Journal of Computers Vol. 37 No. 5, October 2026, pp. 269-285
https://doi.org/10.63367/19911599202610370501 7

Construction of Secure Data Sharing Strategies and Incentive Mechanisms for Industrial Internet of Things Based on Digital Twin

Xiao-Jing Guo[1,2], Cheng-Fang Mei[1], Meng-Ying Yang[1], and Yuan Yuan[1*]

[1] Hebei Mechanical and Electrical Polytechnic,
Xingtai City 054000, Hebei Province, China
{guoxiaojing, meichengfang, yangmengying, yuanyuanxinxi}@hbjd.edu.cn

[2] Data Element and Intelligent Agent Technology Innovation Center,
Hebei Mechanical and Electrical Polytechnic, Xingtai City 054000, Hebei Province, China

Received 10 July 2026; Revised 5 August 2026; Accepted 10 September 2026

Abstract. This paper presents a secure data sharing strategy and incentive mechanism for the Industrial Internet of Things (IIoT) based on digital twin technology. As IIoT systems rely on real-time data exchange among heterogeneous and distributed devices, concerns about data privacy, ownership, and cybersecurity are increasingly critical. Digital twin offer a dynamic virtual representation of physical assets, enabling secure and efficient data tracking and validation. To address the reluctance of stakeholders in sharing data, a game-theoretic incentive model is proposed to promote active and trustworthy participation. The proposed framework ensures data integrity, confidentiality, and traceability while optimizing collaboration across the IIoT network. Experimental results and simulations validate the feasibility and effectiveness of the approach in enhancing secure data sharing and motivating stakeholders. This study contributes to bridging the gap between IIoT data security and economic motivation, laying a foundation for future intelligent and secure industrial ecosystems.

Keywords: Industrial Internet of Things (IIoT), digital twin, secure data sharing, incentive mechanism

1 Introduction

The rapid development of the Industrial Internet of Things (IIoT) has transformed modern manufacturing by enabling seamless connectivity among smart devices, machines, and systems to establish real-time data creation, examination, and sharing [1].

With the rapid advancement of a new round of global technological revolution and industrial transformation, technologies such as information and communication, biology, new materials, and new energy are constantly breaking through and accelerating their integration with advanced manufacturing technologies, providing historical opportunities for the high-end, intelligent, and green development of the manufacturing industry. At present, China's intelligent manufacturing industry still faces serious challenges in industrial transformation and development. In recent years, new generation information technologies represented by Industrial Internet of Things (IIoT), edge intelligence, blockchain, digital twins, and 6th Generation Mobile Networks (6G) have gradually attracted widespread attention from the industrial and academic communities, leading to a gradual increase in the digitalization of industrial production processes. However, due to the differences in the functions of Smart Factories (SF) in the real world, the production of products requires the collaboration of smart factories with different functions. The competitive relationship between different smart factories has led to the phenomenon of "information silos", which limits the execution of production tasks. The data sharing technology of IIoT can to some extent eliminate the phenomenon of "information silos" and achieve the flow of data between smart factories. IIoT collects data through a large number of sensors, and then connects to the Internet through equipment and systems, making industrial production processes more digital and intelligent, so as to provide enterprises with safer, more efficient and more reliable production and operation management solutions. However, at the same time, enterprises are also facing issues such as how to efficiently manage the growing number of devices, how to analyze and process massive sensor data, and how to ensure the high availability and security of production systems.

* Corresponding Author

The traditional data sharing method stores and uses shared data uniformly by building a data sharing model for a common data platform. However, with the continuous development of IIoT, a large number of IoT devices are connected to IIoT, generating massive amounts of industrial data. Uploading massive industrial data to a centralized data platform not only poses data security risks but also affects the performance of the data platform. Although advanced cryptographic techniques can ensure the security of shared data in data platforms, traditional centralized data platforms still face risks such as single point attacks. By leveraging edge intelligence to sink the resources of centralized data platforms to the edge of the network, not only does it avoid the risk of single point attacks, but it also improves the access and storage performance of shared data. However, due to the openness of the network, edge devices in the network face significant privacy protection challenges. Building a blockchain ecosystem on edge networks can effectively ensure the privacy of shared data among edge devices, but the performance of blockchain still needs further improvement. Although, with the help of new generation cryptography, blockchain, edge computing and other technologies, the security of shared data and the efficiency of data sharing can be improved to a certain extent. However, existing industrial IoT data sharing methods still cannot perfectly meet the requirements of high security, high quality, and high efficiency for shared data in intelligent manufacturing tasks.

In this context, Digital Twin (DT) technology has been widely applied in IIoT due to its unique advantages. Digital Twin is an emerging virtual real space interaction technology, whose core is to map physical entities into digital images of virtual space in real time. Through intelligent decision-making, reverse feedback, and control, it achieves real-time monitoring and precise management of physical systems throughout their lifecycle, providing an innovative solution to the above problems. In IIoT systems, the accuracy of digital twins is crucial as it directly affects the overall performance of the system and the precision of decision-making.

This interconnected architecture assures higher operational transparency, predictive maintenance, and intelligent decision-making. The distributed and heterogeneous character of IIoT networks, however, creates serious data security, privacy, and trust issues.

Digital twin technology, which creates virtual copies of physical assets and synchronizes with them in real time, has emerged as a game-changing enabler for smart industrial uses [2]. Digital twin not only support process optimization and adaptive control but also offer potential to improve data governance through real-time monitoring, authentication, and tracing. Despite such advantages, secure integration of digital twin into IIoT data-sharing architectures is still constrained. Besides that, data contributors are reluctant to share precious data due to threats of misappropriation, loss of intellectual property, and poor compensation. These two challenges of safe data exchange assurance and participation demand an end-to-end solution. Towards this objective, this paper presents a digital twin–enabled secure data sharing strategy and a game-theoretic incentive mechanism specially tailored for IIoT environments. The new framework utilizes digital twin to build a security layer with real-time anomaly detection, data provenance, and access control, and a dynamic game theory-based incentive model tracks contributions and rewards fairly to incentivize active participation. The main contributions of this work are: (1) an end-to-end digital twin–based security system for trustworthy data exchange; (2) an incentive mechanism that incentivizes truthful sharing and punishes malicious attack through strategic reward distribution; and (3) simulation-based verification demonstrating improved data sharing rate, security robustness, and participant fairness. This research contributes to the field by combining digital twin intelligence with secure, incentive-based IIoT data governance to deliver the basis for industrial data ecosystems that are secure, cooperative, and economically sustainable.

