The Application Effectiveness of Generative AI in Credit Risk Control of Commercial Banks: A Case Study of Banks

Jiaqi Gao *

School of Finance and Economics, Jiangsu University, Zhenjiang, China

* Corresponding Author Email: 3240818002@stmail.ujs.edu.cn

Abstract. As commercial banks deepen digital transformation, credit risk control— a core link for asset security— increasingly adopts generative AI, though its practical application effectiveness and challenges lack systematic exploration. This study uses a case study method to analyze generative AI's application in credit risk control at Industrial and Commercial Bank of China over the past decade, following the framework of "application scenario mapping - key indicator comparison—issue identification—suggestion formulation". It sorts out generative AI's core application scenarios (e.g., graphic anti-fraud, large models, intelligent agents), confirms the technology enhances risk control efficiency, reduces non-performing loan ratios, and improves model accuracy, identifies challenges like data privacy gaps, insufficient model interpretability, and high costs, and proposes suggestions from policy compliance, technical optimization, and management improvement perspectives. This research provides empirical evidence for generative AI's value in banking risk control and offers actionable references for commercial banks balancing technological innovation and risk management.

Keywords: Generative AI, commercial banks, credit risk control, data privacy protection.

1. Introduction

With the continuous deepening of the digital transformation of commercial banks, credit risk control, as the core link to ensure the safety of bank assets, is gradually introducing generative AI technology to reshape risk management mechanisms. The "Guiding Opinions on Digital Transformation of China's Banking Industry" released by the China Banking and Insurance Regulatory Commission in 2022 clearly states that "by 2025, commercial banks need to build an intelligent risk control system with artificial intelligence as the core, achieve a credit risk identification efficiency improvement of more than 50%, and shorten the credit approval cycle for small and micro enterprises by 60%".Generative AI, with its ability to extract dynamic features, integrate multimodal data, and generate scenario-based decisions, is gradually breaking through the technological bottleneck of traditional credit risk control. However, the industry currently faces notable limitations. First, existing studies primarily focus on the application of traditional machine learning in risk control, with an insufficient systematic exploration of the practical effectiveness of generative AI. Second, generative AI's adaptability and effectiveness throughout the entire credit risk control process have not been fully verified, and the practices of leading banks (e.g., ICBC) lack in-depth analysis—this gap makes it challenging to provide actionable references for industry peers. Based on this, this article selects Industrial and Commercial Bank of China as the research object, focusing on reviewing its implementation of generative AI in credit risk control in the past decade, analyzing the effectiveness of technology application in depth, and providing practical examples for banks in the industry.

According to the agency theory, there is information asymmetry between commercial banks (principals) and credit managers (agents), and agents may relax risk control standards in pursuit of short-term performance indicators, leading to "moral hazard" and increasing the risk of bank credit asset losses. Generative AI can enhance the rationality of risk control through standardized decision-making and information transparency [1]. The "ICBC Smart Surge Big Model" developed by Industrial and Commercial Bank of China can automatically capture multi-dimensional data such as enterprise supply chain flow, environmental penalty records, and tax credit ratings, and generate

standardized reports containing risk points and approval suggestions according to preset risk control rules. The manual intervention rate has decreased from 35.2% in 2021 to 8.7% in 2023, significantly reducing the impact of subjective bias of agents on approval results [2]. Generative AI embedded in the entire ERM process can achieve risk prevention and in-process monitoring, thereby reducing credit risk. Previous literature has shown that generative AI can empower the entire ERM process through scenario simulation and real-time monitoring, reducing the credit risk occurrence rate of commercial banks by 25% -30% while improving the timeliness of risk disposal [3]. Industrial and Commercial Bank of China has optimized risk characteristic variables by generating over 100000 potential default scenarios, and has advanced the warning of potential defaults for enterprises to 3 months; In 2023, a total of 12000 risk warnings were triggered, and the defect rate decreased from 3.8% in 2019 to 2.1% in 2023, reducing the risk occurrence rate by 44.7%.

