Advances, Applications, and Challenges of Federated Learning Technologies in the Financial Domain

Yuan Liu [1],Sha Wang,Xuan Nie[1, *]

[1]School of business, Shenyang Aerospace University, Shenyang 110136, China

[*] Corresponding Author

Abstract

Through inquiry and discussion of various literatures, the current application status of federated learning technology in the financial field and the challenges it faces are analyzed. Federated learning technology is based on the concept of distributed learning and has been applied in anti-fraud, risk management, stock recommendation and other financial fields, and has achieved certain results. However, federated learning still faces many challenges in the financial field due to issues such as data heterogeneity, privacy protection, and model fusion. Future research directions include improving model fusion algorithms and improving security and privacy protection technologies.

Keywords

fnance, federated learning, privacy preserving.

5. Introduction

With the deepening of digitalization and informatization in the financial industry, financial data has been widely used, especially in areas such as risk management, anti-fraud, and customer service. However, this is accompanied by increasing concerns about data privacy and security issues, especially unprecedented challenges in cross-institutional data sharing and compliance. The traditional centralized data processing model is unable to meet these challenges and cannot meet the growing data security and privacy protection needs of the financial industry.

Federated learning technology can not only perform model training without leaking individual data, but also effectively reduce communication overhead and protect data privacy. This article aims to systematically summarize and analyze the progress, application and challenges of federated learning technology in the financial field. Starting from technical principles, application cases, etc., it explores the main challenges and future development directions of federated learning in the financial field, and provides financial Digitalization of industries transformation provides theoretical guidance and practical reference.

6. Federated Learning Overview

The widespread application of machine learning (ML) methods has made training models through a large number of data samples a common solution, allowing enterprises to benefit from machine learning models from different data sources. However, data has privacy characteristics, and users or institutions do not want the data to leave the local area, resulting in a shortage of data sources and limiting model performance. Federated Learning (FL)[1]provides a way to protect user privacy by dispersing data to end devices, allowing clients with sensitive data and heterogeneity to train. There are three main reasons for the emergence of federated learning:

One is data ownership and privacy. Data owners may be reluctant to centralize data in one place for training because it means losing control of data. Federated learning allows data owners to train models locally while maintaining control over the data and protecting personal privacy or business confidentiality.

The second is communication costs and bandwidth limitations. Transferring large amounts of data to centralized servers for training can incur high communication costs and bandwidth limitations. Federated learning reduces communication costs by performing model updates locally and only transmitting model parameters.

The third is data diversity. The distribution and characteristics of data may vary across regions or organizations. The use of federated learning technology can fully integrate data resources from different regions or organizations while ensuring data privacy and security, thus greatly improving the generalization ability of machine learning models. This method provides strong support for the efficient use of big data resources among multiple clients and the effectiveness of machine learning models, and can benefit from it in fields such as finance and medical care.

In addition to privacy, federated learning shares the computing power of different clients, allowing smaller clients to get help. With its decentralized data concept and the requirement to comply with user data protection laws, federated learning has been growing in the field of machine learning in recent years. It brings code into data rather than data into code, solving fundamental issues of privacy, ownership and data locality.

6.1. Federated Learning Process

Classic federated learning aims to utilize a central server to train a high-quality shared global model from dispersed data scattered across a large number of different clients. The federated learning process is mainly divided into the following four steps:

One is model initialization. Initialize the central server's pretrained machine learning model (i.e., the global model) and its initial parameters and share it with all clients in the federated learning environment.

The second is local model training. After the global machine learning model shares parameters, the client uses local training data to train the client-level machine learning model.

The third is the aggregation of global models. The client sends model updates to the central server; the central server updates the global model, and the updated model is shared among various clients.

The fourth is iterative learning. Federated learning is in a continuous iterative learning process, repeating the above steps of local model training and global model aggregation to keep the global machine learning model updated in all customers.

6.2. Progress and Classification of Federated Learning Technology

Federated learning is currently in an active development stage, where various technologies and methods are being expanded and applied in practice. Federated learning can be divided into general federated learning and personalized federated learning according to different target tasks of the client. Universal federated learning aims to train a high-performance machine learning model that applies to all clients, which is usually an aggregated global model optimized through strategies such as client selection and regularization methods[2]. Given that general federated learning is difficult to cope with highly heterogeneous datadistribution, or difficulty in meeting personalized needs, prompting researchers to propose personalized federated learning [3], which allows clients to maintain personalized models based on local data and task requirements.

