Journal of Electronic Research and Application, 2026, Volume 10, Issue 8
http://ojs.bbwpublisher.com/index.php/JERA
Online ISSN: 2208-3510
Print ISSN: 2208-3502

Research on a Trustworthy Collaborative Computing Mechanism for Cross-Domain Sensitive Data Based on Secure Multi-party Computation

Hao Yang, Mutong Chen, Xiong Ni

Shanghai Municipal Big Data Center, Shanghai 200072, China

Abstract: In the digital economy era, cross-domain data circulation has shifted from traditional data exchange to value-based collaborative computing. Cross-institutional data in scenarios such as shipping trade, financial risk control, government supervision, and supply chain collaboration possess characteristics of high sensitivity, strong ownership, and high compliance constraints. Direct sharing of raw data can easily lead to issues such as leakage of commercial secrets, exposure of customer resources, violation of cross-border data regulations, and ambiguity in liability determination. Secure Multi-Party Computation (MPC), with its characteristics of "data not leaving the domain, value can be calculated, and results can be trusted", has become the core privacy-enhancing technology for resolving the core privacy challenges in cross-domain sensitive data collaboration. This paper takes secret sharing, obfuscation circuits, and inadvertent transmission as the core protocols, integrates blockchain, DID, and smart contract technologies, builds a trusted collaborative computing mechanism for sensitive data across various domains, and constructs a standardized task lifecycle and on-chain-off-chain collaborative governance system. By verifying the effectiveness of the mechanism in four typical industry scenarios, it systematically analyzes the core bottlenecks in the implementation of the MPC project, such as performance, standardization, malicious protection, and result inference, and proposes template compilation, verifiable auditing, and privacy governance optimization solutions, providing a reference for the construction of a trusted collaborative infrastructure for privacy data across various domains.

Keywords: Secure multi-party computation; Cross-domain data circulation; Sensitive data; Secret sharing; Garbled circuits; Blockchain; DID; Trusted collaborative computing

Online publication: Sept 3, 2026

1. Introduction

The core contradiction of cross-domain data collaboration lies in the conflict between data value extraction and the protection of original data privacy. Entities in sectors such as shipping, finance, government affairs,

and supply chain have independent ownership rights and prominent data barriers. Various business data are highly sensitive and subject to strict compliance constraints. Traditional blockchain and DID technologies can only achieve process evidence and identity authorization, but cannot solve the privacy protection problem of joint computing of multiple private data. Therefore, this paper takes MPC as the core cryptographic computing layer and builds a cross-domain trusted collaborative computing mechanism. Under the premise of retaining the original data locally, it realizes multi-party joint verification, risk scoring, statistical analysis, and rule matching, effectively balancing the demand for data value release and privacy security control [1].

2. Related work

2.1. MPC basic protocols

The core goal of MPC is to enable multiple mutually untrusting parties to collaboratively complete a pre-specified function computation, with each participant only obtaining the agreed-upon result and unable to steal or infer others' private data. Classical theories form a complete technical foundation: Shamir's threshold secret sharing enables secure data splitting and threshold reconstruction, ensuring static privacy security; Yao's garbled circuits enable Boolean privacy computing without data sharing; GMW and BGW protocols extend secure computation to general multi-party scenarios; Oblivious Transfer (OT) provides underlying support for privacy-preserving matching and circuit computation; Beaver triple pre-processing significantly reduces online computational overhead; and maliciously secure protocols like SPDZ, relying on offline pre-processing and message authentication mechanisms, can resist input forgery, result tampering, and node collusion attacks, making them suitable for high-security-level cross-domain sensitive data trusted collaboration scenarios.

2.2. MPC engineering systems and hybrid protocol frameworks

Currently, MPC (Multi-Party Computation) has moved from theoretical demonstration to practical implementation, forming a mature framework for executing mixed protocols. Mainstream open-source systems such as ABY, MP-SPDZ, and ABY2.0 integrate multiple cryptographic protocols, supporting dynamic mixed arrangements of arithmetic sharing, Boolean sharing, and Yao circuits. They can be seamlessly adapted to complex business functions such as numerical statistics, size comparison, conditional branching, rule matching, and set retrieval. The systems generally come equipped with optimization capabilities such as offline preprocessing, GPU parallel acceleration, communication compression, and dynamic bandwidth adaptation. They can flexibly switch between semi-trustworthy and malicious security protection mechanisms according to the security level of the business. Compared with a single protocol architecture, a hybrid protocol can automatically select the most suitable protocol based on the characteristics of sub-tasks, reducing the cost of domain transitions and significantly reducing the computational power consumption and communication delay of complex cross-domain tasks. This engineering system provides a reusable and iterative technical foundation for highly complex cross-domain scenarios, effectively promoting MPC from a laboratory prototype to industry-scale commercial application [2].

