mode; t1 represents the time of the financial information search tree; t2 represents the time to update the financial information search tree. It can be seen from Table 3 that regardless of the value of the pattern data, the efficiency of establishing and updating financial information is relatively higher.

Table 3. Time to build and update search tree for financial information

n	t1/s	t2/n/s
16	0.000 000 15	103180
32	0.000 000 25	10385
64	0.000 000 36	103195
128	0.000 000 49	103140

256	0.000 00125	103080
512	0.000 00129	103085
1024	0.000 001 35	103095

Table 4 shows the efficiency of extracting location data (the amount of financial information data extracted per unit time), where θ_1 represents the privacy budget. Through the above experimental results, it can be concluded that the time to build the financial information search tree and update the financial information search tree is very fast, which means that the extraction efficiency of financial information data is high.

It can be seen from Table 4 that θ_1 is inversely proportional to the degree of privacy protection. The greater the value of θ_1, the greater the number of extractions per unit time, and the greater the efficiency of financial information data extraction.

Table 4. Financial Information Data Extraction Efficiency

	θ_1					
k	0.02	0.02	0.2	0.6	1.2	1.8
quantity	3120	4560	5789	12560	35890	78962
efficiency	3.12%	4.56%	5.79%	1.26%	35.89%	78.96%

2) Utility analysis. In the three datasets of this experiment, insensitive locations are represented by purple dots, and sensitive locations are represented by green dots. If the visit frequency is p, then p is the boundary between sensitive and non-sensitive locations. When the access frequency reaches p, the location will be a sensitive location, otherwise the opposite. The experimental results are shown in Figures 6-8. Table 5 shows the statistical results of the experimental usefulness.

Table 5. Statistical Results in Different Modes

Number of patterns	Before experiment		After the experiment	
	Number of purple dots	Number of green dots	Number of purple dots	Number of green dots
50	35	15	32	18
100	74	26	62	38
150	110	40	104	46

As can be seen from Figure 6 and Figure 7, the green dots, that is, sensitive financial information, have been increased accordingly after mode protection. When sensitive financial information increases in value, it will be more difficult for information theft to find the real sensitive location (financial information) before protection, thus covering the original sensitive location and achieving the purpose of truly protecting financial information.