From the perspective of data availability and number of clients, federated learning can be divided into cross-device and cross-institution federated learning[4]. Cross-device federated learning, also known as classic federated learning, involves a large number of similar clients in the global domain and faces the challenge of maintaining transaction history and network connection reliability. This type is suitable for applications with a large number of clients, such as IoT or mobile applications. In contrast, cross-institutional federated learning focuses on a smaller population of clients, typically between 2 and 100, which are typically indexed and almost always available in training iterations. Suitable for private data training within or between organizations, such as financial institutions or medical institutions.

According to the distribution of client user data features, the literature [5] conducted further research on the federated learning scenario, in which the user data feature overlap in the two data sets is large and the user overlap is small, which is called horizontal federated learning. This scenario Users may come from different regions, with little overlap; users with large overlap and small overlap of user data features are called vertical federated learning. These users may come from the same region. For example, local banks or e-commerce companies can use these data to Build federated learning models in different institutions; the scenario where the overlap of user and user data features is very small is called federated transfer learning. This scenario may be used in situations where there are few data samples, and other relevant existing data can be used to improve model performance. . Classic federated learning belongs to horizontal federated learning. Compared with horizontal federated learning, the methods and processes of vertical federated learning and federated transfer learning require adaptive changes.

In addition, depending on whether there is a central server setting, federated learning can be divided into centralized federated learning and completely decentralized federated learning. Since federated learning is basically a decentralized data-based approach that relies on a central server to manage the federated environment, including collecting trained models from clients, building a global model, and sharing it with all clients, a third-party system is established to build A central server of trust between clients is the first priority. This server-client hub-and-spoke topology ensures centralized authority to manage and monitor the continuous learning process, but the central server faces greater communication bottlenecks and security risks. At the same time, the hub-and-spoke topology reduces fault tolerance and the central server is paralyzed. This will lead to the paralysis of the entire federal system. The fully decentralized federated learning method avoids dependence on a central server and replaces centralized client authorization with an authorization algorithm to build trust and reliability. As mentioned in [6], each participant improves their model by sharing information with neighbors, although this also brings communication and integrity challenges.

7. Financial field applications

7.1. Credit Card Anti-Fraud

Credit card fraud causes huge annual losses to cardholders and is a common form of financial fraud. Efficient anti-fraud models often require large amounts of transaction data to identify relevant features. Through federated learning, different banks can collaborate to train fraud detection models without sharing sensitive transaction data. This approach allows banks and other financial institutions to improve their overall fraud detection capabilities while protecting customer privacy. For example, the literature [7] shows a federated meta-learning credit card fraud detection framework that protects customer privacy and complies with privacy protection regulations. It uses a cross-site non-IID credit card transaction data set to build a model and learns through improved ternary metric Enhance the discriminative performance of the model.

When processing bank transaction data, we often face a challenge: there are few abnormal transactions and many normal transactions, making it difficult for traditional anti-fraud models to identify minority class features. Literature [8] introduces an oversampling strategy that effectively balances the proportion of categories of transaction data without significantly increasing the amount of calculation and resource consumption. The application of secure federated learning may be affected by the differential privacy mechanism, resulting in reduced model performance. Literature [9] proposed a method that combines differential privacy to enhance the privacy protection capabilities of the model. In addition, literature [10] proposed a scalable federated learning framework Starlit, which solved the limitations of traditional methods in scalability and computational complexity, and optimized computational efficiency. Literature [11] believes that in financial sites, there are fake credit card transaction data that are significantly lower than legitimate transaction data. Therefore, the author proposed a sampling strategy based on independent and mixed methods to ensure that it can adapt to different degrees of class-imbalanced transaction data sets. In addition, based on the balanced data after sampling, the author experimentally verified the impact of independent and mixed methods on different types of downstream classifiers, and then gave suggestions on the balance between computational complexity and performance.

Generally speaking, in terms of credit card anti-fraud, existing research focuses on how to use data security protection technology to further protect customer privacy and how to avoid information leakage caused by model calculation results.