2.3. MPC data analysis and standardized governance

Since 2020, MPC has been deeply integrated with big data and artificial intelligence, giving rise to the privacy machine learning system. Systems such as CrypTFlow, Delphi, and CrypTen can perform model

privacy inference and lightweight training, and are suitable for intelligent risk control, anomaly identification, and other business applications. Compared with federated learning, which relies on model parameter aggregation and has the risk of gradient leakage, MPC can achieve privacy-preserving collaborative computing at the original feature level, with finer data protection granularity and stronger security. At the standardization level, NIST has incorporated MPC into the privacy-enhanced cryptographic tool system. The DID/VC standard of W3C provides regulatory support for cross-domain identity authorization. Combined with the ISO security and privacy system, it forms a dual guarantee of technology and system. Compared with homomorphic encryption, TEE, and zero-knowledge proof, MPC is more suitable for multi-party peer-to-peer joint computing. It can deeply collaborate with blockchain and smart contracts to build a complete cross-domain sensitive data trusted collaboration system, effectively solving the cross-domain trusted collaboration pain points of missing mutual trust among multiple parties, complex data ownership, and strict compliance requirements.

3. Problem analysis of trusted collaborative computing for cross-domain sensitive data

3.1. Participants and data characteristics

Participants in cross-domain sensitive data trusted collaboration can be categorized into five types: data holders, data users, data authorizers, regulatory auditors, and technical service providers. Each entity has independent rights and responsibilities, providing mutual checks and balances. Collaborative data—such as shipping trade documents, financial transactions, government regulatory data, and supply chain logistics—possesses characteristics of low individual-source value but high multi-source fusion value, strict ownership, and strong confidentiality requirements. Traditional centralized data sharing models easily lead to privacy breaches and compliance risks, failing to meet the business and security needs of cross-domain multi-party collaboration.

3.2. Threat model

This paper constructs a dual-layer threat model combining algorithms and governance, covering core risks in cross-domain trusted collaboration. The algorithmic aspect includes two types of attacks: semi-honest and malicious. The semi-honest model follows the protocol but attempts to steal logs and infer privacy; the malicious model can forge inputs, tamper with results, terminate the protocol, and collude for espionage, and is the core protection target for sensitive business. The governance and operation maintenance aspect also has derivative risks, including leakage of task metadata revealing business relationships, false inputs generating invalid results, fine-grained queries triggering differential inference, inconsistent log data across private networks, and ambiguity in multi-party rights and responsibilities making accountability difficult [3].

3.3. Core requirements and constraints

By integrating cross-domain business and security standards, this article has distilled six core requirements: First, local input confidentiality - the original data does not leave the local domain, and cross-domain data transmission only involves protocol protection; second, trustworthy calculation results - accurately resist malicious tampering and false input, ensuring calculation consistency; third, verifiable and controllable authorization - relying on DID/VC to clearly define the scope, scenarios and validity period of data usage;

fourth, minimum result disclosure - only output the coarse-grained results necessary for the business, preventing detailed leakage and reverse inference; fifth, full traceability - store all process information on the chain for evidence, enabling traceability of anomalies and determination of responsibility; sixth, deployment compatibility and adaptation - can be adapted to multiple types of private network environments, supporting stable access of multiple formats of data.

4. Design of MPC-based trusted collaborative computing mechanism

4.1. Overall architecture

This paper constructs a four-layer closed-loop collaborative architecture to achieve deep coupling of privacy computing and governance processes, as well as hierarchical division of responsibilities and full-process controllability. The governance management layer serves as the top-level constraint system. It relies on DID/VC to realize trusted identity identification and refined permission definition across institutions and systems. Through the unified registration of various sensitive data in the global data directory, the semantics of fields, confidentiality level, applicable scenarios, and authorization constraints are defined. The task access rules, frequency limits, data scope, and compliance boundaries are solidified by smart contracts. The MPC task layer, as the core computing core, is responsible for abstracting fragmented business requirements into standardized and compliant task templates, automatically completing protocol intelligent selection, offline cryptographic material preprocessing, online privacy computing, and output granularity control. The cross-domain node layer enables each entity to complete data cleaning, compliance verification, field de-sensitization, and share encoding within the local security domain. It achieves cross-domain trusted communication through encrypted channels and ensures the retention of original data at the physical level. The result auditing layer realizes minimized disclosure of calculation results, hash chain-based evidence storage, and complete archiving of operation logs, providing fallback support for post-event compliance audits, business dispute resolution, and precise determination of responsibilities [4].

