# Research on Data Trusted Sharing Mechanism Based on Trusted Data Space in the Defense Industry

Yuwei Chen[1,a], Songzi Cao[1,b], Zunpeng Yu[1,c], Ning Luo[2,d*]

[1]China Academy of Industrial Internet, Beijing, China
[2]China Changfeng mechanics and electronics technology academy, Beijing, China

[a]chenyuwei@china-aii.com, [b]caosongzi@china-aii.com
[c]yuzunpeng@china-aii.com, [d*]358989910@qq.com

**Abstract.** The military-industrial sector's data sharing faces core challenges such as data silos, lack of standardized protocols, and absence of trust mechanisms. Based on the theory of Trusted Data Spaces, this paper analyzes the current status and pain points of data sharing in the military-industrial sector, explores the suitability of Trusted Data Spaces for the military-industrial domain, and proposes a data-trustworthy sharing mechanism tailored for closed and confidential scenarios in the military-industrial sector. This mechanism leverages technologies such as identity authentication, digital contracts, and audit trail to effectively address data circulation issues between parent companies and their subsidiaries, as well as in edge computing environments. The research findings indicate that this mechanism can enhance the efficiency of data sharing and multi-party collaboration, providing a valuable reference for secure data transmission and sharing in the military-industrial sector.

**Keywords:** Trusted Data Space, military industry, data sharing

## 1 Introduction

As a critical sector for national security and technological advancement, the defense industry features highly sensitive and complex data management. Against the backdrop of accelerating digital transformation, the defense industry is increasingly reliant on data as a key production factor [1]. From weapon and equipment research, design, and development to manufacturing, from testing and verification to operation and maintenance support, every stage generates massive volumes of data resources. However, constrained by the industry's unique characteristics, most of these data resources remain isolated, making it difficult to achieve synergistic effects. As a result, large amounts of data resources fail to be effectively shared, leading to underutilization of data's full potential and severely hampering the industry's innovation capacity and development efficiency. The special nature of defense industry data dictates that it must adhere to stringent security standards during transmission and storage; any potential risk of data


L. W. Koon et al. (eds.), *Proceedings of the 2026 7th International Conference on Management Science and Engineering Management (ICMSEM 2026)*, Advances in Economics, Business and Management Research 399,
https://doi.org/10.2991/978-94-6239-758-3_25

leakage could lead to immeasurable losses. Therefore, exploring a secure and trustworthy data-sharing mechanism has become a critical issue urgently needing resolution in the defense industry.

In recent years, both academia and industry have proposed a variety of approaches and technologies to address the issue of data sharing. Traditional centralized data exchange platforms carry a high risk of single-point failure and struggle to meet the military-industrial sector's stringent requirements for high reliability. Federated learning, due to its algorithmic complexity and high computational resource demands, has been limited in its adoption in resource-constrained environments. Although blockchain technology excels in data security, its decentralized nature clashes with the highly centralized management models prevalent in the military-industrial sector. As a new type of infrastructure, the Trusted Data Space integrates privacy-preserving computation and data monitoring technologies, offering a fresh approach to secure and trustworthy data exchange and providing a novel technological pathway to overcome the challenges of data sharing in the military-industrial sector. This article, based on the theory of Trusted Data Spaces, explores solutions suitable for relatively closed and confidential scenarios in the defense industry.

Data Trustworthy Sharing Mechanism. The research primarily focuses on the following aspects: analyzing the current status and pain points of data sharing in the defense industry; exploring the suitability of trusted data spaces for the defense sector; designing a data trustworthy sharing mechanism based on trusted data spaces; and, in light of the specific business characteristics of the defense industry—such as regional-center, group-subsidiary enterprise, and edge scenarios—demonstrating the effectiveness of this mechanism in practical application scenarios. This paper places particular emphasis on the security and efficiency issues associated with data sharing in multi-party collaboration.

## 2 Current Status and Pain Points Analysis of Data Sharing in the Military Industry

### 2.1 Current Development Status at Home and Abroad

**Current Development Status Abroad.**

Developed countries in Europe and the U.S. started earlier in the field of military-industrial data sharing and have already established relatively mature technological systems. Through the Joint Information Environment (JIE) program, the U.S. Department of Defense has achieved data interconnectivity across services and departments, adopting a zero-trust architecture to ensure secure data access [2]. The NATO has established a coalition data-sharing framework that supports secure data exchange among member countries; however, coordination challenges remain regarding data sovereignty and access control [3]. Europe, via the Gaia-X project, is exploring the development of industrial data spaces, providing a reference paradigm for data sharing in the military-industrial sector. Yet, its openness clashes to some extent with the confidentiality requirements of the military-industrial complex [4].