7.2. Credit risk assessment

Credit risk assessment is an important aspect of the financial sector, including bankruptcy prediction, credit scoring and bond ratings, etc. Federated learning allows different financial institutions to co-train models to more comprehensively understand market risks and develop accurate assessment strategies. Literature [12] proposed using financial data of long-term mortgage assets to establish a credit risk assessment model for fixed asset investment returns under federated learning. In order to solve the problem of reduced accuracy of prediction models caused by long-term loan data, the author proposes to use federated learning methods to jointly establish a long-term loan return prediction model from short-term loan return data from multiple institutions to make up for the shortcomings in the length of single-site data.

Common machine learning methods such as XGBoost in tree models are widely used in credit risk assessment. From the perspective of privacy, literature [13] first introduced the XGBoost method in the field of federated learning, called SecureBoost. Experiments have shown that SecureBoost can achieve comparable performance to models that do not adopt privacy protection protocols and achieve higher scalability. Literature [14] evaluates an individual's creditworthiness from the conceptualization of digital individual characteristics such as social interaction, character background, and economic status. Through federated learning, the author proposes a unified credit assessment model that fuses information on tens of thousands of heterogeneous digital individual characteristics, and combines cognitive modeling and other mechanisms to transform heterogeneous characteristics into customer-level characteristics. Embed features for downstream credit assessment tasks.

In response to the problem of data heterogeneity in joint modeling across banking institutions, the literature [15] uses the chi-square test to model, analyze and evaluate the non-independent and identical problems of financial data, and detect and delete such data heterogeneity. Anomalous data with high levels of disagreement among participants. Considering the asymmetry of information between banks and enterprises, literature [16] proposes a credit risk assessment framework for small and medium-sized enterprises. The framework consists of federation feature selection and participant contribution quantification methods that ensure the federation model. In this framework, federated feature selection mainly uses the integrated tree model to reduce the number of features in multi-dimensional enterprise data to learn an efficient evaluation model; the participant quantification method performs gradient estimation on the calculation results of the participants to ensure that the parameters of the federated model are positive. renew.

7.3. Anti-money laundering

Anti-money laundering requires monitoring abnormal transaction activities and identifying potential criminals. Federated learning can strengthen cross-bank cooperation and improve the ability to identify financial crime patterns. Literature [17] uses graph federated learning to achieve cross-agency sharing of key information, timely identification of emerging money laundering patterns and their identification and response methods, thereby improving the ability to monitor potential global money laundering activities. Literature [18] developed a federal anti-money laundering model based on the SecureBoost framework. Experimental results show that the federated model can accurately detect potential money laundering behavior with less performance loss than the centralized model. Literature [19] believes that less data from a single site is not enough to learn an efficient anti-money laundering model. For this reason, the author designed a DeepProtect that processes and identifies money laundering transactions. It learns bank data based on cross-site federated learning, which is relatively based on a single site. detection method, the protocol can simultaneously locate suspicious transactions and automatically freeze bank accounts of criminals suspected of money laundering.

With the development of blockchain, detecting money laundering behavior in the field of digital currency is an important guarantee for the security and authority of digital currency. Therefore, it is crucial to identify malicious transactions, and current methods do not explore the proximity of traders and transaction characteristics when trading digital currencies. Therefore, literature [20] proposed a detection protocol GraphSniffer based on federated graph learning to locate malicious transactions in the digital currency market. This protocol models the graph structure relationship of on-chain nodes in Bitcoin transactions to update the global identification model. In the identification of federated malicious transactions, the data of participants usually presents a non-independent and identically distributed state. Literature [21] believes that this difference in data distribution leads to a small number of participants generating malicious transaction data and dominating federated learning through model poisoning attacks. process. In response to this problem, the author designed a new filtering algorithm to detect each participant and screen out participants with abnormal false transactions before the global model is aggregated and updated. Considering the privacy risks faced by cross-agency cooperation, literature [22] proposed a scalable federal anti-money laundering platform. Specifically, the author uses confidential computing technology to protect the local privacy data of participants, and at the same time ensures that the developed anti-money laundering algorithms owned by participants will not be leaked.

