GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Journal of Computer, Signal, and System Research

Article

Research on Privacy-Preserving Sharing and Collaborative Computing of Transaction Data for Intelligent Risk Control

Zhijian Liu [1,*]

[1] Tsinghua University, Beijing, China
* Correspondence: Zhijian Liu, Tsinghua University, Beijing, China

Abstract: This paper conducts a systematic study of the challenges in privacy-preserving sharing of transaction data faced by the financial intelligent risk control sector. It first analyzes how data silos lead to specific operational bottlenecks, including fraud detection models that "cannot see and cannot track", credit assessment that "cannot clearly perceive and cannot accurately evaluate", and group-wide risk management that "cannot fully observe and cannot effectively prevent". It also reveals the dual dilemma of traditional plaintext data-sharing models in terms of legal compliance and commercial trust. On this basis, the paper proposes an "One Core, Two Wings, Three Drivers" application framework for privacy-preserving collaborative computing designed to resolve these conflicts. This framework takes business value and joint risk prevention as its core objective, supported by two wings-technical integration and governance collaboration-and driven by three key elements: scenarios, compliance, and performance. The paper provides a systematic and actionable theoretical reference and practical solution for financial institutions to achieve secure data value circulation and collaborative intelligent analytics across institutions and scenarios, while strictly adhering to data security and privacy compliance requirements.

Keywords: intelligent risk control; privacy-preserving computing; data sharing; collaborative computing; federated learning; secure multi-party computation

1. Practical Dilemmas and Deep-Rooted Conflicts in Privacy-Preserving Sharing of Financial Transaction Data

With the rapid digitalization of financial services, transaction data have become a core production factor for intelligent risk control. However, the expansion of data-driven risk management is increasingly constrained by structural conflicts between data utilization demands and privacy protection requirements. In particular, the contradiction between the need for cross-institutional data collaboration and the strict boundaries imposed by compliance, security, and commercial interests has emerged as a fundamental bottleneck. These tensions are not merely technical in nature but are deeply embedded in institutional arrangements, governance mechanisms, and trust structures within the financial ecosystem.

1.1. Data Bottlenecks in the Deepening of Intelligent Risk Control

The effectiveness of intelligent risk control systems relies heavily on the comprehensive integration and joint analysis of large-scale, high-dimensional, and heterogeneous data sources. As financial activities become more interconnected and digitally mediated, risk behaviors increasingly exhibit cross-platform, cross-institutional, and cross-scenario characteristics. Nevertheless, persistent data silos significantly limit the ability of financial institutions to respond to such complex risk patterns.

In the context of fraud detection, criminal groups often exploit fragmented financial infrastructures by orchestrating activities across multiple banks, third-party payment

Received: 06 November 2025
Revised: 26 November 2025
Accepted: 24 December 2025
Published: 29 December 2025

systems, and e-commerce platforms. These groups typically adopt mobile, organized, and adaptive strategies, rapidly shifting transaction paths and operational nodes to evade detection. When fraud detection models are trained solely on the closed internal data of a single financial institution, they can only capture localized and incomplete behavioral traces. As a result, the underlying association networks and full transaction chains of cross-domain criminal activities remain obscured. This structural blindness prevents risk control systems from forming a holistic understanding of group-level dynamics and significantly weakens their ability to respond in a timely manner, leading to delayed identification and intervention in emerging fraud schemes [1].

A similar limitation is evident in credit risk assessment. For small and micro enterprises, as well as individuals with limited credit histories, commonly referred to as "thin-file" customers, internal financial data alone are often insufficient to reflect their true operating conditions, cash flow stability, or repayment capacity. The absence of external transactional, behavioral, or supply-chain-related information makes it difficult for financial institutions to construct accurate and robust risk profiles. Consequently, credit evaluation outcomes may either underestimate potential risks, resulting in elevated default exposure, or overestimate uncertainty, leading to excessive risk aversion and constrained access to financial services. In both cases, the effectiveness and inclusiveness of intelligent risk control are undermined by data incompleteness.

1.2. The Dual Dilemma of Traditional Data-Sharing Models

To alleviate data bottlenecks, the financial industry has historically explored traditional data-sharing approaches, including plaintext transmission of raw data and direct data package transactions. While these methods appear straightforward, they face an inherent and difficult-to-resolve dual dilemma in practical implementation.