**Current Development Status in China.**

In recent years, China's defense industry has made significant progress in building data-sharing capabilities. In terms of data platforms, several major defense conglomerates have established unified data-management platforms, enabling centralized management of certain types of data within their organizations. Regarding communication and transmission, military communication networks now cover multiple links—including fiber optics, satellites, and wireless—yet bandwidth bottlenecks still persist when it comes to cross-domain data transmission. As for standards and regulations, the state has successively introduced legal frameworks such as the "Data Security Law" and the "Cybersecurity Law," providing institutional safeguards for data sharing in the defense industry. However, the industry-level data-sharing standard system remains incomplete [5].

## 2.2 Challenges in Implementing Military Industrial Projects

**Challenges in Data Platform Development.**

The product data management system (PDM), enterprise resource planning system (ERP), and manufacturing execution system (MES) in the defense industry enterprise operate independently, lacking unified data interfaces and standards, which has led to a prominent phenomenon of data silos among these systems [6]. During the development of master data, a certain defense industry enterprise discovered significant differences in data formats and definitions across various departments, resulting in high costs for data integration. Moreover, the existing data management platform has limited security protection capabilities; as a result, when dealing with highly sensitive data, the enterprise still tends to rely on manual handover methods, thereby hindering data sharing.

**Challenges in Communication Transmission.**

Military-industrial projects cover a wide geographic area, and some production bases are located in remote regions with weak network infrastructure, making it difficult to ensure the stability of data transmission. Edge devices are typically deployed in complex environments where network connections may be unstable, and the volume of data generated is enormous. Thus, efficiently collecting, storing, and transmitting edge data has become a significant challenge [7]. In high-concurrency scenarios, the throughput and latency of existing communication protocols may fail to meet the military industry's requirements for real-time data processing.

**Challenges in Security Management and Control.**

Military-industrial data involves national security and commercial secrets, and all participating parties are highly sensitive to the security and privacy protection of such data. The existing data-sharing mechanisms lack sufficient security safeguards, causing enterprises to adopt a cautious attitude toward the risks associated with data sharing. Moreover, the standards for classifying and grading data are not uniform, and there is a lack of clear regulations regarding transmission channels and encryption strengths for

data at different classification levels, thereby increasing the complexity of security management [8].

### 2.3 Pain Points in Data Sharing and Circulation

**Lack of a Trust Mechanism.**

Lack of trust is one of the key factors hindering data sharing. Due to the absence of a credible third-party oversight mechanism, data providers find it difficult to verify the true intentions and scope of data usage by data users, worrying that their data might be misused or leaked [9]. In cross-organizational collaboration scenarios, establishing trust among participating parties involves high costs and lengthy negotiation periods, thereby affecting the efficiency of project advancement.

**Unclear Definition of Rights and Responsibilities.**

In the process of data sharing, unclear definitions of ownership, usage rights, and benefit rights lead to ambiguity regarding the rights and obligations of all parties involved in data sharing. Once a data breach or misuse occurs, it becomes difficult to trace responsibility, thereby undermining the willingness of all parties to participate in data sharing.

**Technical Standards are not Unified.**

The lack of a unified data catalog and standardized specifications means that data formats and definitions may vary significantly across different departments and even within the same department, making it difficult to achieve seamless interconnection and interoperability across departments and systems. Most existing data space exploration initiatives are designed and implemented based on the approach of raw data sharing and circulation, which pose numerous challenges in terms of security risks, mutual trust foundations, and regulatory standards, making it hard for them to fully meet the unique needs of the defense industry.

## 3 Analysis of Industry Adaptability for Trusted Data Spaces

### 3.1 Concepts and Architecture

A Trusted Data Space is a digital infrastructure that connects multiple entities based on consensus rules, designed to ensure the secure, lawful, and trustworthy exchange and circulation of data [10]. Its core concept lies in combining technological solutions with institutional design to achieve efficient utilization and value realization of data assets, adhering to the principle of "data remains static while value flows." Through metadata exchange, it enables data resources to be discoverable, accessible, and controllable [11]. The overall architecture of the Trusted Data Space is depicted in Fig. 1.