7.4. Credit assessment

Credit assessment is a crucial task in the financial field, involving issues such as default prediction. Among them, insufficient data sets and imbalanced category distribution promote the application of federated learning. For example, the data size of a single bank or local bank is small and insufficient to support credit assessment, and the bank's loan defaults are highly imbalanced. Compared with the repaid loans, the loan Defaults are in the minority. Literature [23] uses synthetic minority class comprehensive sampling technology SMOTE to solve data imbalance, and combines distributed learning algorithms to protect data sensitivity. This method not only enables inter-bank sharing of models, but also further improves results through weighted aggregation of models, providing a feasible solution for credit assessment. Literature [24] designed a federated learning model that can share data without exposing customers' hidden information. On the public loan dataset on Kaggle, the model achieved 81% accuracy, highlighting the potential application of federated learning in loan eligibility assessment. Literature [25] proposed a financial problem prediction application based on federated learning, using asynchronous federated learning to solve the problem of extra waiting time in global model generation. Through simulation experiments, the authors demonstrate the performance of the proposed federated learning model under various conditions, highlighting its superiority when dealing with resource-constrained agents and highly skewed data compared with existing methods. Literature [26] discusses the integration of federated learning and blockchain technology in supply chain credit assessment, believing that federated learning can effectively solve the financing problems of small and medium-sized enterprises and combine with blockchain to ensure the credibility and transparency of information. This mechanism provides an innovative solution for the financing of supply chain enterprises by ensuring that their private data is used locally while providing blockchain records.

7.5. Insurance risk control

Federated learning applications in the insurance field mainly focus on insurance fraud detection and vehicle insurance data analysis and risk control. Literature [27] uses technologies such as genetic algorithm and particle swarm optimization for feature selection and model optimization to improve the accuracy and efficiency of fraud detection and protect data privacy. Literature [28] proposed an insurance pricing and risk classification method based on car usage behavior, emphasizing the importance of federated learning in dealing with data privacy and model training. By protecting individual vehicle behavior data, this approach provides the insurance industry with a more reliable way to assess risk. Literature [29] explores the potential value of data sharing to the insurance industry and proposes a framework based on federated learning to address data privacy and cooperative learning. The authors highlight the innovations of this approach in promoting industry collaboration, risk management, and privacy protection. Literature [30] introduces the basic principles of federated learning and emphasizes its advantages in processing large-scale data and protecting data privacy in the life insurance business. By applying federated learning, this approach improves model performance while ensuring data privacy.

7.6. Stock price prediction

One of the main contents of the investment direction in the financial field is stock price prediction. Literature [31] uses technologies such as data enhancement and category estimation to predict edge prices.

The federated learning model is implemented between edge nodes. Literature [32] allows aggregation of local models in a robust manner, improves data distribution problems, reduces computational costs, and has a practical application on financial portfolio management problems, demonstrating the potential application of this method in the financial field. Literature [33] proposes a federated reinforcement learning method, which introduces deep reinforcement learning technology and uses deep learning models to represent the strategies used by reinforcement learning agents. The federated learning algorithm allows portfolio managers to individually improve their transactions. policies and benefit from other policies by sharing them while protecting private data. With this federated reinforcement learning approach, portfolio managers can achieve significant improvements in annual returns and Sharpe ratios. Literature [34] proposed a data trading market based on federated learning, allowing multiple data trading agents to jointly train models without sharing original data. By re-representing local market information, the authors successfully address the problem of non-stationarity in data product revenue patterns. Literature [35] proposed a long short-term memory (LSTM) architecture that combines federated learning and attention mechanisms for stock price prediction. Validated with real datasets, this method improves model performance and protects data privacy.

8. Challenges and prospects

8.1. Privacy protection

As countries gradually establish relevant laws and regulations, the use of financial data has been subject to stricter regulations. It has become an industry consensus to adopt a secure federated learning mechanism to achieve the integration of the financial industry and artificial intelligence technology. The security of federated learning needs to be considered from two levels: On the one hand, based on user privacy protection and regulatory requirements, the introduction of secure federated learning faces many challenges. For example, the calculation results may be obtained by attackers, thereby leaking user information. Therefore, it is necessary to use data encryption technology to protect user privacy while ensuring that performance is not significantly affected. On the other hand, researchers need to ensure acceptable calculation results and prevent malicious actors from using erroneous data to interfere with the learning process. However, the distributed nature of federated learning may increase the risk of model attacks and make data privacy protection more difficult. Due to the sensitivity of financial data, the use of data privacy protection technology is the current consensus for secure federated learning, but it inevitably brings about the problem of performance degradation. Therefore, weighing performance gains and protecting customer data privacy is one of the directions for future research.