The first dimension of this dilemma is legal and compliance-related. Direct sharing or trading of raw financial transaction data that contain personal identifiable information and sensitive business details conflicts with fundamental regulatory principles such as data minimization, purpose limitation, and differentiated authorization. Financial transaction records often reflect highly sensitive aspects of individual behavior and corporate operations. Once transmitted in plaintext form, such data are exposed to risks of unauthorized access, secondary use beyond the original purpose, and cross-border compliance violations. Moreover, operational data that reveal pricing strategies, customer structures, or internal processes may constitute corporate trade secrets. Improper handling of such information exposes institutions to substantial compliance costs, administrative penalties, and litigation risks, ultimately threatening the sustainability of their data-driven business models.

The second dimension is the commercial and trust-related dilemma. From the perspective of data providers, traditional sharing models imply a loss of effective control once data leave the original domain. Shared data can potentially be duplicated, redistributed, or repurposed without adequate oversight, leading to the depreciation of core data assets and heightened risks of privacy leakage. The lack of transparent and enforceable mechanisms to ensure proper data use erodes inter-institutional trust and significantly weakens the willingness of market participants to engage in data collaboration. As a result, even when technical sharing is feasible, practical cooperation often remains limited and fragmented.

1.3. New Opportunities Brought by Collaborative Computing Technologies

Recent advances in privacy-preserving collaborative computing technologies provide new technical pathways to address the aforementioned dilemmas and reconcile the tension between data utilization and data protection. These technologies shift the paradigm from "data sharing" to "value sharing", enabling joint computation and model optimization without direct exposure of raw data.

Federated learning allows participating institutions to retain data locally while collaboratively training machine learning models through the exchange of encrypted intermediate parameters, such as gradients or model weights. By aggregating local training results rather than raw datasets, federated learning enables the construction of more comprehensive and generalized models across institutional boundaries. This approach effectively realizes the principle that data remain within their original domains while intelligence is jointly enhanced, supporting cross-domain risk identification without violating data ownership or privacy constraints.

Secure multi-party computation further strengthens privacy guarantees by enabling multiple participants to jointly perform predefined computations on their respective private inputs. Throughout the computation process, no party gains access to the original data of others, and only the final aggregated result is revealed. This mechanism supports encrypted joint statistics, risk scoring, and rule evaluation, making it possible to conduct collaborative analysis under strict confidentiality conditions.

Trusted execution environments complement these approaches by providing hardware-level isolated secure zones in which sensitive data and code can be processed with assured confidentiality and integrity. By protecting data during computation and execution, such environments reduce the risk of leakage arising from system-level vulnerabilities or malicious interference.

Together, these collaborative computing technologies offer a feasible foundation for constructing privacy-preserving data collaboration frameworks. They not only mitigate legal and commercial risks associated with traditional sharing models but also create new institutional possibilities for scalable, compliant, and trust-enhancing intelligent risk control across the financial ecosystem.

2. Framework Construction: The "One Core, Two Wings, Three Drivers" Privacy-Preserving Collaborative Computing Framework

To systematically promote the practical adoption of privacy-preserving collaborative computing in intelligent risk control, this study proposes a structured and scalable framework termed the "One Core, Two Wings, Three Drivers" model. The framework is designed to translate abstract privacy-preserving computing concepts into an operational architecture that aligns technological feasibility, regulatory compliance, and business value creation. By integrating technical workflows with governance mechanisms, the framework seeks to provide a comprehensive solution for cross-institutional risk collaboration under strict data-protection constraints.

2.1. Overall Framework Design: The "One Core, Two Wings, Three Drivers" Model

The "One Core, Two Wings, Three Drivers" framework is constructed around a clear hierarchical logic that links strategic objectives, foundational capabilities, and operational principles.

The "One Core" represents the fundamental objective of the framework, namely business value creation and joint risk prevention. Rather than pursuing data sharing as an end in itself, the framework emphasizes the realization of measurable risk-control outcomes, such as improved fraud detection accuracy, enhanced credit risk identification, and strengthened systemic risk resilience through collaborative intelligence.