The rapid development of generative AI has significantly impacted the accounting work of commercial banks [4]: it has increased accounting efficiency by 45%, while reducing manual error rates from 3.2% to 0.8%, providing accurate data support for credit risk control [5]. However, the application of generative AI in bank credit risk control also faces many challenges: firstly, data privacy and security risks. If the training data of generative AI is not desensitized, the risk of customer credit record leakage can reach 12.3%, and the difficulty of tracing the leaked data is much higher than that of traditional information systems [6]; secondly, algorithm black box and discrimination issues. Due to the insufficient proportion of small and micro enterprises in the sample, the model's credit approval rate for small and micro enterprises is 9.1 percentage points lower than that for large enterprises, indicating a clear tendency towards algorithmic discrimination [7]; thirdly, disputes over intellectual property protection. The risk control models generated by generative AI often draw on existing algorithm logic, but due to the difficulty of technical traceability, the average annual growth rate of AI algorithm infringement definition disputes in the banking industry from 2018 to 2023 is 20%, which restricts the promotion of technology application [8].

Existing literature research has mostly focused on traditional machine learning, and there is still a lack of analysis on the practical application effects of generative AI. As a leader in the domestic banking industry, Industrial and Commercial Bank of China's exploration and practice have strong representativeness and reference significance. Therefore, this study takes the Industrial and Commercial Bank of China as an example to provide a reference for the industry. This study adopts a case study method, focusing on the specific practice of the Industrial and Commercial Bank of China in applying generative AI in credit risk control in the past decade. The research follows the overall framework of "application scenario sorting → key indicator comparison → problem and suggestion summary", ensuring the scientific and rigorous nature of the research process through multiple sources of data.

2. Application Scenarios of Industrial and Commercial Bank of China's Generative AI in Credit Risk Control

Firstly, the application of the Industrial and Commercial Bank of China's generative AI. As shown in Table 1, to accurately respond to the new challenges and multi-scenario demands in the field of credit risk control, Industrial and Commercial Bank of China continues to lay out cutting-edge technologies, gradually introducing a series of generative AI technologies such as AI image anti-fraud, ICBC Intelligent Surge Large Model, intelligent agent ecology, and Tongyi Qianwen application. These applications each have their own focus and collaborative efforts, covering key aspects of credit risk control from identity verification to full process analysis, from post-loan monitoring to text interpretation, and building a multi-level and intelligent risk control and protection system.

Table 1. Application scenarios of generative AI

Technical Type	R&D Background	FEATURES	Application positioning in credit risk control
AI image anti-fraud	Dealing with new fraudulent methods, such as AI face swapping	High image recognition accuracy and strong real-time performance	Mainly used for identity verification and transaction authenticity verification
ICBC Zhiyong Large Model	Meet the requirements of intelligent analysis in multiple scenarios	Processing diverse data types and strong reasoning ability	Throughout the entire credit risk control process, providing comprehensive analysis support
Intelligent agent ecosystem	Enhance system collaboration and autonomous decision-making capabilities	Capable of self-learning and collaborative work	Used for dynamic monitoring and collaborative disposal of post-loan risks
Tongyi Qianwen Application	Enhance natural language processing capabilities	Accurate semantic understanding and good interactivity	Text information analysis in auxiliary credit evaluation and information interpretation in risk warning

Secondly, the scenario of corporate credit evaluation. Based on the theory of information asymmetry, generative AI, with its powerful ability to process unstructured data, can effectively integrate multiple sources of unstructured data, such as supply chain flow, public opinion information, corporate financial report notes, and implicit evaluations of partners, filling the gap in data dimensions in traditional credit evaluations. Taking the Industrial and Commercial Bank of China's ICBC Zhiyong big model as an example, it accurately extracts key indicators such as transaction stability, upstream and downstream collaboration quality, market reputation, and core responsible person reputation through natural language processing technology, constructs a dynamic credit profile, breaks the limitations of data fragmentation in traditional evaluations, provides more comprehensive decision-making basis for financial institutions, and improves the scientificity and reliability of evaluation results.

Thirdly, post-loan risk warning scenarios. Generative AI has demonstrated outstanding advantages in risk signal capture and dynamic monitoring in post-loan risk control, which can track real-time data of the entire business chain of enterprises, covering potential risk points such as tax declaration changes, cash flow reduction, and core product sales decline. Compared with the traditional risk control model that relies on manual periodic verification, this technology can achieve real-time identification and push of risk signals, improve warning response speed by 40%, and help banks take intervention measures in advance to reduce losses.