2 Related Work

The construction of secure data sharing strategies and incentive mechanisms for the IIoT based on digital twin technology has garnered significant research interest, emphasizing the integration of blockchain, game theory, and innovative incentive models. A prominent approach involves leveraging blockchain technology to facilitate fine-grained and secure digital twin sharing frameworks. For instance, Lee et al. [3] introduces a blockchain-based digital twin sharing architecture tailored for smart construction, emphasizing detailed security and access control mechanisms. Similarly, Kumar et al. [4] reviews the application of blockchain in digital twin-enabled IIoT environments, highlighting its role in ensuring secure and trustworthy data exchanges among digital twin in smart manufacturing. Security concerns in digital twin data sharing are further addressed through cryptographic protocols. Shamsoshoara et al. [5] proposes a blockchain and physically unclonable function (PUF)-based secure key establishment protocol, which enhances cross-domain IoT device authentication, thereby strengthening data

security in digital twin architectures. Incentive mechanisms are crucial for motivating data sharing among IoT devices and digital twin. Maddikunta et al. [6] provides a comprehensive survey of incentive techniques, noting that artificial intelligence can be employed to develop data-driven incentive models that encourage participation. Building on this, Wen et al. [7] introduces a diffusion-based incentive mechanism utilizing contract theory to motivate IIoT devices to share sensing data for digital twin construction, addressing the challenge of incentivizing data contribution in large-scale IoT networks. Game-theoretic approaches also play a vital role in designing effective incentive strategies. Zhu [8] presents an evolutionary game model based on blockchain smart contracts to promote digital twin data sharing, aiming to establish stable and mutually beneficial sharing behaviors among participants. This approach underscores the importance of strategic incentives in fostering sustainable data exchange. Furthermore, the integration of digital twin into urban and industrial contexts demonstrates practical implementations of secure and incentivized data sharing. For example, Lv et al. [9] discusses a digital twin city framework that facilitates secure data sharing among digital twin in smart city construction, highlighting the role of blockchain in ensuring data security and trustworthiness. Additionally, Prathiba et al. [10] explores a federated learning framework assisted by blockchain to enhance trust and security in digital twin data sharing, addressing challenges related to data privacy and integrity. Policy and strategic guidance also influence the development of secure data sharing mechanisms. The Zheng et al. [11] report emphasizes the importance of establishing robust data sharing and exchange mechanisms within the broader context of industrial Internet development, advocating for policies that support secure and incentivized data collaboration. In summary, current research underscores a multifaceted approach to constructing secure data sharing strategies and incentive mechanisms for digital twin-enabled IIoT. Blockchain technology emerges as a central tool for ensuring security and trust, while game theory and AI-driven incentives are pivotal in motivating data contribution. These strategies collectively aim to foster a secure, trustworthy, and efficient digital twin ecosystem within the industrial Internet landscape.

3 System Model

A smart industrial environment with an IIoT framework consists of a heterogeneous network of physical devices and their corresponding mapping DT entities. Each physical device has a digital twin that mirrors real-time operational status, contextual metadata, and historical logs. They are connected to a centralized cloud data platform that enables the exchange of data between stakeholders such as equipment suppliers, system integrators, maintenance service providers, and third-party analytics services [12].

In this architecture, data providers continuously generate real-time operational data that may be business-critical and sensitive. These streams of data are communicated to the centralized data platform through their digital twin, and data consumers can access this data for decision-making, process optimization, and predictive maintenance. The digital twin acts not only as a relay of information, but also as a security agent responsible for data integrity verification, data provenance tracing, and access control policy enforcement [13].

However, this data-sharing model brings up some concerns on security and trust. On the one hand, the openness and distributive nature of IIoT networks make it vulnerable to threats such as unauthorized data access, eavesdropping, data tampering, and leakage of intellectual property. On the other hand, there is a lack of a general trust mechanism that would discourage participants from providing quality data, especially when data providers believe the data will be used in an inappropriate way or are not able to obtain appropriate rewards.

To address these issues, develop a secure and incentive-compatible data sharing solution that satisfies three basic security principles: confidentiality (ensuring that the data can be read only by the authorized consumers), integrity (ensuring that the data has not been tampered with or modified during communication), and availability (ensuring that the data is accessible when needed without unnecessary delays or loss). In addition, the system ought to have a way of offering an incentive to data providers to report honestly and receive a fair and proportionate reward for their contributions.

The IIoT environment is modeled as a multi-agent system, where each agent represents either a data provider or a data consumer. Each provider $i \in \mathrm{P}$ contributes data d_i to the platform, while each consumer $j \in C$ accesses a subset of this data, The representation method is as follows:

$$D_j \subseteq \{d_1, d_2, ..., d_n\} \tag{1}$$

The data is under predefined access policies. The platform includes a security module S that monitors data

flow and ensures compliance with authentication, encryption, and access control protocols. Each agent's behavior and utility are influenced by both security configuration parameters and incentive parameters. The overall objective is to jointly optimize these parameters to:

1) Maximize system-wide data utility and stakeholder participation;

2) Minimize security risks and data compromise incidents;

3) Ensure sustainable and fair compensation to data providers.

Let the utility function of a data provider be denoted as:

$$U_i = R_i - C_i \tag{2}$$

In the equation, where R_i is the reward received for data contribution and C_i is the cost incurred due to privacy loss, computational overhead, and energy consumption. For a consumer j, utility U_i depends on the quality, availability, and trustworthiness of the accessed data. The following optimization problem:

$$\max_{\theta,\gamma} \sum_{i \in p} U_i(\theta_i, \gamma_i) + \sum_{j \in c} U_i(\theta_j) \tag{3}$$

Here, θ is the security strategy vector and γ the incentive strategy vector. The architecture must ensure Nash equilibrium conditions in the incentive model, so that no agent benefits from unilaterally deviating, thereby ensuring stable cooperation. In summary, the challenge of secure data sharing and incentivization in IIoT is posed in this section as a constrained multi-agent optimization problem that requires security as well as economic incentives to be coordinated dynamically. This formulation sets the base for scalable algorithm design for security enforcement and fair reward distribution in digital twin-augmented IIoT systems.

The digital twin continuously transmits data to the data platform and adds keys at critical nodes to ensure data security. When the corresponding intelligent manufacturing equipment of the digital twin applies to access the data platform, the digital key is triggered to generate a key for the entire system [14]. The process is as follows:

1) Select a set of prime numbers and choose the largest prime number $p_{\max}$ from the set, making it difficult to solve discrete logarithm problems. At the same time, generate random numbers based on block timestamps and randomly select integer x_{random} as the key $k_{private}$ for intelligent manufacturing equipment. The range of key values is represented as follows:

$$1 < k_i < p_{\max} - 1 \tag{4}$$

If element e is selected for generation, the public digits of the corresponding digital twin of the terminal device should be represented as follows:

$$k_{public} = e^{k_{private}} \bmod p_{\max} \tag{5}$$

The system sends the generated private key to the corresponding intelligent manufacturing device and stores the public key of the intelligent manufacturing device in the system [15].

2) Intelligent manufacturing devices use private keys to sign the identity information they generate. If the identity information is represented as I_{id}, the hash value of the device's digital twin's identity is as follows:

$$\begin{cases} i_{id} = H\left(I_{id}\right) \\ s.t. 0 \le i_{id} \le p_{\max} - 1 \end{cases} \tag{6}$$

Intelligent manufacturing devices select random numbers and then calculate their information signatures.

