WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n3.27
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on the Application of Differential Privacy Algorithm in Financial AI Security Risk Prevention and Response

Kaijie Qin

School of Computer Science and Information Technology, Shanghai Institute of Technology, Shanghai, 201418, China

ABSTRACT

This research focuses on the field of financial AI security, and discusses the role of cryptographic algorithms in risk prevention and response. With the wide application of artificial intelligence technology, the financial industry is facing unprecedented security challenges. This research aims to reveal potential AI security risks in the financial system and propose solutions based on cryptographic algorithms to enhance the security and stability of the financial system.

KEYWORDS

Differential privacy; Financial AI security; Personal privacy; Data protection; Noise addition; Precision control; Laplacian mechanism; Native differential privacy; Homomorphic encryption; Data analysis

1. INTRODUCTION

This research aims to solve the problem of personal privacy and data protection in the field of AI financial security. By proposing more accurate precision control methods, developing noise addition strategies that adapt to different data characteristics, and conducting in-depth experimental research, the effectiveness of different noise mechanisms is evaluated. I hope to combine the knowledge of data science, information theory and applied mathematics to provide innovative privacy protection solutions for the field of financial AI, with a view to achieving the dual goals of protecting privacy and improving the accuracy of data analysis.

2. AN OVERVIEW OF RELEVANT THEORIES AND TECHNOLOGIES

2.1. Basis of Differential Privacy

Differential privacy, as a mathematical framework, is designed to ensure that individuals' information is not disclosed in the results of statistical database queries. Its core is to obscure individual data by introducing a certain degree of randomness, so that even if an attacker has all the information except a record, it is impossible to accurately determine whether the record exists in the database. Differential privacy typically uses techniques such as noise addition and data sampling. For a random algorithm M and any two adjacent data sets D and D', where proximity means they differ on one record, differential privacy can be defined as: $\Pr[M(D) \in S] \leq \mathrm{e} \Pr[M(D') \in S] + \delta$. Where, ϵ is the privacy budget, which controls the intensity of privacy protection; δ is a very small probability value that deals with the imprecision caused by ϵ; S is the set of output results of the algorithm.

2.2. Security Risk Analysis in Financial AI

In the field of financial AI, the prevention and response of security risks has become an increasingly prominent research topic. With the development of technology, financial institutions are increasingly relying on these advanced technologies to improve the efficiency of service to users, optimize the ability to manage risks, and enhance the customer experience. However, the application of these technologies in the financial sector has also brought a series of security risks, especially in the area of data privacy protection. The financial system usually contains a large amount of sensitive data, such as users' personally identifiable information and transaction records. The leakage of such data will not only violate personal privacy, but also lead to a series of consequences such as economic losses and reputation damage.

2.3. Fundamentals of Homomorphic Encryption

In the field of financial AI security risk prevention and response, homomorphic encryption technology as an advanced means of privacy protection, its importance cannot be ignored. The technology allows data to be calculated in the ciphertext state, while the result of the calculation remains encrypted until it is decrypted by an authorized user, thus ensuring privacy security during data processing. At its core lies its mathematical construction, which uses complex algebraic structures to design specific encryption algorithms that ensure that arithmetic operations on ciphertext data correspond directly to corresponding operations on plaintext data.

3. SECURITY COMPARISON BETWEEN DIFFERENTIAL PRIVACY AND HOMOMORPHIC ENCRYPTION

3.1. Security Analysis of Differential Privacy

Differential privacy is a technique that protects the privacy of an individual by adding just the right amount of noise to the data release process, and its core is to ensure that any attacker trying to infer information about an individual from a data set cannot determine whether that individual is included in the data set. This differential privacy protects the privacy of the data by defining a strict privacy loss boundary, known as ε-differential privacy. Even if an attacker has all the other data except the targeted individual, it is impossible to accurately tell whether that individual participated in the dataset. This makes differential privacy a powerful tool for protecting sensitive information and for inversion attacks. However, the application of differential privacy is not without challenges, and one of the main difficulties is how to achieve an adequate level of privacy protection while guaranteeing data availability. Although the introduction of noise enhances the privacy of data, it may also affect the accuracy and practicality of data.