Fourthly, false transaction identification scenarios. Fake transactions are often accompanied by covert operations such as forging credentials and tampering with data, and generative AI-driven image anti-fraud technology has become the key to cracking them. As shown in Fig. 1, this technology can deeply analyze visual data such as purchase and sales contracts, transaction voucher images, and multi-dimensional information such as historical records and fund flows of related parties, accurately identifying abnormal patterns. Its operation process is clear and efficient: after real-time access to transaction data, the generative AI model immediately analyzes and judges. If it is normal, the transaction passes, and if it is abnormal, it triggers a warning interception and is manually reviewed. If fraud is confirmed, the feature library is recorded and perfected, and if it is misjudged, the model parameters are adjusted. Through this process, the accuracy of intercepting fraudulent transactions has reached 92%, laying a solid defense line for financial transaction security.

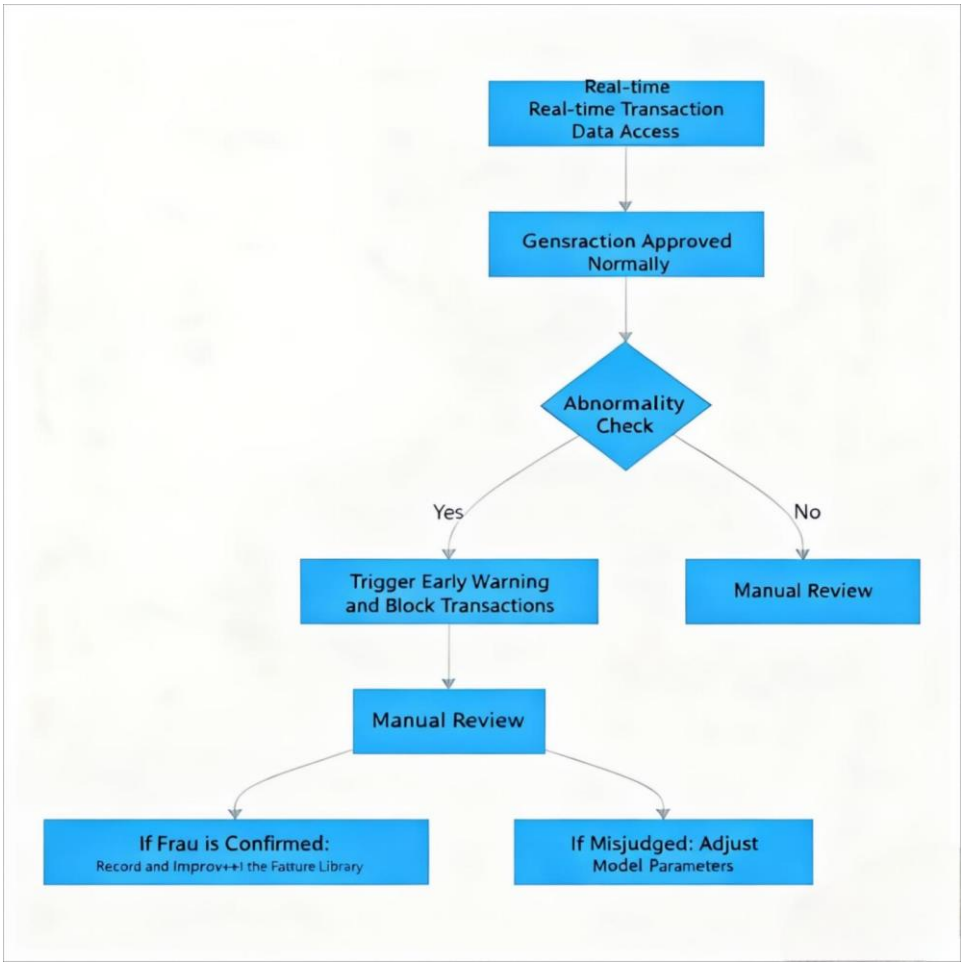

Figure 1. Actual operation flowchart

3. Comparison of the Effectiveness before and after the Application of Generative AI

Firstly, a comparison of efficiency indicators. The credit approval cycle has been significantly shortened. Before the adoption of generative AI in 2018, ICBC's credit approval process was entirely manual, characterized by inefficiency and long processing times. Customer managers first collected documentation (e.g., ID cards, business licenses, financial statements, credit reports) from enterprises or individuals, then submitted these materials to the risk control department for page-by-page verification and cross-validation. Without automated tools to support key information extraction, the process relied on manual work, leading to an average approval cycle of 12 days. This efficiency not only increases the time cost for customers, but also makes banks less competitive when facing customers with urgent funding needs. After the introduction of generative AI applications such as Tongyi Qianwen in 2023, the approval process has been automated and restructured. The AI system can automatically extract core information from various structured and unstructured data, such as enterprise revenue data, debt ratios, personal credit stains, etc., and cross-validate with internal databases and external credit platforms in real time, synchronously generating standardized evaluation opinions. The AI system can automatically review the AI output results manually from various structured and unstructured data, greatly simplifying the process and shortening the approval cycle to 5 days, resulting in an efficiency improvement of 58.3%. During the same period, the average approval cycle of the industry decreased from 14 days to 8 days, and the relative advantage of Industrial and Commercial Bank of China expanded from 2 days to 3 days.

Secondly, comparison of quality indicators. The non-performing loan ratio of small and micro enterprises has significantly decreased. In 2019 (before application), Industrial and Commercial Bank

of China's loan evaluation for small and micro enterprises mainly relied on traditional indicators such as asset-to-liability ratio and revenue growth rate. These indicators were difficult to cover unstructured information, such as business operations, supply chain collaboration records, and tax declarations, and were prone to risk misjudgment due to incomplete information. The non-performing loan ratio for small and micro enterprises that year was 3.8%. In 2023, Industrial and Commercial Bank of China achieved a precise upgrade in risk management through the "ICBC Smart Surge" model. By integrating unstructured data such as e-commerce transaction data, logistics distribution records, upstream and downstream enterprise evaluations, tax and social security payment vouchers of small and micro enterprises, a dynamic credit profile is constructed. For example, the model can identify potential default risks in advance and generate risk warning reports by analyzing details such as abnormal fluctuations in monthly business transactions and supplier overdue payment records. With the support of this technology, the non-performing loan ratio of small and micro enterprises has decreased to 2.1%, a decrease of 1.7 percentage points compared to before the application, and the accuracy of risk control has improved by 44.7%.