3) Verify the identity information signature of intelligent manufacturing devices [16], and the verification information is represented as:

$$I_{ver} = k_{public} \cdot m_{id} \tag{7}$$

In the formula, m_{id} represents the signature information. Assuming successful verification, the system generates unique signature information for the smart device, stores the information of the smart manufacturing device in the system, returns the error message to the smart manufacturing device, and adds it to the blacklist. The pseudocode representation of the entire process is as follows:

```
// Algorithm 2-1: Trusted Authentication Algorithm for Smart Manufacturing Equipment
// ---------- Key Generation Phase ----------
// 1. Select a set of primes and choose the largest prime p
Select prime set P_set
Let p = max(P_set)
// 2. Randomly choose integer x as IME's private key Prk, and choose a generator g
Randomly choose Prk such that 1 < Prk < p-1
Choose a generator g of the multiplicative group modulo p
// 3. Compute partial public key Puk_y using Puk_y ≡ g^{Prk} mod p
Puk_y = g^{Prk} mod p
// 4. Assemble the full public key Puk = {Puk_y, g, p}
Puk = (Puk_y, g, p)
// 5. Send the private key to the corresponding IME
Send Prk to IME securely
// 6. Store the public key into the blockchain
Store Puk into the blockchain
// ---------- Identity Signing Phase (performed by IME) ----------
// 7. IME's identity information M_id
Let M_id be the identity information of IME
// 8. Compute hash of identity: m_id = H(M_id)
m_id = Hash(M_id)
// 9. IME randomly selects a random number r_sig
Randomly choose r_sig such that 1 < r_sig < p-1 and gcd(r_sig, p-1) = 1
// 10. Compute partial signature S_x ≡ g^{r_sig} mod p
S_x = g^{r_sig} mod p
// 11. Compute signature component S_y ≡ r_sig^{-1} * (m_id - Prk * S_x) mod (p-1)
//      (Note: original text says mod p^{-1}, interpreted as mod (p-1) for modular
inverse)
S_y = (r_sig^{-1} * (m_id - Prk * S_x)) mod (p-1)
// 12. Assemble the signature S = (S_x, S_y)
S = (S_x, S_y)
// 13. IME sends (M_id, S) to the EMSC (Edge/Middle Security Controller) for
verification
// ---------- Identity Verification Phase (performed by EMSC) ----------
// 14. EMSC computes hash of received identity: m'_id = H(M_id)
m'_id = Hash(M_id)
// 15. Compute partial verification V_x ≡ Puk_y^{S_x} * S_x^{S_y} mod p
V_x = (Puk_y^{S_x} * S_x^{S_y}) mod p
// 16. Compute partial verification V_y = g^{m'_id} mod p
V_y = g^{m'_id} mod p
// 17. Verify the signature
if V_x == V_y then
    // Signature verification successful
    // 18. Generate an alias (pseudonym) for the IME and store it in the blockchain
    M_alias = Hash256(M_id)
    Store M_alias into the blockchain
    Return "Verification success"
else
    // Signature verification failed
    // 19. Return error message to IME and add it to the blacklist
    Send error message to IME
      Add IME to the blacklist
      Return "Verification failed"
  end if
```

4 Proposed Secure Data

To meet the dual security and performance requirements of IIoT systems, this paper proposes a secure data sharing solution that combines digital twin technology with multi-layer security mechanisms. The main goal of this framework is to ensure data confidentiality, integrity, and authenticity throughout the data lifecycle without sacrificing the low latency expectations of real-time industrial systems.

The core of this solution is the digital twin, which is a real-time dynamic virtual counterpart that mirrors the state, behavior, and lifecycle of each physical device. In addition to traditional system simulation and predictive diagnostic applications, the digital twin is enhanced here as a security-aware agent [17]. Each digital twin continuously monitors the health of its corresponding physical asset and maintains a synchronized telemetry data stream. This feature enables early detection of abnormal behavior, such as sensor spoofing, data tampering, or illegal command injection. The digital twin performs data preprocessing and authentication before transmitting the data to the centralized platform. Suspicious data patterns identified through rule-based filters or anomaly detection algorithms are flagged or discarded, reducing the spread of malicious data and improving the overall robustness of the system.

To preserve data confidentiality without compromising system responsiveness, lightweight encryption schemes are applied at the edge. The encryption latency is modeled as a function of key length and data size:

$$T_{enc} = \alpha \cdot log_2(k) + \beta \cdot S \tag{8}$$

Where T_{enc} is the encryption time, k is the encryption key length, S is the data size in bytes, and α and β are system-based constants. The model dynamically adjusts the encryption level based on available resources and latency thresholds. In addition, attribute-based access control (ABAC) is implemented to enable context-aware permissions based on user roles, device status, and action priority.

Mutual authentication is enforced before any data transfer between providers and consumers. The system uses token-based identity verification, with the probability of successful authentication defined as:

$$P_{auth} = 1 - (1 - \frac{n_{valid}}{n_{total}})^m \tag{9}$$

Where n_{valid} is the number of verified identities, n_{total} is the total number of authentication attempts, and m is the number of retries. The model is based on probabilities that account for dynamic identity management and also for a balance between authentication strength and processing cost. All authenticated identities are stored in a blockchain ledger for auditability and immutability.

Here, θ represents the security policy parameters, $D(\theta)$ is the delay induced by the selected policy, $S(\theta)$ is the corresponding security score.

$$\min_{\theta} \lambda_1 \cdot D(\theta) + \lambda_2 \cdot (1 - S(\theta)) \tag{10}$$

5 Design and Exam Setup

In a decentralized IIoT environment, data is provided by heterogeneous parties with different incentive mechanisms and trustworthiness, so it is a challenging task to encourage homogeneous, high-quality data exchange. To address this problem, an incentive mechanism based on game theory in Table 1, which dynamically investigates the contributions of data providers and gives corresponding compensation. The mechanism aims to promote fairness, prevent malicious behavior, and achieve long-term participation, thereby improving the overall robustness and utility of the data sharing system.

Table 1. Summary of incentive mechanism components in IIoT secure data sharing

Component	Function	Purpose
Contribution-based utility modeling	Quantifies individual utility as reward minus cost; rewards depend on data quality and frequency.	Encourages high-quality and frequent data contributions.
Reputation-driven feedback loop	Maintains evolving trust scores; influences reward scaling and access rights.	Reinforces long-term engagement and platform trust.
Free-Rider and Attack Resilience	Detects and penalizes low-quality or dishonest behavior; enforces participation thresholds.	Maintains fairness and deters malicious or free-riding behavior.
Incentive distribution algorithm	Periodically aggregates metrics, updates reputations, calculates rewards, and executes payouts.	Ensures transparent and fair reward distribution aligned with contributions.

5.1 Contribution-based Utility Model

In this model, every data provider is treated as a rational agent whose objective is to maximize their utility through participation. Their utility consists of rewards for sharing data minus costs for data preparation, encryption, energy, and privacy exposure among others. The incentives for each participant depend on two primary factors; data quality (DQ) and frequency of sharing (SF). These can be brought together in a weighted way to introduce the relative importance to the data providers. The utility for a participant i is expressed as follows:

$$U_i = w_1 \cdot DQ_i + w_2 \cdot SF_i - C_i \tag{11}$$

Where U_i is the utility of provider i. w_1 and w_2 are the weights for data quality and sharing frequency, respectively, which determine their relative importance. Q_i and SF represent the data quality and sharing frequency of provider i. C_i represents the cost incurred by provider i, including data preparation, encryption, energy consumption, and privacy exposure. To ensure data quality, the system employs a digital twin-based verification process, which includes: Consistency checks and Anomaly filtering. This incentivizes data providers to contribute only accurate and beneficial data, which enhances the reliability of the system.