The "Two Wings" constitute the essential supporting dimensions that enable the realization of the core objective. The first is the technology integration wing, which encompasses privacy-preserving computing techniques, secure communication infrastructures, and distributed model architectures. This wing ensures that collaborative risk computation can be technically executed without exposing raw data. The second is the governance collaboration wing, which provides institutional guarantees through organizational coordination, contractual arrangements, and standardized operational

rules. Together, these two wings ensure that collaborative computing is both technically viable and institutionally sustainable.

The "Three Drivers" function as guiding principles for the design, deployment, and continuous optimization of the framework.

First, the scenario-driven principle requires that collaborative computing initiatives originate from concrete business pain points, such as fraud detection, credit evaluation, or cross-institutional risk penetration analysis. This principle prevents technological abstraction detached from practical needs and ensures that model design is closely aligned with real-world risk scenarios.

Second, the compliance-driven principle treats regulatory and data-protection requirements as binding constraints rather than post hoc considerations. Compliance requirements are embedded directly into technical architectures, data-processing logic, and inter-institutional collaboration protocols, thereby reducing legal uncertainty and operational risk.

Third, the performance-driven principle emphasizes pragmatic trade-offs among computational efficiency, model accuracy, security strength, and system complexity. Instead of pursuing theoretical optimality, the framework prioritizes deployable solutions that balance effectiveness with cost and operational feasibility.

As shown in Figure 1, these elements jointly form an integrated framework in which strategic objectives, enabling conditions, and operational drivers are coherently aligned.

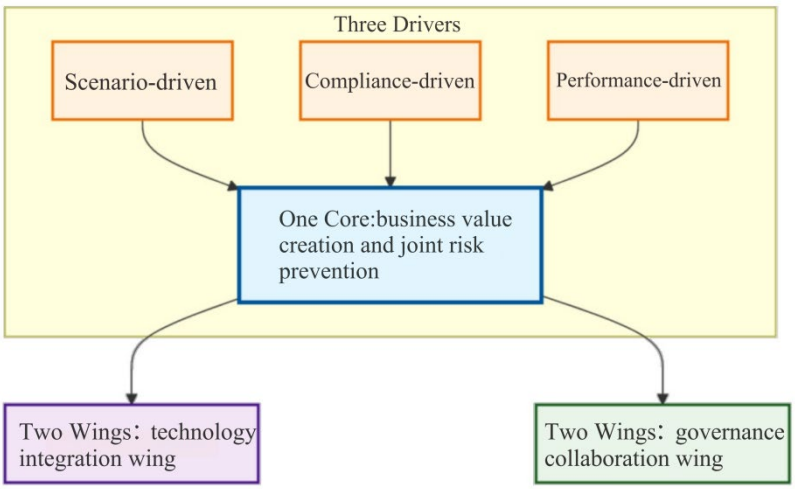

Figure 1. The "One Core, Two Wings, Three Drivers" Framework.

2.2. Core Layer: Collaborative Computing-Based Risk Control Workflow

The core layer of the framework is manifested in the end-to-end workflow of specific intelligent risk-control models built upon privacy-preserving collaborative computing technologies. This layer translates the abstract framework into executable processes that directly support risk identification and decision-making.

The first stage is task initiation and sample alignment. Participating institutions jointly determine the objectives of the collaborative task, such as detecting fraudulent transactions or assessing credit default risk. At this stage, parties also agree on feature categories, label definitions, and evaluation metrics. To ensure consistency of modeling samples without revealing full customer datasets, cryptographic techniques such as private set intersection are employed. Through encrypted matching of identifiers, shared samples are aligned across institutions while each party's complete customer list remains undisclosed.

The second stage is distributed model training and inference. Each institution independently computes gradients, intermediate statistics, or local model updates using its own plaintext data within a secure internal environment. These intermediate results are then protected using privacy-enhancing mechanisms such as homomorphic encryption or the injection of differential privacy noise. Encrypted values are transmitted via secure aggregation protocols to a coordinating entity or exchanged among participants. The coordinating process aggregates encrypted information, updates global model parameters, and redistributes them to participating institutions. This iterative process continues until model convergence is achieved [2]. During the inference phase, similar encrypted collaborative computation mechanisms are applied to generate joint risk scores for specific transactions or entities without revealing underlying data.