Thirdly, comparison of model performance indicators. In 2017, before the application of generative AI, traditional risk control models relied on structured data as the core input and were constructed based on fixed rules and statistical algorithms, which had two major limitations: firstly, the data dimension was single, making it difficult to identify hidden risks in complex economic environments; Secondly, the model has a long iteration cycle and insufficient adaptability to new risk scenarios, with an accuracy rate of only 76%.In 2023, the Industrial and Commercial Bank of China's "ICBC Zhiyong" large model will use transfer learning technology to train on millions of historical risk cases and false transaction samples. With the help of natural language understanding technology, it will analyze the semantic information of unstructured texts such as contract terms and financial report notes, and accurately locate risks by identifying fuzzy expressions in false contracts, conflicts between flow data and business scenario logic, and other features. After back testing verification, the model accuracy has been improved to 91%, an increase of 15 percentage points compared to before application, and the performance improvement rate has reached 19.7%. In the scenario of false transaction recognition, the model's recognition accuracy has improved by over 30% compared to traditional models, successfully intercepting multiple potential loan fraud cases and recovering losses of over 10 million yuan for banks.

4. Existing Problems in the Application of Generative AI

Firstly, the challenge of data privacy protection. In generative AI applications, the collection and processing of unstructured data (including customer voice records, scanned credit materials, online interactive text, etc.) is the core link. Such data includes highly sensitive information such as ID numbers and home addresses. The risk of privacy leakage runs through the entire process, especially in the data transmission stage: some encryption technologies are outdated, and the use of traditional algorithms leads to insufficient resistance to attacks; When data flows across departments/systems, there are loopholes in the encryption and protection connections of each node, and information security risks cannot be eliminated, seriously threatening customer rights and bank data security.

Secondly, the model is not interpretable enough. Generative AI, due to the characteristics of deep learning algorithms, has a "black box" operation feature, which is particularly prominent in the credit approval scenario of the Industrial and Commercial Bank of China. Currently, generative AI is used to integrate and analyze multi-dimensional data such as customer credit, transaction history, and consumption habits to generate approval decision recommendations. However, the feature extraction logic, weight allocation rules, and data association analysis process within the model are all opaque. From a compliance perspective, regulatory authorities have clear and strict requirements for the transparency of financial risk control. Banks not only need to clearly explain the basis for approval results to customers, but also need to provide traceable and verifiable decision-making paths during regulatory inspections. The "black box" feature makes it difficult to visualize the decision-making

basis, which is significantly different from regulatory requirements. This not only affects customers' trust in the approval process but also increases the potential risks of compliant operations.