4.2. Full task lifecycle

This paper designs an eight-stage standardized task lifecycle to achieve controllable and auditable privacy computing throughout the process. The process is as follows: The data holder completes the registration of data capabilities; The user initiates the task application and completes the authorization of ownership; The smart contract verifies compliance and triggers the task; Each node locally completes data verification and share processing; The system matches the optimal protocol and completes offline preprocessing; Nodes exchange protocol data and conduct online secure computing; The authorization entity obtains the minimized disclosure result; Finally, the task data and logs are archived on the chain, handling abnormal risks, and throughout the process, no original data is transferred across domains.

4.3. Core protocol adaptation paths

For differentiated business scenarios, this paper designs four types of dedicated protocol paths to balance security and performance. The secret sharing path is suitable for arithmetic tasks such as multi-party statistics and risk scoring, and reduces computational costs by relying on threshold sharing and Beaver triplets; the obfuscation circuit path is suitable for Boolean tasks such as document verification, numerical comparison, and rule judgment, ensuring the privacy security of logical computing; the oblivious transmission path

realizes private set intersection based on OT extension, suitable for scenarios such as blacklist matching and duplicate financing identification; the hybrid protocol path uses the ABY architecture to achieve dynamic conversion of multiple protocols, suitable for complex risk control and supervision tasks that involve statistics, judgment, and matching [5].

4.4. On-chain/off-chain synergy mechanism

This paper proposes a collaborative model of "chain-based management of processes and offline calculation of privacy", which balances the requirements of privacy protection and compliance auditing. The blockchain and smart contracts only store management data such as task numbers, DID identities, authorization summaries, result hashes, and audit logs, without retaining original data or secret shares. This avoids the risk of transparent leakage on the chain. The DID/VC system realizes multi-level identity control and traceable authorization, and supports permission revocation. The smart contracts automatically complete task access, process arrangement, and abnormal monitoring, replacing manual review and achieving standardized and auditable operation of the privacy computing process.

4.5. Cross-network deployment and evaluation system

This article adopts a localized node deployment model. Each participant deploys MPC nodes in their own secure domain to achieve local data control and completely avoid the risks of aggregation leakage and over-range usage brought by traditional centralized data platforms. The nodes complete cross-domain trusted communication through security gateways and encrypted dedicated lines. They adopt two-way identity authentication, traffic auditing, and abnormal breakage mechanisms, transmitting only protocol messages and audit summaries, thus eliminating the risk of data leakage in centralized storage. At the same time, a multi-dimensional evaluation system is established. From five dimensions, including privacy security, computational correctness, running performance, business adaptability, and compliance governance, the security, stability, and practicality of the mechanism are quantitatively evaluated. It is adapted to heterogeneous cross-domain deployment scenarios such as government dedicated networks, financial intranets, and enterprise private clouds, effectively solving the data collaboration problems in multi-network isolation environments.

5. Cross-domain application scenarios

5.1. Joint verification of shipping trade document authenticity

Shipping trade document verification is a critical requirement for trade financing and warehouse receipt pledging, where traditional sharing models carry significant forgery and leakage risks. Based on the mechanism proposed in this paper, entities such as shipping companies, ports, customs authorities, and warehousing institutions locally submit authorized fields. Through OT-based set matching, garbled circuits, and secret sharing, they perform document consistency comparisons, interval checks, and pledge risk scoring. The system outputs only the verification conclusion and risk level to banks, without disclosing document details or commercial data, effectively preventing fraudulent trade and duplicate pledging risks while balancing financial security, data privacy, and government compliance requirements.

5.2. Financial joint risk control and credit assessment

Joint financial risk control has long faced the challenges of cross-institutional data silos and compliance constraints. The mechanism proposed in this paper enables privacy-preserving collaborative computing of data from banks, logistics, taxation, and insurance. Each institution retains its data locally throughout the process. Through a hybrid protocol, it achieves multi-dimensional feature fusion, enabling risk control functions such as enterprise credit scoring, duplicate financing screening, and false transaction identification. The system only outputs score ranges, risk levels, and admission conclusions, effectively avoiding the risk of data leakage of customers and transactions, breaking through the limitations of a single data source, and significantly improving the accuracy and compliance of cross-domain risk control.

5.3. Government joint supervision and risk identification

There are problems such as data fragmentation among multiple departments and insufficient collaborative investigation in government supervision. The data of different departments cannot be compliantly shared, resulting in missed detection of abnormal risks for enterprises. Relying on the MPC mechanism, departments such as customs, taxation, market supervision, and maritime affairs do not need to share detailed data. They can jointly identify high-risk behaviors such as abnormal customs declarations, invoice violations, abnormal trajectories, and cumulative penalties across departments, and only output risk clues and regulatory marks. By integrating smart contracts to solidify regulatory authorization and processes, we can achieve full traceability and clear rights and responsibilities, addressing the pain points of "lack of willingness to share and difficulty in collaboration" in government data, and supporting precise and compliant cross-departmental joint supervision.