3.2. Security Analysis of Homomorphic Encryption

The core of homomorphic encryption technology is to ensure that data can still be processed and analyzed after encryption, while ensuring the privacy and security of data content. From a security perspective, homomorphic encryption relies on the complexity of mathematical problems to keep it secure, and these mathematical problems are designed to be difficult enough that even in the age of quantum computing, cracking them would require enormous resources and time. Thus, from this perspective, homomorphic encryption offers a relatively reliable measure of security protection. However, a major limitation of homomorphic encryption is its efficiency. Due to the need to perform computational operations directly on the encrypted data, this often leads to a significant increase in computational complexity, which in turn affects the usefulness of the algorithm.

3.3. General Comparison and Discussion

From a security point of view, differential privacy and homomorphic encryption have their own characteristics. Differential privacy provides strong privacy protections by ensuring that no outside observer can accurately tell whether a particular individual participated in the construction of the data set. This mechanism is particularly suitable for scenarios dealing with aggregated data, however, a major challenge with differential privacy is balancing the strength of the privacy protection with the accuracy of the data analysis. In contrast, homomorphic encryption allows calculations to be performed while the data remains encrypted, fundamentally solving the problem of data leakage during data transmission and processing, but its computational complexity and efficiency issues remain a big obstacle in practical applications.

On the practical side, differential privacy has been widely used in several fields due to its relatively simple way of implementation and small computational burden. Especially in financial AI applications that require frequent access to and analysis of large amounts of data, differential privacy offers a solution that protects user privacy without significantly affecting system performance. In contrast, homomorphic encryption, while extremely powerful in theory, is currently limited by its high computational costs and complex key management requirements, which limit its application in real-time or high-performance demanding scenarios.

4. PRECISION EXPLORATION AND ALGORITHM DESIGN OF NOISE ADDITION

4.1. High-precision Noise Addition Strategy Design

An innovative high-precision noise addition strategy involves careful regulation of the noise distribution itself. $f: D \rightarrow RdTraditional$ Laplacian noise, while effective in some situations, may not be sufficient for the diverse data sensitivity and privacy needs with its fixed-scale parameters. Therefore, a method of dynamically scaling noise can be developed that automatically adjusts the size and morphology of noise based on the properties and sensitivity levels of the data. The sensitivity Δf of an algorithm is defined as the greatest difference in the output of the algorithm on adjacent data sets. For a function, its L1 sensitivity is defined as: $\Delta f = maxD, D'\|f(D) - f(D')\|1$ According to the Laplacian mechanism, in order to satisfy (ϵ, δ) -differential privacy, the algorithm output f(D) needs to add random noise X drawn from the Laplacian distribution Lap (0, bϵ), where b is the L1 sensitivity of f. The LCDP-FL algorithm combines local differential privacy (LDP) and central differential Privacy (CDP). In the local training phase, the client updates the wi and adds local noise according to the local data set Di. The goal of the algorithm is to provide the client with the desired privacy protection while reducing the computational overhead.

4.2. Design and Implementation of New Algorithm

The core of the algorithm lies in a dynamic noise adjustment mechanism, which adjusts the size of the noise according to the sensitivity of the data set and the real-time feedback of the model training. The innovation of this method is that, unlike traditional static noise addition methods, it can be more flexible to meet the needs of different data sets and model training stages. For data sets containing more sensitive information, the algorithm will automatically increase the intensity of noise to enhance privacy protection. And when the model approaches convergence, it will appropriately reduce the noise to improve the accuracy of the model.