8.2. Computational and communication efficiency

To enhance privacy protection, secure federated learning needs to combine multiple data protection mechanisms, which inevitably introduces additional computing and communication costs. At the same time, in order to decrypt the encryption results, synchronous collaboration is required between some servers and financial outlets, which may affect the scalability of the method and the training efficiency of the model. For example, federated learning methods based on homomorphic encryption require a large amount of computing resources during the encryption and decryption processes, resulting in performance losses. Methods incorporating secure multi-party computation or obfuscated circuits may increase communication volume or limit model complexity due to the increase in participants. In order to reduce communication overhead, strategies such as model quantization, periodic federated averaging, or asynchronous federated learning can be considered to improve efficiency. Considering the need for high scalability in model decision-making driven by financial data, how to design efficient and lightweight secure federated learning for financial data may be one of the focuses of future research.

8.3. Data heterogeneity

The heterogeneity of financial data is reflected in two aspects in federated learning: First, there is a significant difference in the amount of data held by each participant, which may cause participants with less data to be covered by the party with more data; second, in a single institution , the amount of normal transaction data far exceeds that of illegal transactions, resulting in uneven data distribution. Current methods mainly achieve site data balance through data generation, oversampling, and other methods. However, these methods will bring additional noisy data, causing the performance of federated learning methods to decrease. Therefore, further research on how to handle imbalanced data distribution through federated learning and achieve high-precision, personalized model decision-making remains one of the keys to research on federated systems in the financial field. For example, adversarial feature enhancement technology is used to improve the long-tail distribution problem of participant data class labels and balance the system class distribution.

8.4. Reward mechanism

Since there are large differences in the amount of data held by financial institutions, the introduction of a reward mechanism can increase the enthusiasm of participants and ensure fair cooperation. However, cross-institutional data heterogeneity, differences in participant model quality, and data privacy requirements all bring challenges to the design of reward mechanisms. Currently, the reward mechanisms for federated learning for financial data are mainly designed from the perspectives of reputation and resource allocation, but these mechanisms are difficult to adapt to the increasingly complex federated system environment. Related work achieves the goal of reasonably allocating benefits to each participant by measuring the update quality of the model, the reliability of the participants, and calculating the contribution level of the participants in each federal communication round. However, related work on the federal financial model , no more consistent conclusion has been reached. Therefore, designing a reward mechanism that can accurately assess the contributions of participants and reasonably distribute benefits is a focus of future research.

9. Conclusion

Overall, the application of federated learning in the financial field shows great potential and value. From anti-fraud to credit assessment to insurance and investing, federated learning provides effective solutions to protect customer privacy and improve data efficiency. Through cross-agency collaboration, the challenges of uneven data distribution and privacy protection can be better addressed. In the future, with the advancement of technology and further application in the financial field, federated learning will continue to promote innovation in financial technology and bring more value to the industry and customers.

References

[1] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[DB/OL]. (2023-01-26)[2024-03-19]. https://arxiv.org/abs/1602.05629.

[2] Zhang Min, Liang Meiyu, Xue Zhe, et al. Regular optimization algorithm for heterogeneous data federated learning model based on structural enhancement [J]. Pattern Recognition and Artificial Intelligence, 2023, 36(9): 856-865.

[3] TAN A Z, YU H, CUI L, et al. Towards personalized federated learning[DB/OL]. (2022-03-17)[2024-03-19]. https://arxiv.org/abs/2103.00710.

[4] KAIROUZ E B P, MCMAHAN H B. Advances and open problems in federated learning[J]. Foundations and Trends® in Machine Learning, 2021, 14(1).

[5] ROY A G, SIDDIQUI S, PÖLSTERL S, et al. Braintorrent: A peer-to-peer environment for decentralized federated learning[DB/OL]. (2019-05-16)[2024-03-19]. https://arxiv.org/abs/1905.06731.

[6] Yang Qiang. AI and data privacy protection: How to crack "federated learning" [J]. Information Security Research, 2019(11):961-965.

[7] ZHENG W, YAN L, GOU C, et al. Federated meta-learning for fraudulent credit card detection[C]//Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence, 2021: 4654-4660.

[8] YANG W, ZHANG Y, YE K, et al. Ffd: A federated learning based method for credit card fraud detection[C]//Big Data – Big Data 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25 – 30, 2019, Proceedings 8. Springer International Publishing, 2019: 18-32.

[9] BYRD D, POLYCHRONIADOU A. Differentially private secure multi-party computation for federated learning in financial applications[C]//Proceedings of the First ACM International Conference on AI in Finance, 2020: 1-9.