The technical architecture of a Trusted Data Space is typically built around the full lifecycle of data value circulation, comprising three core components: trusted governance, resource interaction, and co-creation of value [12]. The trusted governance layer

provides trust management capabilities by leveraging mechanisms such as access authentication, data permission allocation, and evidence-based traceability, thereby establishing a solid foundation of trust for data interactions[13]. The resource interaction layer aims to establish a mechanism for data interconnectivity and interoperability. Through standardized processes—including data ingestion, data publication, data discovery, data transformation, and data delivery—it facilitates the transformation of raw data resources into standardized, high-quality data resources. The value co-creation layer focuses on promoting the realization of data value across multiple scenarios. By matching supply and demand, conducting operational oversight, and supporting application development, it ultimately empowers both data providers and users with data products and services.

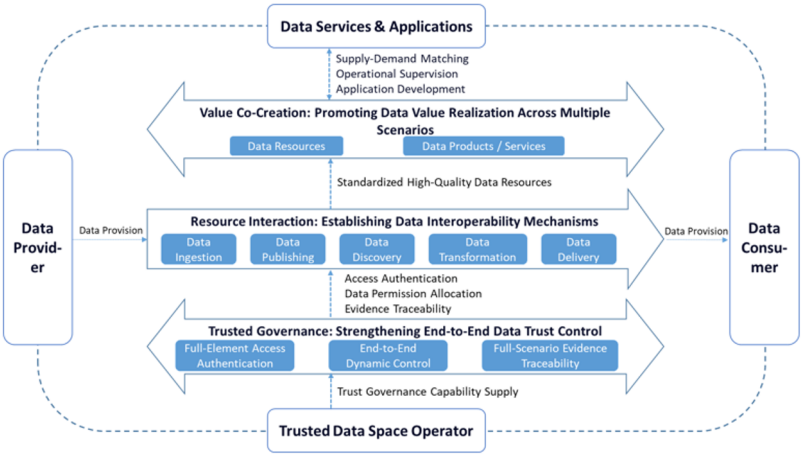


**Fig. 1.** Overall Architecture of Trusted Data Space.

### 3.2 The Key Role of Trusted Data Spaces in Data Sharing

**Establish a Foundation of Trust.**

The Trusted Data Space establishes a trust mechanism among participants through technological means, thereby reducing the trust costs associated with data sharing. The identity authentication module ensures the authenticity and reliability of the identities of participating entities, while smart contract technology automatically enforces data-sharing rules, minimizing human intervention and disputes [14].

**Ensure Data Security.**

Privacy-preserving computation technologies enable a data-sharing model where data is "available but invisible," allowing data to participate while remaining encrypted. Computing ensures that the raw data remains undisclosed. Data monitoring technology records and tracks the entire data flow process, thereby enabling controllability and auditability of data usage [15].

**Promote Co-Creation of Value.**

A trusted data space supports data collaboration and value extraction among multiple entities, generating new business insights through data fusion and analysis. In a trusted environment, both data providers and data demanders achieve mutual benefits, thereby maximizing the value of data as an economic factor[16].

### 3.3 Adaptability Analysis for the Defense Industry

The security and trustworthiness features of trusted data spaces align closely with the needs of the defense industry. Its distributed architecture can accommodate the hierarchical relationship between a group and its subsidiaries, while its edge computing capabilities enable deployment in edge scenarios. Moreover, its policy engine meets the requirements for multi-level classification management. Privacy-preserving computation technologies can unlock and share data value without exposing the original data itself, making them highly compatible with the defense industry's core requirement for data confidentiality.

However, certain features of the Trusted Data Space need to be specifically adapted for the defense industry. The unique characteristics of the defense sector dictate that it cannot fully adopt a decentralized architectural design; instead, data storage and circulation must be subject to stringent centralized oversight. The transparency inherent in blockchain technology conflicts with the defense industry's confidentiality requirements: since transaction records on the blockchain are visible to all nodes, sensitive information could potentially be leaked. Consequently, it is inappropriate to directly employ blockchain technology in military industry scenarios.