5.2 Reputation-driven Feedback Loop

Each data provider has a dynamic reputation score that is adjusted over time to encourage long-term trust and responsible behavior. The reputation score is based on the data provider's past behavior and the reliability of their data, such as data accuracy, response rate, and compliance with system policies through a factor for as long as have been keeping track. The reputation score for each data provider is recalibrated periodically; this is accomplished by measuring historical behavior against the latest contributions. The most recent reputation score $R_i(t)$ for provider i at t is calculated as:

$$R_i(t) = \alpha \cdot R_i(t-1) + \beta \cdot A_i(t) \tag{12}$$

Where α is the decay factor ($0 < \alpha < 1$), which limits the weight of past data. $R_i(t-1)$ is the reputation score at the last period. $A_i(t)$ denotes the accuracy score of the provider's recent contributions at time t, including aspects such as consistency to platform standards and accuracy of data. Quality and consistent contributors will have higher reputation scores, which allow them to have better privileges on the platform, including higher reward rates and in some cases exclusive data.

5.3 Free-riding and Attack Resilience

One of the key risks of an open data-sharing system is the free riders who take resources without offering constructive data in return. To reduce this risk an open data sharing system requires the providers to

maintain reputation score above the minimum reputation threshold R to continue accumulating rewards. Data providers that provide bad contributions are penalized. In addition, misconduct, such as providing false data in order to manipulate the reward calculation process, is detected using some sort of anomaly detection system. The anomaly detection system provides an output of malicious score $M_i(t)$ to determine the level of suspiciousness of a data providers contributions:

$$M_i(t) = Anomaly\,Detection(D_i(t)) \tag{13}$$

Where $M_i(t)$ is the malicious score for provider i at time t. $D_i(t)$ represents the data provided by provider i at time t. If the malicious score exceeds a threshold M, the provider's reputation score is reduced, and their account is temporarily suspended. This system operates as a repeated game with clear consequences for bad behavior, encouraging rational participants to cooperate honestly over the long term.

5.4 Incentive Allocation Algorithm

The system uses an incentive allocation algorithm to periodically calculate and distribute rewards to voluntary data contributors. The process consists of several steps. First, contribution metrics such as data quality and frequency are collected over a certain period of time. Second, reputation scores are updated based on recent activity. Third, rewards are calculated by multiplying each agent's updated reputation score by its latest contribution metric. Participants whose activities fall below the specified trust level will be penalized or excluded from the reward mechanism for a period of time. Finally, the system pays rewards - either in the form of tokens through smart contracts or in platform-native credits in a timely and transparent manner. This mechanism synchronizes individual incentives with team goals and promotes the construction of a sustainable and reliable data sharing ecosystem across the entire Industrial IoT network.

To validate the effectiveness of the proposed secure data sharing and incentive mechanism in an IIoT environment, designed and conducted a series of simulation experiments based on a high-fidelity digital twin simulation platform. The testbed is implemented in MATLAB and contains real industrial process parameters as well as virtualized networked devices, controllers, and communication layers. The digital twin paradigm enables the synchronous interaction between physical layer simulation and information layer processes.

5.5 Simulation Environment

In this study, a high-fidelity digital twin simulation platform was developed using MATLAB to verify the effectiveness of the proposed secure data sharing and incentive mechanism in an IIoT environment. The simulation platform integrates real industrial process parameters with virtualized network devices, controllers, and communication layers to achieve synchronous interaction between the physical layer and the information layer. Each physical device, such as a temperature sensor, vibration monitor, and programmable logic controller (PLC), is mapped to a corresponding digital twin that continuously records and synchronizes its telemetry data, including operating status, control logs, and time series data, formalized as:

$$D_i(t) = \{s_i(t), l_i(t), \tau_i(t)\} \tag{14}$$

Where $s_i(t)$ represents the device state, $l_i(t)$ represents the operation log, and $\tau_i(t)$ represents the data stream with timestamps. The communication is simulated using a publish-subscribe message bus that embodies an industrial messaging protocol and contains adjustable network latency, packet loss rate, and encryption complexity parameters. The sensor dataset is derived from public industrial benchmarks and contains synthetic variants for testing the system's robustness to data noise and malicious interference. In addition, controlled adversarial scenarios are injected, including data tampering and unauthorized access attempts, to evaluate the system's anomaly detection, intrusion response, and access control mechanisms under different network and load conditions. This setup allows for comprehensive and repeatable simulation of real-world Industrial IoT dynamics while balancing physical realism and cybersecurity fidelity.

5.6 Evaluation Metrics

In order to comprehensively evaluate the performance of the proposed secure data sharing and incentive mechanism in an IIoT simulation environment, we define five key performance indicators (KPIs), each targeting a specific aspect of system behavior and efficiency. First, data throughput measures the amount of valid secure data successfully transmitted per unit time, which is a direct indicator of communication efficiency and is calculated as follows:

$$T = \frac{B_{valid}}{\Delta t} \tag{15}$$

Where B_{valid} is the total volume of accepted secure data, and Δt is the observation window. Second, latency quantifies the total time taken from data generation at the device to its final consumption by a trusted user, including all intermediate processes such as encryption, transmission, and digital twin synchronization; it is measured as:

$$L = t_{recv} - t_{gen} \tag{16}$$

Where t_{recv} is the reception timestamp and t_{gen} is the generation timestamp. Third, confidentiality violation rate evaluates the system's vulnerability to unauthorized access and is calculated as:

$$C_v = \frac{N_{breaches}}{N_{attacks}} \tag{17}$$

Where $N_{breaches}$ denotes the number of successful breaches and $N_{attacks}$ is the total number of simulated attack attempts; this KPI is critical for assessing the robustness of access control and anomaly detection layers. Fourth, the fairness of incentive distribution assesses the economic equity of the reward mechanism among participating agents using Jain's Fairness Index, defined as:

$$F = \frac{(\sum_{i=1}^{n} r_i)^2}{n \otimes \sum_{i=1}^{n} r_i^2} \tag{18}$$

Where r_i is the reward for agent i, and n is the total number of agents, this reflects the system's ability to provide balanced incentives in proportion to contribution. Lastly, computational overhead evaluates the feasibility of deploying the system in resource-constrained IIoT environments by measuring average processing cost per node, calculated as:

$$O_c = \frac{1}{n} \sum_{i=1}^{n} \left(\frac{U_i^{\mathrm{CPU}} + T_i^{\mathrm{proc}}}{2} \right) \tag{19}$$

Where U_i^{CPU} represents CPU usage and T_i^{proc} denotes processing time for node i. Together, these metrics provide a multidimensional view of system efficiency, security integrity, incentive effectiveness, and practical deployment viability.