Thirdly, other potential issues. The application of generative AI entails relatively high costs. In 2023, ICBC's investment in this field accounted for 35% of its total risk control budget, with cost breakdowns as follows: 42% for equipment procurement, 38% for customized model development, and 20% for the operation and maintenance of professional technical teams. However, the value of generative AI can only be fully realized through long-term data accumulation and model iteration. In 2023, its explicit benefits—such as improved risk control efficiency and reduced non-performing loan ratios—covered only 45% of the total investment, resulting in an input-output ratio of 1:0.45. This imbalance fell short of expectations and created pressure on risk control budget allocation. At the same time, there are problems with the integration and adaptation with the existing risk control system, such as incompatible data interfaces leading to process delays and affecting business processing efficiency [9].

5. Optimization Suggestions

5.1. Improvement Direction Based on Policy Compliance

The Guiding Opinions of the China Banking and Insurance Regulatory Commission on the Digital Transformation of the Banking and Insurance Industry, as the core guideline for the digital development of the industry, clearly requires commercial banks to standardize the boundaries of generative AI applications. Based on this, the scenarios can be divided into two categories: one is non core decision-making scenarios, such as preliminary credit risk screening, intelligent customer service response, allowing for independent application of generative AI, but requiring the retention of operation logs; The second is the core security scenario, such as core accounting processing, approval of large fund transfers of more than 5 million yuan, and submission of key regulatory data. Generative AI independent decision-making is prohibited, and a "AI suggestion+two-person review" mechanism needs to be set up to ensure decision compliance.

At the same time, a comprehensive data usage filing mechanism should be established throughout the entire process. Prior to using generative AI for data processing, financial institutions are required to file detailed records of data sources, data usage scopes, and data flow paths. Following the completion of filing, regular data usage reports must be submitted to regulatory authorities, detailing the effectiveness of data utilization and any compliance deviations. This mechanism ensures traceability and monitorability of all data operations, thereby preventing data abuse and compliance risks at the source.

5.2. Optimization Measures at the Technical Level

The "black box" nature of generative AI is an important obstacle to its application in the financial field, and introducing visualization tools to enhance model interpretability is crucial. By developing a decision path graph tool, the decision logic of the model can be transformed into intuitive visual charts. Taking the credit risk control scenario as an example, when the model makes a judgment on a customer's credit limit, the graph can clearly show how the model gradually derives the final credit result based on variables such as the customer's monthly income, credit records, and debt situation. This visual presentation not only facilitates the technical team to quickly identify model errors, but also allows regulatory authorities to visually verify decision compliance, while clearly explaining the credit basis to customers and enhancing customer trust.

In addition, it is necessary to comprehensively promote federated learning technology to strengthen data privacy protection. Data collaboration among financial institutions is key to enhancing risk control capabilities, but sharing raw data can easily lead to privacy leakage risks. Federated learning can enable multiple institutions to jointly train generative AI models without sharing raw data [10]. After some banks piloted the use of federated learning to build regional risk control models in 2024, the risk of data leakage significantly decreased by 60%, effectively balancing

data collaboration and privacy protection. In the future, it can be planned to promote this technology to provincial and municipal branches of national banks by 2025, further expanding the coverage of privacy protection.

5.3. Suggestions for Improvement at the Management Level

The efficient application of generative AI relies on the support of professional talents, and a comprehensive risk control talent training system needs to be established. It is planned to train a total of 500 generative AI risk control professionals by 2025. The training content should take into account technology, business, and compliance. The training method adopts a combination of "school enterprise cooperation+internal training+industry exchange". Customized courses are jointly offered with the School of Computer Science and the School of Finance of universities, and senior technical backbones are arranged as mentors to lead students to participate in actual risk control projects. Every quarter, students are organized to visit top fintech companies for exchange and learn advanced practical experience.