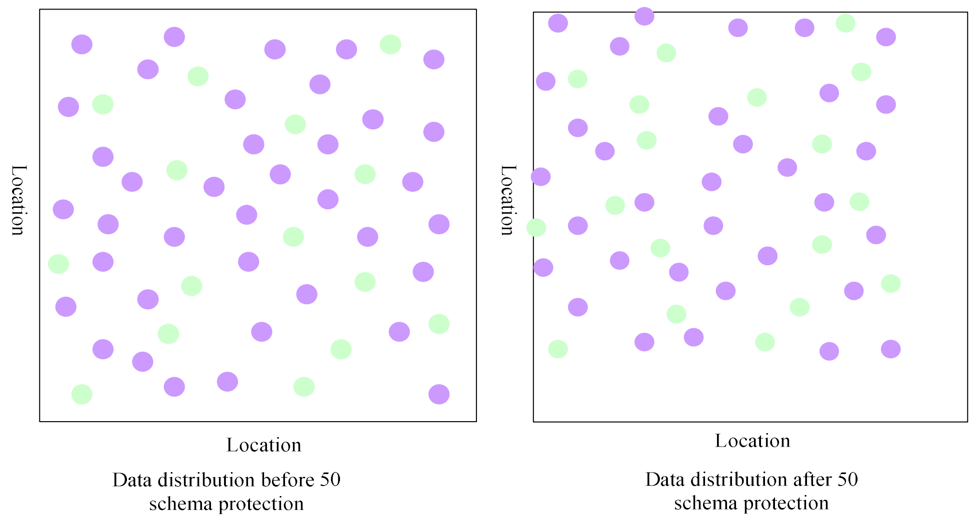

Fig. 6. Data distribution before and after 50 schema protection

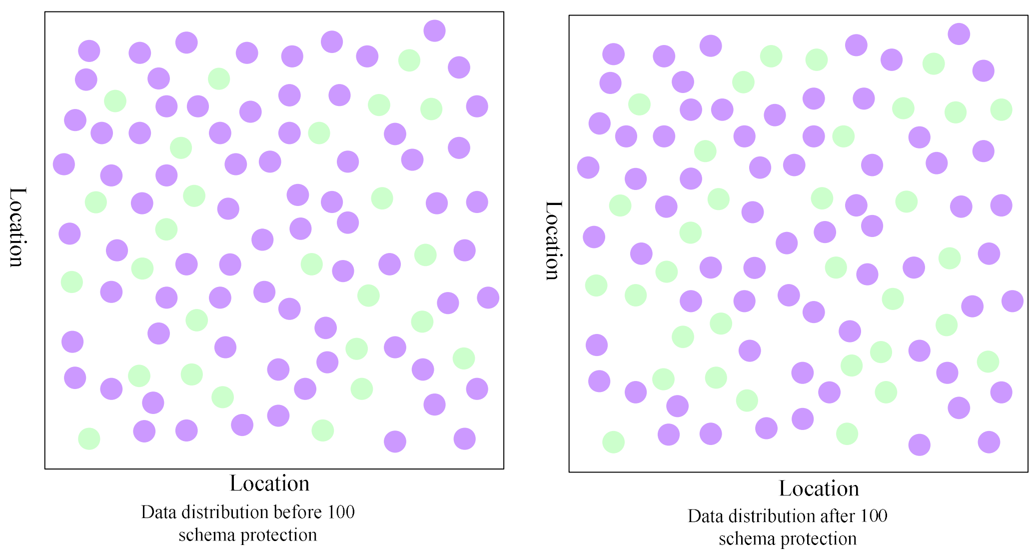

Fig. 7. Data distribution before and after 100-pattern protection

Figure 8 shows that the degree of change of the frequent pattern of 150 positions is the same as that of Figure 6 and Figure 7. After the mode protection, the green dots have changed from 40 at the beginning to 46. From the changes of the above data points, it can be seen that when the frequency of access increases, the actual frequency of access to each big data financial information data will also increase, which also leads to some non-sensitive locations becoming sensitive locations. The sensitive location will also be covered, which also achieves the function of protecting the actual sensitive location.

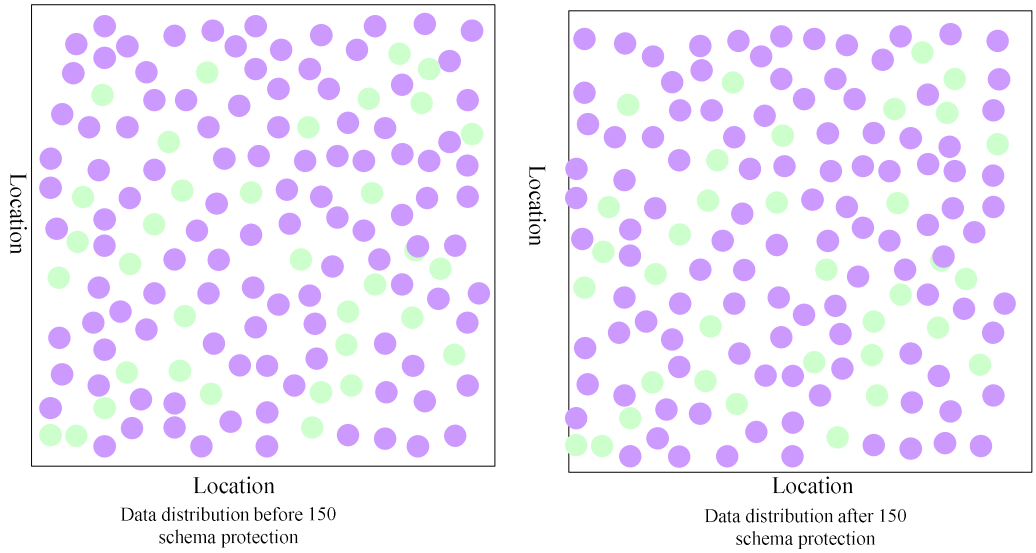

Fig. 8. Data distribution before and after 150 schema protection

4. Conclusions

This paper mainly applies the three-dimensional encrypted information model and differential privacy model to financial information protection in detail. First, this paper briefly introduces a representative algorithm of artificial intelligence, namely the Pagerank algorithm, and analyzes how the algorithm steals financial information. Secondly, it introduces the specific algorithm formulas of the three-dimensional encrypted information model and the differential privacy model in detail. Finally, the accuracy of the two models for financial information protection is analyzed separately, which proves that the models are effective in protecting financial information. Although the two models play a certain role in the protection of financial information, due to the complex structure and algorithm of the three-dimensional encrypted information model in application, the required database is too large, and someone needs to continuously optimize the password in the later stage, so it requires a lot of human and financial resources. The differential privacy method is more complicated and difficult to apply. However, compared with the theft of financial information, these defects are acceptable. It is believed that in the near future, through continuous optimization of the existing model, the existing defects will definitely be overcome.

References

[1] Yang, K., Shi, Y., Zhou, Y., Yang, Z., Fu, L., & Chen, W. (2020). Federated machine learning for intelligent IoT via reconfigurable intelligent surface. IEEE network, 34(5), 16-22.