5.7 Baseline Comparison

To assess how effective and adding value the proposed secure data sharing and incentive mechanism is in IIoT systems, we compared three models that ran under the same simulation conditions. The first model - the no-

security model, excludes all the security measures of the proposed secure data sharing and incentive mechanism. Therefore, this model simulates best-effort data communication; in other words, information can be shared over a communication medium without protection. Therefore, the amount of payload as bits that can travel over a communication channel is maximized, and delays between when the agent accesses the data at source to when they access the data at destination are minimized. In this mode there is no indication of how unauthorized parties access data nor how it may be compromised. The no-security model provides a baseline from which we can determined the amount of computational and time overhead incurred by using the security protocols included in the secure data sharing and incentive mechanism. The second model, the unincentivized secure model - provides the same full security measures of the secure data sharing and incentive mechanism that allow the data to achieve high confidentiality and integrity, but contains no incentive or reward structure to motivate agents to share data. Therefore, the unincentivized secure model is vegetative or passive, and agents are able to share data and have no economic motivation to do so. Therefore, the unincentivized secure model is critical to passively isolating socio-technical behavioral patterns and perform quantitative analysis of the fairness outcomes that can be realized from the presence and absence of rewards. The third and full model, the full model - describes the collaborative environment we propose that aims to combine advanced security controls and the decentralized incentive structure that incentivizes the sharing of data. By systematically comparing the three models on multiple performance metrics such as data throughput, latency, confidentiality violations, fairness of incentive distribution, and computational cost, the results show that the full model achieves a reasonable trade-off: it provides strong security guarantees and fair reward distribution while keeping a very reasonable processing cost. This demonstrates the importance of integrating incentive design with security architecture in order to integrate security in a meaningful way and promote cooperation in the IIoT environment.

6 Results and Discussion

Fig. 1 shows the data throughput performance of the baseline and proposed secure data sharing environments over a 10-minute test period. Throughput is measured in Mbps (megabits per second) and plotted as a function of time to demonstrate the temporal fluctuations and sustained throughput capabilities of the two environments.

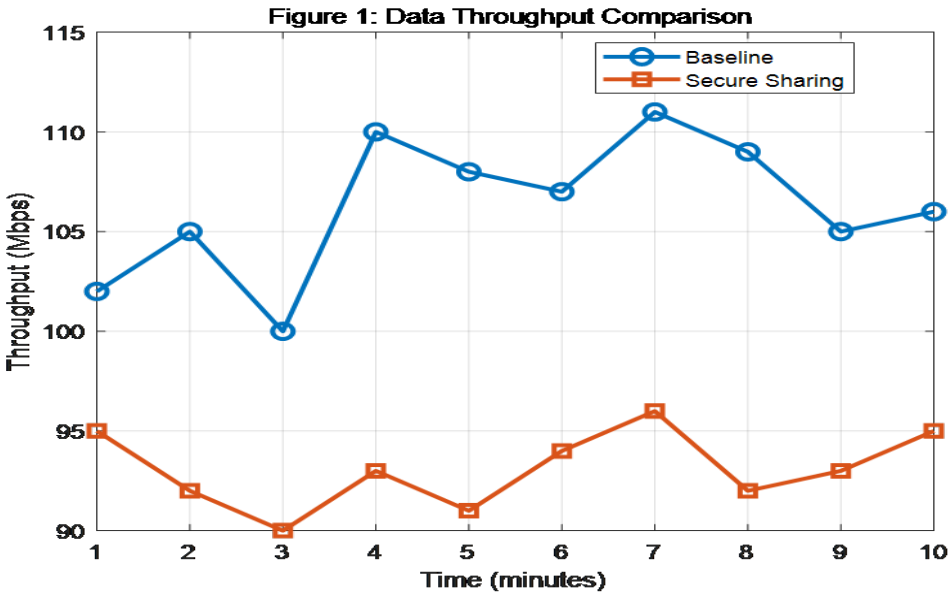


Fig. 1. Data throughput under secure sharing strategies vs baseline

In the baseline case (represented by the blue line and circular markers), throughput remains above 100 Mbps with several peaks at 110-112 Mbps. This is to be expected for a system with no encryption, authentication, or

verification layers, so the overhead is minimal and near-optimal channel capacity utilization is achieved. The baseline throughput fluctuations are minimal, indicating normal variations in network and data processing loads.

In contrast, the secure sharing strategy (represented by the orange square markers) has much lower throughput, typically staying between 90 and 95 Mbps throughout the test. This reduction is due to the additional computational operations and control delays introduced by security features such as encryption, authentication, anomaly detection, and access control, which reduce data transfer efficiency by about 10% to 15%. Despite the overhead, the shared throughput remains predictable and reliable, which is critical in industrial applications where data reliability and integrity are more important than absolute speed.

Fig. 1 highlights one of the trade-offs inherent in secure IIoT systems: ensuring the robustness of security protocols always reduces performance, namely throughput. This reduction is not excessive, but reflects the cost of ensuring confidentiality, integrity, and availability [18]. Notably, the secure system still keeps throughput within acceptable operating limits, proving that it can be used in applications that require secure and verifiable data exchange.

Fig. 2 is a comparative analysis of confidentiality leakage rates between the baseline scenario and the secure data sharing mechanism in an IIoT system. The leakage rate is expressed as a percentage that measures the number of successful attacks that intrude sensitive data without authorization during the simulation time [19]. In the baseline scenario, the leakage rate is close to 20% because the data transmission is not encrypted or authenticated. Such a high percentage reflects the vulnerability of insecure IIoT platforms, where attackers can exploit the lack of cryptographic defenses and access control to gain access to the system. These systems are susceptible to eavesdropping, replay attacks, and unauthorized data interception, especially in heterogeneous distributed industrial networks. On the other hand, the security setup consisting of lightweight cryptographic mechanisms, authentication mechanisms, and digital twin-driven anomaly detection shows an impressively low leakage rate of less than 5%. This significant drop reflects the practical effectiveness of the proposed security framework. The cryptographic technique ensures that the payload data remains ineffective to intruders even if the communication channel is compromised. In addition, the digital twin, as a security agent, helps to identify and reject suspicious or abnormal requests as early as possible without exposing the data. The evidence in Fig. 2 supports a key conclusion: while security solutions incur computational and throughput overhead, they are effective in preventing confidentiality leaks, which is particularly important in industries that handle proprietary, real-time, or safety-critical information. The over 75% reduction in leak rates demonstrates the effectiveness of the security framework in real-world IIoT deployment scenarios.

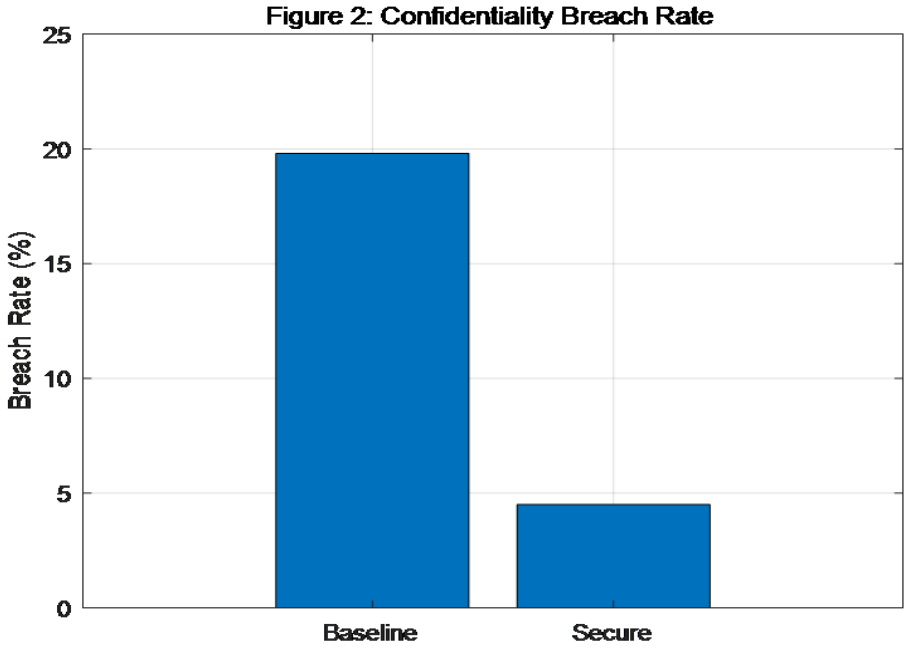


Fig. 2. Measured confidentiality breach rates demonstrating encryption effectiveness