## 4 Practical Path for a Credible Data Sharing Mechanism in the Military Industry

### 4.1 Mechanism Design Principles

The design of a trustworthy data-sharing mechanism for the defense industry must adhere to the following core principles: First, the principle of security first, ensuring the security of data throughout its entire lifecycle—from collection and transmission to storage and use. Second, the principle of tiered management and control, implementing differentiated control strategies based on data classification levels and sensitivity [17]. Third, the principle of least privilege, granting data access permissions only to the minimum scope necessary for completing business tasks. Fourth, the principle of full-process traceability, ensuring that all data flows are fully traceable. The entire process is fully traceable, supporting audit trail and accountability identification.

### 4.2 Technical Architecture Design

The trusted data-sharing mechanism proposed in this paper aims to address the challenges of trust establishment and secure data sharing in cross-entity data interactions.

This architecture is divided from bottom to top into an infrastructure layer, a trusted-mechanism layer, and a data-services layer, and achieves business empowerment through top-level scenario applications. The overall logic is centered around the "Group Data Space," which connects multiple "Enterprise Data Spaces" via standardized interfaces, thereby forming a distributed collaborative network of the "1+N" model. The architecture of the trusted data sharing mechanism is depicted in Fig. 2.

**Infrastructure Layer.**

The infrastructure layer serves as the physical and logical foundation for the operation of the data space, comprising four key components: Space Management is responsible for defining the organizational boundaries of the data space, managing member permissions, and configuring basic settings; Connector Management enables the access and registration of various enterprise nodes, monitors link statuses, and performs heartbeat detection by deploying standardized connectors; the Service Discovery mechanism supports automatic registration of microservices, subscription-based queries, and dynamic routing; and the Protocol Adaption component provides multi-protocol conversion and interface standardization capabilities, bridging technological stack differences among different enterprises and ensuring seamless interoperability between systems.

**Trusted Mechanism Layer.**

The Trust Mechanism Layer is the core control layer of the architecture, designed to establish a closed-loop trust system across the entire process, ensuring the compliance, security, and traceability of data interactions. Digital contracts codify data usage rules, enabling automated creation, signing, and execution of contracts. Identity authentication rigorously verifies interacting entities, preventing unauthorized access. Usage control implements fine-grained access policies, performing real-time validation and interception of data requests based on pre-defined usage rules. The Trusted Evidence Storage is responsible for recording and auditing the full operation logs, guaranteeing the authenticity of recorded actions and providing a basis for subsequent accountability.

**Data Service Layer.**

The data service layer, oriented toward business needs, provides standardized capabilities for data asset operation and delivery. This layer includes a data catalog service that enables retrieval and presentation of standardized data resulting from governance efforts. Data product management processes raw data into standardized products to support upper-layer business applications. The data delivery service offers secure and efficient data transmission channels, supporting various modes such as API calls and batch exports. Finally, the data application service encapsulates common data processing capabilities, providing direct invocation interfaces for upper-layer business applications.

**Scenario Application Layer.**

The scenario application layer directly serves the group's business value chain, covering four major areas: design, production, analysis, and management. Based on the trusted data service capabilities provided by the underlying layer, this layer supports specific business scenarios such as collaborative design across enterprises, coordinated production in the supply chain, operational data analysis, and group-level governance, thereby fully unlocking the value of data elements.