The third stage is output delivery and application. Upon completion of model training or inference, participants obtain either jointly optimized model parameters or encrypted risk-scoring outputs that can be locally decrypted and applied within their respective decision systems. Throughout the entire workflow, raw transaction data remain visible only within each institution's local secure domain. This design realizes a form of data value circulation that is "usable but invisible", allowing institutions to benefit from collective intelligence without compromising data sovereignty or privacy.

2.3. Support Layer: Governance and Operational Assurance Mechanisms

Beyond technical execution, the long-term stability and scalability of the privacy-preserving collaborative computing framework depend on a comprehensive governance and operational assurance system. This support layer functions as the institutional foundation that sustains trust, accountability, and interoperability among participating entities.

Organizational assurance serves as the initial pillar. Participating institutions should establish a joint operations committee composed of senior management representatives, business leaders, technical specialists, and compliance professionals. This committee is responsible for strategic coordination, resource allocation, major technical and policy decisions, and the resolution of disputes that may arise during collaboration.

Contractual assurance forms the core of institutional governance. Detailed legal agreements, potentially supplemented by automatically executable smart contracts, should explicitly define data usage boundaries, intellectual property ownership of jointly developed models, benefit-sharing arrangements, security responsibilities, penalty mechanisms for breaches, and emergency response procedures for security incidents. Such clarity reduces uncertainty and aligns incentives across institutions.

Standards assurance promotes interoperability and reduces integration costs. By adopting or jointly developing standards for feature definitions, encryption algorithm interfaces, communication protocols, and system security classifications, institutions can lower technical barriers to entry and facilitate scalable ecosystem expansion.

Finally, audit assurance introduces independent oversight across the collaborative computing lifecycle. This includes compliance audits to verify adherence to privacy and data-protection rules, algorithmic audits to assess fairness and bias risks, and security audits to evaluate resistance against external attacks and internal collusion. These mechanisms enhance transparency, reinforce mutual trust, and strengthen the overall resilience of the collaborative risk-control ecosystem.

3. Application Deepening of Collaborative Computing in Typical Intelligent Risk Control Scenarios

On the basis of the proposed privacy-preserving collaborative computing framework, this section further explores its application deepening in representative intelligent risk control scenarios. By embedding collaborative computing technologies into concrete business processes, financial institutions can overcome long-standing data fragmentation

constraints while maintaining compliance and data security. The following scenarios illustrate how different collaborative computing paradigms can be adapted to distinct risk-control objectives, highlighting both their technical feasibility and practical value.

3.1. Cross-Industry Joint Fraud Prevention and Control

In the face of increasingly organized, cross-platform, and rapidly evolving financial fraud activities, traditional single-institution risk-control approaches have proven insufficient. Collaborative computing provides an effective technical foundation for cross-industry joint fraud prevention and control by enabling multi-party behavioral correlation analysis without direct data sharing.

In a typical scenario, commercial banks, licensed payment institutions, and major e-commerce platforms jointly construct a gambling- and fraud-related transaction and syndicate association detection model based on horizontal federated learning. Each participating party contributes complementary but non-overlapping data dimensions. Commercial banks locally extract and encrypt account transaction patterns, abnormal fund-flow structures, and large-value transaction features. Payment institutions provide encrypted fast-payment sequences, transaction timing characteristics, and device-fingerprint association features. E-commerce platforms contribute encrypted shopping behavior patterns, abnormal logistics address relationships, and login-behavior anomalies. Throughout the process, raw data remain within local systems, and collaborative model training is achieved through encrypted gradient or parameter exchanges.

By integrating these heterogeneous behavioral features at the model level, the joint model can identify abnormal cross-platform fund transfers, device-sharing patterns, and address associations that are difficult to detect within isolated datasets. Compared with traditional static and lagging blacklist-sharing mechanisms, this approach shifts risk control from retrospective list matching to proactive and dynamic behavioral correlation analysis. As a result, emerging and mutating fraud schemes can be detected and suppressed at earlier stages, while personal privacy, transaction confidentiality, and commercial data interests are effectively protected.