5.4. Supply chain collaborative analysis

In the financial scenarios of supply chain and industrial chain, enterprise operation data is highly sensitive, and there is a high risk of data sharing. Data barriers restrict the implementation of risk sharing and inclusive finance. Traditional supply chain collaboration mainly relies on the centralized collection of data by core enterprises, which easily leads to the monopoly and abuse of business information by upstream and downstream small and medium-sized enterprises, and poses significant compliance and privacy risks. This mechanism enables collaborative analysis of supply chain privacy. Each participant locally uploads the authorization fields, and through MPC, it can complete order verification, inventory assessment, performance scoring, and accounts receivable verification. Only aggregated indicators, warning levels, and financing suggestions are output, without disclosing the detailed business data of the enterprises. This model can effectively break down the data barriers in the supply chain, balance the risk control requirements of the core enterprises with the privacy rights of small and medium-sized enterprises, and assist in the risk management of the industrial chain. It can be widely applied to multiple industries such as manufacturing, cross-border e-commerce, and energy.

6. Challenges and outlook

At present, there are still significant engineering and governance bottlenecks in the cross-domain large-scale application of MPC, which restrict the large-scale implementation of the technology. Firstly, the heterogeneous network environment across different specialized networks is complex. The isolation degrees

of government affairs, finance, and enterprise networks are high, and the communication delay and jitter are large. The optimal performance in the laboratory cannot be replicated in real cross-domain scenarios, and the overall computing efficiency is limited. Secondly, the industry data standardization system is lacking. The field definitions and risk statistics standards of each institution are not unified, resulting in poor generalizability of MPC task templates, high customization costs, and difficulty in batch reuse. Thirdly, the data authenticity governance is weak. MPC can only guarantee the privacy and security of the computing process, but it cannot actively identify deliberate falsification by participants, field mismatches, or selective submission of data, leading to potentially unsafe but ineffective computing results. Fourthly, fine-grained and frequent repeated queries can be achieved through differential iteration for reverse data inference, and there is a risk of implicit privacy leakage. Fifthly, the balance between chain-level transparent evidence storage and privacy protection is difficult. Blockchain is suitable for evidence storage and auditing, but the chain-level information is permanently visible, and the task frequency, participant relationships, and result summaries may also constitute sensitive metadata, posing a leakage risk. Sixthly, the industry standard evaluation benchmarks, performance specifications, and regulatory explainability systems are not yet complete, which is not conducive to compliance implementation and industry promotion.

To address these bottlenecks, future optimization and iteration can be carried out in four aspects: Firstly, by combining GPU acceleration and batch processing optimization to reduce computing power and communication costs, and improving deployment stability; Secondly, unifying industry data semantics and computing standards, and building a reusable privacy computing function library that can be compiled and reused; Thirdly, constructing a dual mechanism of protocol protection and governance constraints, through input commitment, on-chain verification, DID responsibility binding, anomaly detection, post-event inspection, and differential privacy to prevent data fraud and privacy inference risks; Fourthly, improving the industry standard evaluation and auditing system, and building a traceable and supervisable cross-domain trusted collaborative infrastructure.

7. Conclusion

This paper addresses the challenges of cross-domain sensitive data collaboration, confidentiality, and auditability by constructing an MPC-based trusted collaborative computing mechanism. The mechanism integrates blockchain, DID, and smart contract technologies to achieve notarization, auditing, process control, and identity authorization, forming a closed-loop model of “on-chain governance, off-chain privacy computation”. It achieves the goals of data not leaving its domain, value being computable, processes being auditable, and accountability being traceable. This alleviates the contradiction of cross-domain data that “cannot be shared but needs collaboration”, and is particularly suitable for scenarios such as joint verification of shipping trade document authenticity, financial joint risk control and credit assessment, government joint supervision and risk identification, and supply chain collaborative analysis. The paper identifies core issues in MPC deployment, including performance, standardization, and data quality, and clarifies future optimization directions, providing both theoretical and practical support for compliant cross-domain privacy data collaboration and large-scale privacy-preserving computation deployment.

Funding

2024 National “Blockchain” Key Special Project “Key Technology Research on Cross-Sector Data Access and Circulation Management for Shipping Trade” (Project No.: 2024YFB2705403)

Disclosure statement

The authors declare no conflict of interest.

References

[1] Shamir A, 1979, How to Share a Secret. Communications of the ACM, 22(11): 612–613.

[2] Yao A, 1982, Protocols for Secure Computations. Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, 160–164.

[3] Yao A, 1986, How to Generate and Exchange Secrets. Proceedings of the 27th Annual Symposium on Foundations of Computer Science, 162–167.

[4] Goldreich O, Micali S, Wigderson A, 1987, How to Play Any Mental Game. Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 218–229.

[5] Ben-Or M, Goldwasser S, Wigderson A, 1988, Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. Proceedings of the 20th Annual ACM Symposium on Theory of Computing, 1–10.