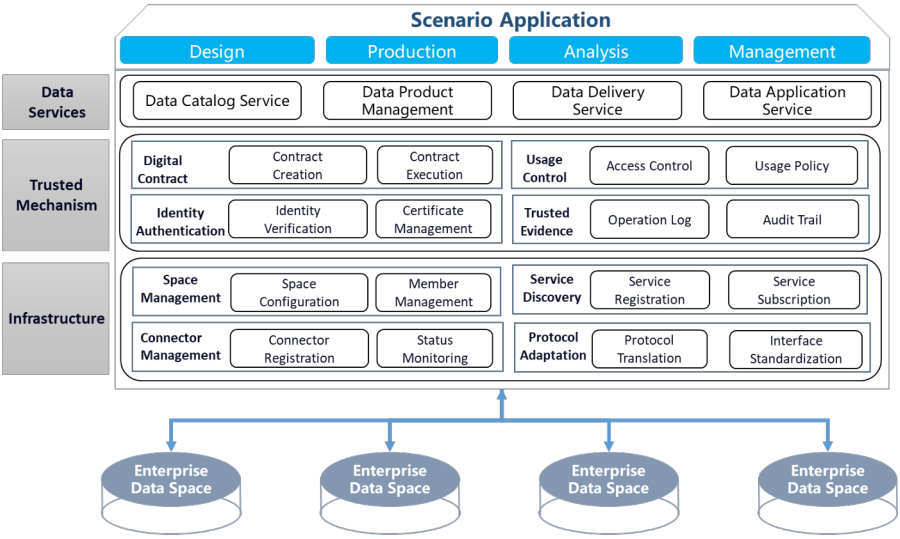


**Fig. 2.** Trusted Data Sharing Mechanism Architecture.

It is worth noting that the trusted data sharing mechanism proposed in this paper is based on the trusted data space architecture, rather than blockchain technology. Although both aim to address trust issues, our proposed scheme focuses more on endpoint security and the trustworthiness of transmission channels.

## 4.3 Comparative Analysis

**Performance Evaluation and Analysis.**

This paper conducts a performance analysis of the mechanism based on the Trusted Data Space architecture, with the results presented in Table 1. The evaluation benchmarks reference the *International Data Spaces Benchmark Report* published by the International Data Spaces Association (IDSA), as well as empirical studies on national cryptographic algorithms in embedded environments conducted domestically. The test results indicate that following security reinforcement using the SM2 and SM4 algorithms, the transmission performance of the Connector aligns with the performance trends of the IDS Connector tested by Fraunhofer ISST, maintaining a throughput of over 800 Mbps, which satisfies the requirements of high-bandwidth industrial scenarios.

**Table 1.** Quantitative Evaluation Metrics and Results

| Evaluation Dimension | Metric | Test Scenario | Results (Reference) |
|---|---|---|---|
| Transmission Performance | Throughput | Encrypted transmission of large files | 800 - 900 Mbps (in Gigabit LAN) |
| Response Latency | Authentication & Handshake Delay | Establishing secure channels and identity authentication | 15 - 30 ms (SM2 bidirectional authentication) |
| Computational Overhead | Policy Enforcement Overhead | Parsing and matching Digital Contracts (Usage Control Policies) | <2 ms per policy match |
| Resource Consumption | CPU / Memory Usage | Connector service running on edge nodes | < 500 MB (Idle Memory) |

Regarding transmission efficiency, the system employs the SM4 algorithm for streaming encryption. This approach maintains throughput close to the physical network card limit while ensuring data security, demonstrating that the mechanism is capable of handling efficient data circulation in military industry scenarios.

In terms of system latency, although bidirectional identity authentication based on digital certificates and fine-grained digital contract policy verification have been introduced, the overall additional latency remains within the millisecond range. For non-hard real-time industrial data transmission, this minimal performance overhead is entirely acceptable and yields a high degree of data sovereignty control.

Tests on resource overhead indicate that the Connector component features lightweight characteristics and low hardware resource consumption on edge nodes, demonstrating strong feasibility for engineering implementation.

In conclusion, the quantitative data confirms that the mechanism achieves a favorable balance between security and performance.

**Comparative Analysis of Mechanisms.**

To further elucidate the superiority of the proposed Trusted Data Space-based sharing mechanism, this paper compares it with traditional centralized data platforms and Federated Learning schemes, as presented in Table 2.

Compared with traditional centralized platforms, the proposed solution addresses the ambiguity regarding data sovereignty attribution caused by the "unified construction systems" in military groups. Through the use of Connectors, subordinate enterprises retain physical control over their data, thereby avoiding the risks of data abuse or leakage by a central node.

In comparison with Federated Learning, while the latter protects privacy, it fails to meet the core requirement of the military industry for raw data interaction. The proposed mechanism utilizes Usage Control technology to allow the circulation of raw data within a controlled environment, filling the business gap that Federated Learning cannot cover.

**Table 2.** Comparative Analysis of Different Data Sharing Mechanisms

| Comparison Dimension | Centralized Data Platform | Federated Learning | Proposed Mechanism |
|---|---|---|---|
| Data Sovereignty Control | Weak (Physical data concentration) | Strong (Data stays within domain,) | Very Strong (Data transmissible, but usage rights and lifecycle strictly controlled via contracts) |
| Data Circulation Form | Physical migration of raw data | no raw data transmission | Controlled flow of raw data |
| Single Point of Failure Risk | High (Center server failure causes total network paralysis) | Medium (Relies on parameter server) | Low (Distributed connector architecture, single point failure does not affect the whole network) |
| Applicable Business Scenarios | Internal management systems, non-sensitive data aggregation | Joint modeling, AI training scenarios | Scenarios requiring raw data interaction e (Cross-organizational collaborative design, supply chain production) |
| Audit and Traceability | Relies on central administrator, prone to tampering | Difficult to trace risks of model inversion attacks | Full-process log storage (Connectors record logs independently, tamper-proof, bidirectional audit) |

## 4.4 Application Scenario Analysis

The data trust-sharing mechanism for the defense industry, based on a trusted data space, can be applied to a variety of typical business scenarios. Below, we describe the specific application methods of this mechanism from three perspectives: collaboration between the group and its subsidiaries, edge-side data collection and transmission, and joint R&D across organizations.