[2] Battiston, S., Mandel, A., Monasterolo, I., Schütze, F., & Visentin, G. (2017). A climate stress-test of the financial system. Nature Climate Change, 7(4), 283-288.

[3] Preece, A. (2018). Asking 'Why'in AI: Explainability of intelligent systems–perspectives and challenges. Intelligent Systems in Accounting, Finance and Management, 25(2), 63-72.

[4] Sarker, I. H. (2022). AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN Computer Science, 3(2), 158.

[5] Baruník, J., & Křehlík, T. (2018). Measuring the frequency dynamics of financial connectedness and systemic risk. Journal of Financial Econometrics, 16(2), 271-296.

[6] Saunders, A., Cornett, M. M., & Erhemjamts, O. (2021). Financial institutions management: A risk

management approach. McGraw-Hill.

[7] Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund.

[8] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE access, 8, 25579-25587.

[9] Fichtner, J., Heemskerk, E. M., & Garcia-Bernardo, J. (2017). Hidden power of the Big Three? Passive index funds, re-concentration of corporate ownership, and new financial risk. Business and politics, 19(2), 298-326.

[10] Giudici, P. (2018). Fintech risk management: A research challenge for artificial intelligence in finance. Frontiers in Artificial Intelligence, 1, 1.

[11] Guiso, L., Sapienza, P., & Zingales, L. (2018). Time varying risk aversion. Journal of Financial Economics, 128(3), 403-421.

[12] Cao, L. (2022). Ai in finance: challenges, techniques, and opportunities. ACM Computing Surveys (CSUR), 55(3), 1-38.

[13] Demirgüç-Kunt, A., & Singer, D. (2017). Financial inclusion and inclusive growth: A review of recent empirical evidence. World bank policy research working paper, (8040).

[14] Chintalapati, S., & Pandey, S. K. (2022). Artificial intelligence in marketing: A systematic literature review. International Journal of Market Research, 64(1), 38-68.

[15] Singer, D. A. (2017). Regulating capital: Setting standards for the international financial system. Cornell University Press.

[16] Dowling, M., & Lucey, B. (2023). ChatGPT for (finance) research: The Bananarama conjecture. Finance Research Letters, 53, 103662.

[17] Chance, D. M., & Brooks, R. (2021). An introduction to derivatives and risk management. South-Western, Cengage Learning.

[18] Arslanian, H., & Fischer, F. (2019). The future of finance: The impact of FinTech, AI, and crypto on financial services. Springer.

[19] Schildberg-Hörisch, H. (2018). Are risk preferences stable?. Journal of Economic Perspectives, 32(2), 135-154.

[20] Mogaji, E., Soetan, T. O., & Kieu, T. A. (2020). The implications of artificial intelligence on the digital marketing of financial services to vulnerable customers. Australasian Marketing Journal, j-ausmj.

[21] Goodell, J. W., Kumar, S., Lim, W. M., & Pattnaik, D. (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. Journal of Behavioral and Experimental Finance, 32, 100577.

[22] Pallathadka, H., Ramirez-Asis, E. H., Loli-Poma, T. P., Kaliyaperumal, K., Ventayen, R. J. M., & Naved, M. (2023). Applications of artificial intelligence in business management, e-commerce and finance. Materials Today: Proceedings, 80, 2610-2613.

[23] Wall, L. D. (2018). Some financial regulatory implications of artificial intelligence. Journal of Economics and Business, 100, 55-63.

[24] Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector. Information & Communications Technology Law, 27(3), 267-283.

[25] Kumar, S., Sharma, D., Rao, S., Lim, W. M., & Mangla, S. K. (2022). Past, present, and future of sustainable

finance: insights from big data analytics through machine learning of scholarly research. Annals of Operations Research, 1-44.

[26] Ahmed, S., Alshater, M. M., El Ammari, A., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. Research in International Business and Finance, 61, 101646.

[27] Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. Risks, 7(1), 29.

[28] Xu, K., Wu, Y., Li, Z., Zhang, R., & Feng, Z. (2024). Investigating financial risk behavior prediction using deep learning and big data. International Journal of Innovative Research in Engineering and Management, 11(3), 77-81.

[29] Song, Y., & Peng, Y. (2019). A MCDM-based evaluation approach for imbalanced classification methods in financial risk prediction. IEEE Access, 7, 84897-84906.

[30] Morgan, P. J., Huang, B., & Trinh, L. Q. (2019). The need to promote digital financial literacy for the digital age. IN THE DIGITAL AGE.

[31] Black, S. E., Devereux, P. J., Lundborg, P., & Majlesi, K. (2017). On the origins of risk - taking in financial markets. The Journal of Finance, 72(5), 2229-2278.

[32] Maggiori, M. (2017). Financial intermediation, international risk sharing, and reserve currencies. American Economic Review, 107(10), 3038-3071.