3.2. Joint Credit Risk Control for Small and Micro Enterprises

Information asymmetry remains a core obstacle in financing for small and micro enterprises. Secure multi-party computation offers a practical pathway to integrate dispersed operational data from multiple entities into a unified credit assessment framework without exposing sensitive information.

When evaluating the creditworthiness of a small or micro enterprise, a financial institution may collaborate with relevant data holders such as taxation systems, customs information platforms, core supply-chain enterprises, and logistics service providers. Under pre-designed secure multi-party computation protocols, taxation indicators (e.g., tax payment continuity), customs indicators (e.g., declaration amounts), supply-chain indicators (e.g., order stability), and logistics indicators (e.g., shipping frequency and regularity) are processed in encrypted form within their respective systems.

Through joint encrypted computation, composite indicators reflecting the enterprise's actual operating performance can be generated, such as a continuous tax-growth index or a supply-chain stability score [3]. The final output takes the form of an encrypted joint credit evaluation result or risk score, which is disclosed only to the authorized financial institution. No participating party gains access to any other party's raw data during the computation process.

This collaborative model strictly adheres to the principles of data minimization and informed authorization, enabling fragmented public and commercial data resources to be transformed into a coherent and credible credit profile. By improving the accuracy of primary repayment source assessment, financial institutions can make more informed

lending decisions, thereby alleviating financing constraints for small and micro enterprises while preserving data sovereignty and security boundaries.

3.3. Group-Wide Penetrative Risk Management

For diversified financial holding groups, achieving penetrative and consolidated risk management across subsidiaries poses a persistent challenge. While group-level oversight requires a comprehensive view of risk exposures, regulatory and internal compliance requirements mandate strict data isolation among subsidiaries. Federated learning provides a viable solution to reconcile these competing demands.

In a group-wide risk management scenario, the group-level risk management function acts as the coordinating entity and initiates a vertical federated learning task targeting specific risk categories, such as related-party transaction risk or liquidity contagion risk. Subsidiaries, including banking, securities, and insurance units, participate by locally training sub-models or computing encrypted intermediate statistics based on their respective customer portfolios, fund flows, and transaction records [4].

Encrypted model parameters or intermediate results are securely aggregated by the group coordinator to construct a group-level global risk insight model. This model enables the identification of concealed abnormal related-party transaction patterns, shared vulnerable counterparties across subsidiaries, and potential risk contagion chains. The resulting outputs provide a panoramic view of group-wide risk exposures and generate early-warning signals for emerging systemic vulnerabilities.

Throughout the entire process, granular subsidiary-level business data remain confined to local systems, and the group-level entity accesses only aggregated and abstracted risk intelligence. This design fully aligns with compliance requirements for data segregation and subsidiary autonomy, while simultaneously enhancing the group's ability to conduct penetrative risk analysis and coordinated risk response.

4. Discussion

The empirical and scenario-based analyses presented in the previous sections indicate that privacy-preserving collaborative computing offers a feasible and scalable solution to long-standing structural challenges in intelligent financial risk control. However, beyond demonstrating applicability, it is necessary to further examine the framework from the perspectives of effectiveness boundaries, implementation conditions, and practical trade-offs, in order to provide a more comprehensive understanding of its real-world deployment.

First, from a technical perspective, the effectiveness of collaborative computing-based risk control is closely related to data quality, feature alignment, and model design consistency across participating institutions. While privacy-preserving mechanisms ensure that raw data are not exposed, they do not inherently resolve issues such as feature heterogeneity, inconsistent data semantics, or imbalanced sample distributions. In practice, insufficient feature coordination or misaligned labeling standards may weaken the marginal gains of collaboration. This suggests that collaborative computing should be accompanied by prior agreements on feature abstraction levels, data preprocessing logic, and evaluation criteria to fully realize its technical advantages.

Second, the discussion highlights the importance of cost-benefit balance in large-scale deployment. Privacy-preserving techniques such as federated learning and secure multi-party computation inevitably introduce additional computational overhead, communication latency, and system complexity. While these costs are justified in high-risk or high-value scenarios, such as fraud prevention and systemic risk monitoring, their applicability to low-frequency or low-impact risk scenarios requires careful evaluation. Therefore, scenario prioritization and phased implementation are critical to ensuring that collaborative computing delivers sustainable value rather than becoming a purely technical exercise.