**Group - Subsidiary Enterprise Collaboration Scenarios.**

Military-industrial groups typically adopt a multi-tiered organizational structure consisting of "headquarters—second-level units—third-level units." The headquarters needs to distribute technical documents such as design drawings and process specifications to its subordinate enterprises, while also collecting feedback information—including production schedules and quality data—from these enterprises. Under the traditional model, such data exchange often relies on manual copying and dedicated-line transmission, which suffer from low efficiency, difficulty in traceability, and high risks. The mechanism described in this paper is applied as follows:

Data publication and catalog registration: The group headquarters will classify and label the data resources that need to be shared, and register them through the data catalog service with the Trusted Data Space Management Center. The data catalog includes metadata information such as data name, security classification, format, and update cycle, but does not include the actual data content itself.

Access Request and Approval: Subsidiary enterprises retrieve the required data resources through the Trusted Data Space portal and submit data access requests. The request information includes the purpose of use, scope of use, duration of use, and other relevant details. The Group's headquarters strategy control layer conducts automatic or manual approval based on pre-defined authorization rules.

Data delivery and usage control: After approval, the system generates a data access token, which subordinate enterprises can use to obtain the data. The data is encrypted and transmitted using national cryptographic algorithms and stored within the local secure domain of the subordinate enterprises. A digital contract imposes constraints on data usage behavior, such as limiting the number of copies, prohibiting secondary distribution, and setting specific expiration date, etc.

Employ monitoring and auditing. Access logs and operation records generated during data usage are transmitted in real time to the group's headquarters audit system, establishing two-way supervision. Any abnormal behavior triggers a risk alert; the system automatically suspends access permissions and notifies the administrator.

This mechanism enables the standardization, automation, and traceability of data sharing between the group and its subsidiaries, reducing costs associated with manual intervention, enhancing data flow efficiency, and ensuring the security and controllability of data throughout its entire lifecycle.

**Edge Data Collection and Transmission Scenarios.**

The production and testing base for the defense industry is located in a remote area with relatively weak network infrastructure. Edge devices—such as sensors, testing instruments, and production equipment—need to upload real-time data they collect to a central server for analysis and processing. Such scenarios face challenges including unstable network connections, large data volumes, and high security requirements. The mechanism described in this paper is applied as follows:

Edge node deployment: Deploy trusted data space edge nodes at the edge site, equipped with features such as data caching, local processing, and encrypted transmission. The edge nodes establish a secure communication channel with the central node, supporting resumable uploads and data synchronization.

Local data preprocessing. Data collected at the edge is first subjected to preliminary processing at the edge node, including data cleansing, format standardization, and sensitive information masking. After processing, the data volume is reduced, thereby improving transmission efficiency.

Lightweight encrypted transmission: Data is encrypted using a lightweight encryption algorithm, and compression techniques are employed to reduce bandwidth usage during transmission. A two-way authentication mechanism is used throughout the transmission process to ensure the identity of both communicating parties is trustworthy. The central node and edge nodes periodically synchronize their data states to maintain data consistency.

This mechanism can adapt to complex network environments at the edge, enhancing the stability and efficiency of data transmission, reducing reliance on central nodes, and ensuring secure collection and transmission of edge data.

## 5 Conclusions

Based on the theory of Trusted Data Spaces, this paper proposes a data-trustworthy sharing mechanism tailored for the defense industry. This mechanism integrates privacy-preserving computation, data monitoring, and access control policies to enable efficient collaboration among multiple entities while ensuring data security. The research findings indicate that by employing technical measures such as hierarchical classification, digital contracts, encrypted transmission, and bidirectional auditing, the mechanism can effectively address data circulation challenges in scenarios involving group-subordinate enterprise collaborations, edge-device-to-edge-device interactions, and cross-organizational coordination. The mechanism demonstrates strong potential for wide-scale adoption in terms of data transmission efficiency, security, and collaborative effectiveness.