Fig. 3 shows a box plot comparison of system latency for the baseline and secure configurations. Latency is measured in milliseconds (μs) and represents the time from data generation to successful reception by an authorized recipient [20]. This metric is critical in IIoT applications because time affects control accuracy, decision making, and responsiveness. In the baseline setting, latency is consistently low, with most values clustered around 20 μs, ranging from approximately 18 μs to 23 μs. This low latency reflects the absence of computationally intensive processes such as encryption, authentication, anomaly detection, or incentive calculation. It represents a best-effort communication environment that prioritizes speed over security or accountability. In contrast, latency for the secure configuration increases significantly, with values clustered around 35 μs, ranging from approximately 33 μs to 38 μs. This increase is attributed to the multiple layers of processing involved in the secure system, including data validation through digital twin, access control enforcement, token-based authentication, and incentive evaluation routines. These operations, while designed to be lightweight, add cumulative latency, which is unavoidable in a security-focused framework. The relatively narrow distribution of latency values for both configurations indicates stable system behavior under varying loads. However, the variation in median latency clearly highlights the performance tradeoffs associated with safety and incentives. While this additional latency is tolerable in many industrial applications, especially those without hard real-time constraints, it is a factor that must be considered in deployment decisions.

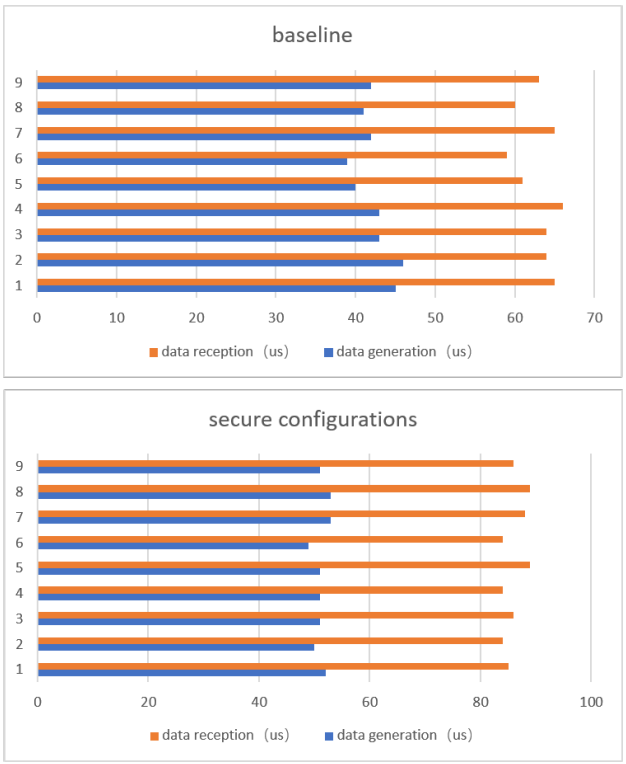


Fig. 3. Latency incurred by security and incentive operations

Fig. 4 depicts the effect of the proposed game-theoretic incentive mechanism on activity within a population of 20 IIoT data providers. The y-axis represents number of successful data uploads a proxy for engagement level and the x-axis lists the unique IDs of individual participants. Two groups of data points are shown: blue dots representing levels of engagement before incentives, and red dots representing behavior after incentives. Before the incentive mechanism was applied, most participants experienced moderate activity with frequencies of uploads binned between 6 and 8 events. Several outliers towards the lower end consistently returned the minimum, showing a general problem with volunteer data-sharing schemes: participants only participate if there is something in it for them, especially if participating costs anything computationally or in terms of privacy. With the introduction of the reward system, increased participation is observed in nearly all the participants. Incentive period uploads are distinctly between 9 and 12, with some participants achieving the maximum

seen level of participation that is 12. The increased dispersion and levelling of red data points distinctly reveal that average participation not only increased due to the reward-based motivation but also the issue of passive or "free-riding" agents was reduced. Even the erstwhile low contributors demonstrated considerable change in behavior. This figure provides strong empirical support for the performance of incentive schemes in IIoT networks. It demonstrates that if rewards depend on data quality and quantity, computed and distributed under an open algorithm, stakeholders will be much more likely to be actively engaged and persistent. This engagement is a must in decentralized data-sharing networks, where data variability and volume directly impact system performance and intelligence quality.

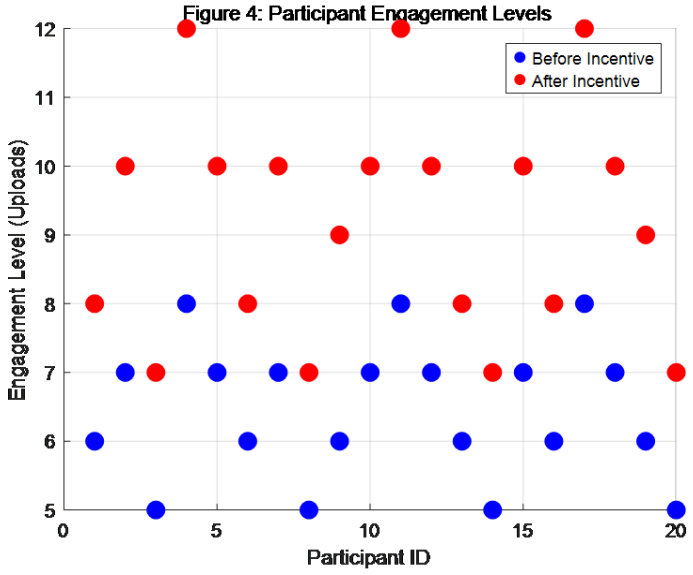


Fig. 4. Participant engagement levels before and after applying the incentive mechanism