At the same time, it is necessary to establish a cross-departmental collaborative evaluation mechanism and conduct comprehensive reviews of the application effectiveness of generative AI every quarter. The review team consists of the technical department, risk control department, compliance department, and business department: the technical department evaluates the performance of the model, the risk control department verifies the effectiveness of risk control, the compliance department reviews whether it meets regulatory requirements, and the business department provides feedback on the improvement of business efficiency. At the end of each quarter, a review report is formed to continuously promote scenarios that meet the application standards, and improvement plans are formulated for non-compliant scenarios. The technical department needs to supplement data dimensions and optimize algorithms within one month, while the risk control department tracks the optimized results to ensure that generative AI applications are always consistent with business needs and compliance requirements.

6. Conclusion

The application of generative AI technology in the credit risk control of the Industrial and Commercial Bank of China has shown positive impacts in various aspects. On the one hand, this technology significantly improves the efficiency of risk control processes, especially in the credit approval process, which realizes automated processing and intelligent analysis, greatly reducing the review time. On the other hand, by integrating multiple sources of unstructured data, generative AI enhances the accuracy and comprehensiveness of risk identification, effectively reducing the non-performing loan ratio. However, this study also identifies notable gaps in data privacy protection—specifically, security risks persist in the collection, transmission, and utilization of user information and have not been fully addressed. Furthermore, the inherent "black box" nature of generative AI models leads to limited transparency in decision-making logic. This lack of transparency not only hinders internal and external audits and compliance reviews but also restricts the technology's application in high-risk approval scenarios to a certain degree. These issues indicate that the application of generative AI in risk control is still in the development and optimization stage, and systematic improvements are still needed at the technical, management, and institutional levels.

Looking ahead, the application of generative AI in credit risk control of commercial banks will be more extensive and in-depth. With the continuous optimization of algorithms and the improvement of computing power, generative AI is expected to achieve further breakthroughs in complex risk scenarios, multimodal data fusion, and real-time response capabilities. The practice of the Industrial and Commercial Bank of China provides an important reference for peers, especially indicating that only by closely integrating technological innovation with compliance management can AI maximize its effectiveness while controlling risks. In the future, the industry needs to accelerate the establishment of unified data security and model interpretable standards, and promote the formation

of a standardized and orderly AI governance environment; On the other hand, banks also need to increase their talent reserves and cross departmental collaboration to truly embed generative AI into the entire risk control process, achieving a transformation from “auxiliary tools” to “core competencies”. Ultimately, generative AI will not only help improve risk control efficiency but also potentially reshape credit assessment and risk management models, injecting new impetus into the digital transformation of the banking industry.

References

[1] Zhao H, Han Z, Yin S, et al. From interface to inference: mapping the impact of generative artificial intelligence affordances on user risk perception. Telematics and Informatics, 2025, 10.1016.

[2] Zhai Ji. Exploration on the Application of Generative Artificial Intelligence in Commercial Banks. Agricultural Bank Journal, 2025, (04): 23 - 27.

[3] Wang Fangfang, Zhang Fu. The opportunities, risks, and responses of empowering enterprise financial management with generative artificial intelligence. Chinese Market, 2025, (08): 110 - 113.

[4] Li Huayi. Generative Artificial Intelligence and Accounting Transformation in Commercial Banks. Financial Accounting, 2025, (06): 26 - 32.

[5] Lin Zhaoyu. Research on the challenges, opportunities, and response strategies of generative AI in the accounting industry. Brand Marketing for Time-Honored Brands, 2025, (18): 37 - 39.

[6] Wang T, Zhang Y, Qi S, et al. Security and privacy on generative data in AIGC: A survey. ACM Computing Surveys, 2025, 57 (4): 101145.

[7] Ouyang Rihui, Gong Wei. Digital Credit, Algorithmic Discrimination, and Dynamic Competition Policy. Nankai Journal (Philosophy and Social Sciences Edition), 2022, (01): 78 - 92.

[8] Ullrich C. A risk-based approach towards infringement prevention on the internet: adopting the anti-money laundering framework to online platforms. International Journal of Law and Information Technology, 2018, 26 (3): 226 - 251.

[9] Lv Zhongtao. The application and prospect of AI large models in the financial industry: A case study of Industrial and Commercial Bank of China. New Finance, 2024, (10): 7 - 9.

[10] Jia B, Zhang X, Liu J, et al. Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. IEEE Transactions on Industrial Informatics, 2022, 18 (6): 4049 - 4058.