First, the original financial data is cleaned to remove outliers and erroneous data to ensure the accuracy of the analysis; This is followed by the use of time series decomposition techniques to break down the data into trends, seasonality and random components in order to more clearly identify the underlying patterns and cyclical changes in the data. In the financial data training process, the various

participants (such as different banks or financial institutions) use their local data sets for model training, and the raw data is not shared in the process. Before uploading model updates to the central server, each client adds the right amount of noise to the model parameters, based on the characteristics and privacy needs of its data set. This addition of noise is based on the local Differential Privacy (LDP) principle to protect the client's local data. The central server can also add additional noise when aggregating model updates from various clients to further protect privacy, which is based on the concept of Central differential Privacy (CDP) to ensure data security during aggregation. The LCDP-FL algorithm can dynamically adjust the local and central noise policies according to the weight and privacy requirements of the clients to achieve the optimal privacy protection effect. The noised model updates are sent to the central server, which aggregates these updates to improve the global model. During aggregation, various optimization techniques can be employed to improve model stability and convergence. Throughout the process, the relationship between privacy protection and model utility needs to be balanced. By adjusting the differential privacy parameters (e.g., privacy budget ϵ and δ), the model can be as accurate and useful as possible while protecting privacy. Because the financial industry has strict requirements for risk management and compliance, when implementing the LCDP-FL algorithm, it is necessary to ensure that the algorithm complies with relevant laws, regulations and industry standards. After the model is deployed, it is also necessary to continuously monitor the model performance and privacy protection effect, and adjust and optimize according to feedback.

In addition, the design of the high-precision noise addition strategy should also consider the computational efficiency of the algorithm and optimize the computational steps of the noise generation and addition process without sacrificing too much privacy protection.

5. EXPERIMENTAL ANALYSIS

5.1. Experimental Evaluation and Analysis

In the process of experimental evaluation, special attention was paid to the effect of noise addition on model performance. The experimental results show that the amount and type of noise added is crucial for maintaining data privacy and maintaining an effective information balance between the data. On the one hand, although excessive noise can provide stronger privacy protection, it will also lead to data distortion, affecting the training effect of the model and the final decision quality. On the other hand, too little noise may not achieve the desired level of privacy protection.

The experiment examines the performance of different differential privacy algorithms in processing specific financial data sets. By comparing several algorithms, including hybrid noise algorithm based on local and central differential privacy (LCDP-FL), local differential privacy (LDP-FL) and central differential privacy (CDP-FL), the performance of each algorithm in terms of accuracy, loss rate and privacy security is analyzed in depth. The results show that the hybrid noise algorithm can provide more balanced performance in most cases, especially when dealing with financial datasets with different privacy requirements and data sensitivities.

6. SUMMARY AND PROSPECT

6.1. Summary

In this study, we deeply explore the application of differential privacy algorithm in financial AI security risk prevention and response, and conduct research on this basis.

In this study, we successfully combined differential privacy technology with federal learning framework to design a new hybrid noise algorithm LCDP-FL. The algorithm not only considers the privacy requirements and data weights of different clients, but also minimizes the computing cost while ensuring the privacy of users. Compared with traditional local differential privacy (LDP-FL)

and Central Differential Privacy (CDP-FL) algorithms, LCDP-FL shows better performance in terms of accuracy, loss rate and privacy protection.

6.2. Future Research Directions

In future research, differential privacy technology should be integrated with other privacy protection measures to form a more comprehensive privacy protection strategy. At present, although differential privacy can effectively protect data privacy to a certain extent, it may still need to be combined with other technologies such as encryption algorithms and secure multi-party computing in specific scenarios to deal with more complex data leakage scenarios.

REFERENCES

[1] Sun Min, Ding Xining, Cheng Qian. Federated Learning Scheme based on differential privacy [J]. Computer Science, 2019, 51(S1): 912-917. < br

[2] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information [J]. The Federal Register / The FIND, 2024 (107) (in Chinese)

[3] ZHANG Xu. Research on Data privacy protection based on Differential privacy Mechanism [D]. Tutor: WANG Yufeng. Nanjing University of Posts and Telecommunications, 2022.

[4] Ding Zhiping. Research and application of privacy protection technology based on big data environment [J]. Journal of Physics: Conference Series, 2021, 1982(1)