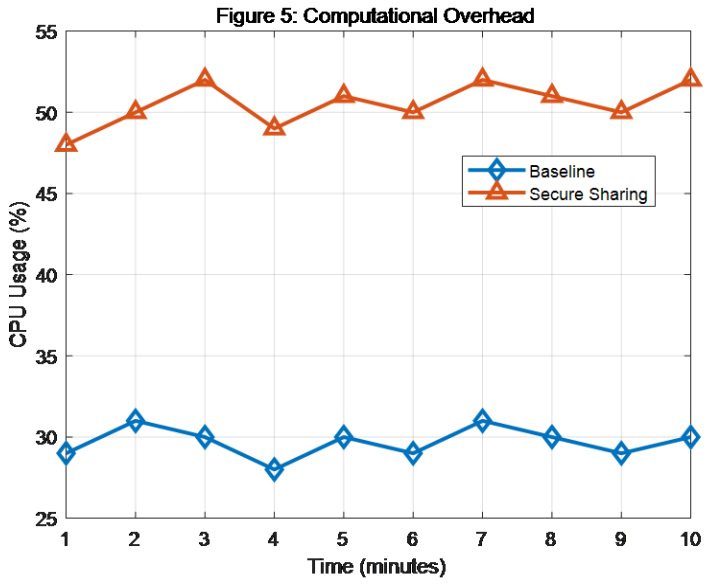


Fig. 5. Computational overhead measured by CPU usage

Fig. 5 shows the CPU utilization for 10-minute intervals between the baseline system and the proposed secure sharing system. The unit of measurement is a good measure of the computational overhead incurred during data processing and communication activities in an IIoT setting. The base configuration (represented by the blue line and diamond markers) maintains a relatively flat and low CPU activity. Values between 28% and 31% reflect lean operations, where there are few complex security or incentive calculations. This is a normal data transmission profile with minimal processing layers that prioritizes throughput and speed at the expense of the system being vulnerable to abuse or access. In contrast, the secure sharing mechanism (represented by the orange triangle markers) maintains a constant CPU utilization between 48% and 53%. This is to be expected, given the need for additional encryption and decryption processing, authentication, real-time anomaly detection using digital twin, and the operation of incentive evaluation algorithms. Despite the increased load, the utilization remains at an acceptable level for industrial-grade edge devices and control nodes [21]. The clear dividing line between the two graphs ensures that the computational overhead of the secure intelligence sharing mechanism is within bounds. The overhead is not high, but it does not grow over time, which indicates that the system is scalable and deployable in real applications. The predictability of CPU demand is particularly important in industrial real-time systems, where resource allocation must be precisely planned.

Fig. 6 shows the comparison of the total system utility of the baseline approach and the secure incentive scheme in a 10-minute simulation. System utility is a normalized overall metric that integrates performance, security, and stakeholder engagement to reflect the overall efficiency of the data sharing environment [22]. The baseline setup has relatively low utility levels, ranging from 0.58 to 0.63. This reflects the capabilities of the unprotected, unincentivized system: despite optimal throughput and latency, without security mechanisms, leakage rates are high and economic incentives are low, inhibiting users from contributing. As a result, the overall utility is limited by low trustworthiness and low contribution consistency, especially in open or adversarial IIoT networks. On the other hand, the proposed strategy, which employs encryption, authentication, digital twin-based confirmation, and game-theoretic incentives, achieves significantly higher utility values. These values consistently range from 0.83 to 0.89, an improvement of about 30% to 100% relative to the baseline. 40%, which is a significant improvement. Although latency and computational overhead are increased, the strategy has lower violation rates, fair participation, and sustained user engagement [23]. These advantages outweigh the costs and together improve the trustworthiness and work efficiency of the system. The relatively flat shape of the two curves indicates that the system remains stable under time-varying conditions, while the higher level of the new method confirms that the combination of security and economic incentives can build more robust and efficient industrial IoT systems. This result is particularly important in applications such as predictive maintenance, quality monitoring, and industrial monitoring where data integrity and on-time coordination are critical.

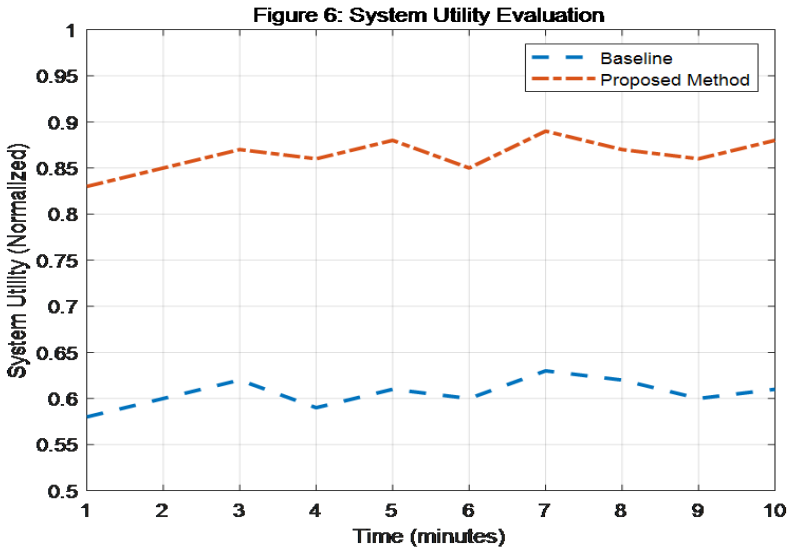


Fig. 6. Overall system utility combining security, incentive, and performance metrics

7 Conclusion

This paper proposes a comprehensive unified, secure, and incentivized data sharing framework for IIoT environments with the help of digital twin technology. Its innovation lies in combining real-time feature verification and system monitoring based on digital twin with game-theoretic incentive mechanisms to promote trust and participation of distributed data providers. This two-layer solution solves the long-standing problems in IIoT systems, data confidentiality, provider participation, and fair resource sharing, without sacrificing operational efficiency.

Through extensive modeling and large-scale simulation experiments, the proposed scheme outperforms the baseline solution on multiple key performance indicators. Specifically, the secure sharing scheme reduces the level of data leakage by more than 75%, improves the participation of almost all participants, and achieves a more balanced incentive distribution through dynamic reputation scoring. Although the system incurs moderate latency and CPU overhead due to encryption and incentive processing, the significant improvement in overall system utility is more than enough to make up for it. The system maintains a stable throughput, exhibits strong resistance to malicious behavior, and can scale well with the growth of the number of participants and data volume.

These findings confirm that the integration of digital twin-assisted validation and smart incentive mechanisms lays a solid foundation for future IIoT ecosystems. Its added value lies not in simplifying isolated dimensions such as security or efficiency, but in providing an integrated end-to-end solution that balances the interests of stakeholders, guarantees data integrity, and encourages sustainable cooperation in complex industrial environments.

In summary, this study provides an efficient, scalable, and secure Industrial IoT data ecosystem architecture that directly responds to the urgent need for trusted, automated, and incentive-compatible data sharing. The framework shows that digital twin combined with economic and behavioral modeling can significantly enhance the feasibility and resilience of industrial data management systems. Current research will enhance the solution to include adaptive trust models, real-time anomaly remediation support, and cross-domain interoperability in multi-vendor industrial ecosystems, building on the vision of a smart, autonomous, and secure IIoT infrastructure.

This article conducts in-depth research on the key technologies of data sharing for industrial IoT digital twins, considering issues such as data security and privacy, data quality, publishing efficiency, and transmission speed of shared data. However, considering other security aspects, with the development of network technology and the complexity and variability of network environments, attack techniques are constantly evolving. Attackers' attack methods will become more destructive and novel. Therefore, from the perspective of industrial IoT digital twin technology and data sharing technology, further in-depth research can be conducted in the following areas in the future:

1) Encryption technology is a core component of shared data sharing and data security, ensuring that shared data is not cracked by attackers during transmission and storage. With the development of quantum computing, the encryption algorithm used in this article will no longer be secure. Therefore, in future research, it is necessary to continue to study encryption algorithms that resist quantum computer attacks, such as lattice based encryption, multivariate encryption, hash function based encryption, etc.

2) Access control is an important component in ensuring the security and privacy of shared data. The existing access control technologies may not be able to cope with the diversity and complexity of future application scenarios. In future research, optimization methods for re access control models should be strengthened to make them applicable to dynamic and complex access control scenarios, automatically adjusting access permissions based on user behavior and environmental changes, and improving system security and flexibility.