## Acknowledgments

Yuwei Chen and Songzi Cao are Co-first author.

This work was supported by the National Natural Science Foundation of China (No. 92467203) and Beijing Natural Science Foundation (No.L251038).

## References

1. FANG Yiping. Thoughts and prospects on military industry digital construction [J]. National Defense Science & Technology Industry, 2020(03): 40-41.
2. WANG Yujing, ZHAO Wenyu, XIE Kun, et al. A data security access control system based on zero trust architecture under data element circulation scenarios [J]. Electronic Design Engineering, 2026, 34(03): 107-112. DOI:10.14022/j.issn1674-6236.2026.03.023.
3. LI Haisheng, ZHOU Lina, LI Qin'fu, et al. Thoughts on the construction of a military data cross-domain information exchange model [J]. Journal of China Academy of Electronics Technology, 2024, 19(06): 504-510.
4. TANG Yijie, XU Wen, LI Wei. Experience and enlightenment from the construction of the European data space and its implications for China [J/OL]. Frontiers of Data and Computing, 1-12 [2026-04-02]. https://link.cnki.net/urlid/10.1649.TP.20260401.0955.004.
5. ZENG Jiahe. Dilemmas and responses in corporate data security compliance during the big data era [J]. Journal of Nanyang Institute of Technology, 2023, 15(01): 31-35. DOI:10.16827/j.cnki.41-1404/z.2023.01.006.
6. HUANG Liangchao. Research on data security in military enterprises during the AI era [J]. Tank & Armored Vehicle, 2025(24): 81-82. DOI:10.19486/j.cnki.11-1936/tj.2025.24.010.
7. XU Xiaoming. Design and implementation of a data information exchange system based on one-way isolation gate [D]. Nanjing: Nanjing University of Science and Technology, 2020. DOI:10.27241/d.cnki.gnjgu.2020.002124.
8. LIU Yanfang, ZHANG Lei, LI Hanxuan. Practice and prospects of data element circulation and security governance in the civil aviation field [J]. Big Data, 2024, 10(06): 149-160.

9. LI Shike. Research on key technologies for privacy protection and trust management in internet of vehicles applications [D]. Beijing: North China Electric Power University, 2024. DOI:10.27140/d.cnki.ghbbu.2024.000190.
10. ZHUANG Ziyin. Building a trusted data space to assist the high-quality development of the digital economy [J]. People's Tribune, 2026(01): 60-65.
11. TANG Changle. Theoretical construction and practical reflection on the multi-element collaboration of trusted data spaces [J/OL]. Library Tribune, 1-12 [2026-04-02]. https://link.cnki.net/urlid/44.1306.G2.20260209.1610.002.
12. XIA Lei, LYU Dongyang, ZHOU Ziwen, et al. Research on the business model of trusted data spaces under the background of data element marketization [J]. Cybersecurity and Data Governance, 2026, 45(01): 48-55. DOI:10.19358/j.issn.2097-1788.2026.01.008.
13. DUAN Keran, ZHANG Ziyi, ZHANG Xi, et al. The integration path of technology and institutions for trusted data spaces oriented towards data value release [J/OL]. Journal of Harbin Institute of Technology, 1-14 [2026-04-02]. https://link.cnki.net/urlid/23.1235.T.20260313.1045.008.
14. LIU Yongjian, GUO Xueyin. Analysis of the core path mechanism and application scenarios for the construction of a trusted data space in the publishing industry [J]. Wide Angle, 2026(01): 12-19+38. DOI:10.16491/j.cnki.cn45-1216/g2.2026.01.002.
15. LIANG Man. Research on the privacy computing application and security supervision system of the Shanghai urban trusted data space [J]. China Information Security, 2025(05): 29-33.
16. YIN Ximing, WANG Shuaimin, WANG Yipei, et al. Scenario-driven construction and integrated application of trusted data spaces: Theoretical mechanisms and practical approaches [J]. Think Tank, 2025(01): 9-18. DOI:10.19881/j.cnki.1006-3676.2025.01.02.
17. DONG Guishan, BAI Jian, WANG Xunqiao. Research on a data security system based on cryptography [J]. Information Security and Communications Privacy, 2025(04): 62-74.