Third, from an institutional and governance standpoint, collaborative computing reshapes traditional inter-organizational relationships in risk management. The framework reduces reliance on direct data ownership transfer and shifts cooperation toward jointly generated intelligence outputs. This transformation helps alleviate trust deficits among institutions but also places higher demands on governance structures. Clear responsibility allocation, transparent benefit-sharing mechanisms, and effective dispute-resolution procedures are essential to prevent coordination failures and ensure long-term cooperation stability.

Finally, it is worth noting that collaborative computing does not replace existing internal risk-control systems but rather complements them. Its value lies in extending the analytical boundary of individual institutions, enabling them to perceive cross-domain risk signals that are otherwise inaccessible. As such, collaborative computing should be embedded into a layered risk-control architecture, where local models and collaborative models interact in a coordinated manner. This integrated approach can enhance overall risk sensitivity while preserving institutional autonomy and compliance integrity.

5. Conclusion

This study proposes the "One Core, Two Wings, Three Drivers" privacy-preserving collaborative computing framework as an integrated methodological approach for intelligent risk control in the financial industry. By systematically aligning business objectives, technical architectures, and governance mechanisms, the framework provides a coherent pathway that bridges top-level design and practical deployment. It shifts the focus of data collaboration from direct data exchange to value-oriented joint computation, offering a structured solution to the long-standing tension between data utilization efficiency and privacy protection requirements.

Through in-depth analysis of representative application scenarios, including cross-industry joint fraud prevention and control, collaborative credit risk assessment for small and micro enterprises, and group-wide penetrative risk management, this study demonstrates the practical feasibility and effectiveness of collaborative computing under strict data-protection constraints. Across these scenarios, the framework enables the integration of heterogeneous and fragmented data resources at the model and computation levels rather than at the data level. As a result, intelligent risk control systems can achieve broader coverage, higher accuracy, and stronger timeliness, while ensuring that raw transaction data remain confined within local secure domains. This approach effectively realizes the principle that data remain static while analytical value flows across institutional boundaries, strengthening both risk identification capability and compliance assurance.

From an institutional perspective, the framework highlights the importance of coupling technical solutions with governance arrangements. Organizational coordination, contractual safeguards, standardized technical interfaces, and independent audit mechanisms jointly constitute the operational foundation for sustainable collaboration. These elements not only mitigate legal and commercial risks but also foster mutual trust among participating institutions, thereby enhancing the long-term viability of collaborative risk-control ecosystems.

Looking forward, the continued evolution of privacy-preserving computing technologies, the gradual improvement of technical and operational standards, and the maturation of cross-institutional cooperation mechanisms are expected to further expand the applicability of collaborative computing in financial risk management. As these conditions advance, the proposed framework can serve as a reference model for supporting the digital transformation and high-quality development of the financial industry, enabling more resilient, inclusive, and forward-looking intelligent risk control practices.

References

1. M. R. Sumalatha, A. Kumar, N. Janardhanan, and S. Abhinash, "Blockchain Based Privacy Preservation and Misbehavior Analysis in Financial Supply Chain," In *International Conference on Optimization and Data Science in Industrial Engineering*, November, 2023, pp. 231-248. doi: 10.1007/978-3-031-81458-7_14
2. P. Chatzigiannis, W. C. Gu, S. Raghuraman, P. Rindal, and M. Zamani, "Privacy-enhancing technologies for financial data sharing," *arXiv preprint arXiv:2306.10200*, 2023.
3. M. Qiu, K. Gai, H. Zhao, and M. Liu, "Privacypreserving smart data storage for financial industry in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 5, p. e4278, 2018. doi: 10.1002/cpe.4278
4. K. Savchuk, S. Rzaieva, T. Savchenko, and D. Rzaiev, "Data Protection Strategies and Technologies for Ensuring National Financial Security," In *Innovative and Intelligent Digital Technologies; Towards an Increased Efficiency: Volume 1*, 2024, pp. 431-440. doi: 10.1007/978-3-031-70399-7_32