3) Although the lightweight sensor data integrity detection method proposed in this article for industrial Internet of Things effectively improves the quality of shared data by detecting forged data, missing data, duplicate data, and erroneous data, this method cannot effectively cope with data integrity detection of complex structures. In future research, the data integrity detection method proposed in this article should be optimized to further improve its performance.

8 Acknowledgement

Research on Key Technologies of Machine Vision Recognition and Flexible Sorting for Multi-variety and Small-batch Parts (ZD26002).

References

[1] S. Munirathinam, Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT), Advances in Computers 117(2020) 129–164.
https://doi.org/10.1016/bs.adcom.2019.10.010

[2] M.B. Al Zami, S. Shaon, V.K. Quy, D.C. Nguyen, Digital Twin in Industries: A Comprehensive Survey, IEEE Access 13(2025) 47291–47336.
https://doi.org/10.1109/ACCESS.2025.3551532

[3] D.-M. Lee, S.-H. Lee, N. Masoud, M.S. Krishnan, V.C. Li, Integrated digital twin and blockchain framework to support accountable information sharing in construction projects, Automation in Construction 127(2021) 103688.
https://doi.org/10.1016/j.autcon.2021.103688

[4] P. Kumar, R. Kumar, A. Kumar, A.-A. Franklin, S. Garg, S. Singh, Blockchain and Deep Learning for Secure Communication in Digital Twin Empowered Industrial IoT network, IEEE Transactions on Network Science and Engineering 10(5)(2023) 2802–2813.
https://doi.org/10.1109/TNSE.2022.3191601

[5] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, A survey on physical unclonable function (PUF)-based security solutions for Internet of Things, Computer Networks 183(2020) 107593.
https://doi.org/10.1016/j.comnet.2020.107593

[6] P.-K.-R. Maddikunta, Q.-V. Pham, P. Dev, M. Prabadevi, B. Rodrigues, R. Kumar, Incentive techniques for the Internet of Things: A survey, Journal of Network and Computer Applications 206(2022) 103464.
https://doi.org/10.1016/j.jnca.2022.103464

[7] J.-B. Wen, J.-W. Kang, D. Niyato, Y. Zhang, S.-W. Mao, Sustainable Diffusion-Based Incentive Mechanism for Generative AI-Driven Digital Twins in Industrial Cyber-Physical Systems, IEEE Transactions on Industrial Cyber-Physical Systems 3(2024) 139–149.
https://doi.org/10.1109/TICPS.2024.3524483

[8] Y.-C. Zhu, Research on evolutionary game of digital twin data information sharing based on blockchain technology, Measurement and Control 58(1)(2024) 24–49.
https://doi.org/10.1177/00202940241245035

[9] Z.-H. Lv, D.-L. Chen, H.-B. Lv, Smart City Construction and Management by Digital Twin and BIM Big Data in COVID-19 Scenario, ACM Transactions on Multimedia Computing, Communications, and Applications 18(2s)(2022) 1–21.
https://doi.org/10.1145/3529395

[10] S.-B. Prathiba, G. Vignesh, R. Vinayakumar, M. Ghosh, R. Alharbi, M. Conti, Fortifying Federated Learning in IIoT: Leveraging Blockchain and Digital Twin Innovations for Enhanced Security and Resilience, IEEE Access 12(2024) 68968–68980.
https://doi.org/10.1109/ACCESS.2024.3401039

[11] X. Zheng, L. Tian, Z.-P. Cai, A Fair and Rational Data Sharing Strategy Toward Two-Stage Industrial Internet of Things, IEEE Transactions on Industrial Informatics 19(1)(2023) 1088–1096.
https://doi.org/10.1109/TII.2022.3179361

[12] D. Ivanov, A. Dolgui, B. Sokolov, Cloud supply chain: Integrating Industry 4.0 and digital platforms in the 'Supply Chain-as-a-Service', Transportation Research Part E: Logistics and Transportation Review (160)(2022) 102676.
https://doi.org/10.1016/j.tre.2022.102676

[13] S. Li, Y.-M. Li, S. Li, Digital Twin Assisted Edge Computing Task Offloading and Resource Allocation Strategy in Industrial Internet of Things, Journal of South China University of Technology (Natural Science Edition) 53(3)(2025) 88–96.
https://doi.org/10.12141/j.issn.1000-565X.240262

[14] X.-H. Zhao, H.-L. Liu, Y. Wang, Trusted fog computing resource allocation method with blockchain empowerment, Computer Engineering and Design 46(5)(2025) 1318–1326.
https://doi.org/10.16208/j.issn1000-7024.2025.05.011

[15] Q.-H. Xie, Z.-D. Bai, J.-Z. Zhao, Q.-H. Xie, Security sharing method of monitoring data of power grid equipment based on improved certificateless signature, Automation & Instrumentation (7)(2024) 168–171+175.
https://doi.org/10.14016/j.cnki.1001-9227.2024.07.168

[16] J.-J. Wang, D.-D. Mao, G.-T. Han, L.-F. Shen, N. Wang, A Survey of Physical Layer Secure Authentication and Key Agreement for 6G Wireless Communications, Mobile Communications 50(1)(2026) 25–34.
https://doi.org/10.3969/j.issn.1006-1010.20251106-0001

[17] N. Alhamam, M.M.H. Rahman, A. Aljughaiman, A Comprehensive Review on Cybersecurity of Digital Twin Issues, Challenges, and Future Research Directions, IEEE Access 13(2025) 45106–45124.
https://doi.org/10.1109/ACCESS.2025.3545004

[18] A. Tchernykh, U. Schwiegelsohn, E.-G. Talbi, M. Babenko, Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability, Journal of Computational Science 36(2019) 100581.
https://doi.org/10.1016/j.jocs.2016.11.011

[19] S. Alneyadi, E. Sithirasenan, V. Muthukkumarasamy, A survey on data leakage prevention systems, Journal of Network and Computer Applications 62(2016) 137–152.
https://doi.org/10.1016/j.jnca.2016.01.008
[20] B. Briscoe, A. Brunstrom, A. Petlund, D. Hayes, D. Ros, G. Tsoukaneri, J. Iyengar, M. Welzl, M. Fairhurst, R. Islam, Reducing Internet latency: A Survey of Techniques and Their Merits, IEEE Communications Surveys & Tutorials 18(3) (2016) 2149–2196.
https://doi.org/ 10.1109/COMST.2014.2375213
[21] D. Hästbacka, M. Kuusisto, O. Koskimäki, A. Heikkilä, P. Kuikka, Dynamic Edge and Cloud Service Integration for Industrial IoT and Production Monitoring Applications of Industrial Cyber-Physical Systems, IEEE Transactions on Industrial Informatics18(1)(2022) 498–508.
https://doi.org/10.1109/TII.2021.3071509
[22] X.-H. Zhao, Q.-Q. Liu, J.-L. Huang, X.-S. Wang, Research Developments on Utility Analysis and Evaluation Optimization of Traffic Sign System, China Journal of Highway and Transport 28(12)(2025) 174–199.
https://doi.org/10.19721/j.cnki.1001-7372.2025.12.003
[23] K. Menychtas, K. Shen, M.L. Scott, Disengaged scheduling for fair, protected access to fast computational accelerators, ACM SIGARCH Computer Architecture News 42(1)(2014) 301–316.
https://doi.org/10.1145/2541940.2541963