[10]ABADI A, DOYLE B, GINI F, et al. Starlit: Privacy-Preserving Federated Learning to Enhance Financial Fraud Detection[DB/OL]. (2024-01-22)[2024-03-19]. https://arxiv.org/abs/2401.10765.

[11] ABDUL SALAM M, FOUAD K M, ELBABLY D L, et al. Federated learning model for credit card fraud detection with data balancing techniques[J]. Neural Computing and Applications, 2024: 1-26.

[12]LEE C M, FERNÁNDEZ J D, MENCI S P, et al. Federated Learning for Credit Risk Assessment[C]//HICSS, 2023: 386-395.

[13]CHENG K, FAN T, JIN Y, et al. Secureboost: A lossless federated learning framework[J]. IEEE Intelligent Systems, 2021, 36(6): 87-98.

[14]HOANG M D, LE L, NGUYEN A T, et al. Federated Artificial Intelligence for Unified Credit Assessment[C]//International Conference on Human-Computer Interaction, 2020: 44-56.

[15]LI Y, WEN G. Research and Practice of Financial Credit Risk Management Based on Federated Learning[J]. Engineering Letters, 2023, 31(1).

[16]XU Z, CHENG J, CHENG L, et al. MSEs credit risk assessment model based on federated learning and feature selection[J]. Computers, Materials & Continua, 2023, 75(3).

[17]SUZUMURA T, ZHOU Y, BARACALDO N, et al. Towards federated graph learning for collaborative financial crimes detection[DB/OL]. (2019-10-02)[2024-03-19]. https://arxiv.org/abs/1909.12946.

[18]GUEMBE B, AZETA A, OSAMOR V, et al. A federated machine learning approaches for anti-money laundering detection[J]. Available at SSRN 4669561, 2023.

[19]KANAMORI S, ABE T, ITO T, et al. Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks[J]. Journal of Information Processing, 2022, 30: 789-795.

[20] DU H, SHEN M, SUN R, et al. Malicious transaction identification in digital currency via federated graph deep learning[C]//IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, 2022: 1-6.

[21]MYALIL D, RAJAN M A, APTE M, et al. Robust collaborative fraudulent transaction detection using federated learning[C]//2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA), IEEE, 2021: 373-378.

[22] SEARLE R, GURURAJ P, GUPTA A, et al. Secure implementation of artificial intelligence applications for anti-money laundering using confidential

computing[C]//2022 IEEE International Conference on Big Data (Big Data), IEEE, 2022: 3092-3098.

[23] SHINGI G. A federated learning based approach for loan defaults prediction[C]//2020 International Conference on Data Mining Workshops (ICDMW), IEEE, 2020: 362-368.

[24] AZZEDIN F, GHALEB M, EL-ALFY Y, et al. A Federated Learning Approach to Banking Loan Decisions[C]//2023 International Symposium on Networks, Computers and Communications (ISNCC), IEEE, 2023: 1-7.

[25] IMTEAJ A, AMINI M H. Leveraging asynchronous federated learning to predict customers financial distress[J]. Intelligent Systems with Applications, 2022, 14: 200064.

[26] MA Q, YANG H, WANG D, et al. Supply Chain Credit Evaluation Mechanism Integrating Federated Learning and Blockchain[C]//Proceedings of the 11th International Conference on Computer Engineering and Networks, Springer Singapore, 2022: 1471-1480.

[27] SUPRIYA Y, VICTOR N, SRIVASTAVA G, et al. A Hybrid Federated Learning Model for Insurance Fraud Detection[C]//2023 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2023: 1516-1522.

[28] YIN T, PENG C, TAN W, et al. Federated Learning Model for Auto Insurance Rate Setting Based on Tweedie Distribution[J]. CMES-Computer Modeling in Engineering & Sciences, 2024, 138(1).

[29] DONG P, QUAN Z, EDWARDS B, et al. Privacy-Enhancing Collaborative Information Sharing through Federated Learning--A Case of the Insurance Industry[DB/OL]. (2024-02-22)[2024-03-19]. https://arxiv.org/abs/2402.14983.

[30] GUPTA H, PATEL D, MAKADE A, et al. Risk prediction in the life insurance industry using federated learning approach[C]//2022 IEEE 21st Mediterranean Electrotechnical Conference.