International Journal on Semantic Web and Information Systems
Volume 20 • Issue 1

Blockchain-Based Lightweight Authentication Mechanisms for Industrial Internet of Things and Information Systems

Mingrui Zhao, Shenyang Ligong University, China
Chunjing Shi, Shenyang Ligong University, China*
Yixiao Yuan, Northeastern University, China

ABSTRACT

The industrial internet of things (IIoT) necessitates robust cross-domain authentication to secure sensitive on-site equipment data. This paper presents a refined reputation-based lightweight consensus mechanism (LRBCM) tailored for IIoT's distributed network structures. Leveraging node reputation values, LRBCM streamlines ledger consensus, minimizing communication overhead and complexity. Comparative experiments show LRBCM outperforms competing mechanisms. It maintains higher throughput as the number of participating nodes increases and achieves a throughput approximately 10.78% higher than ReCon. Moreover, runtime analysis demonstrates LRBCM's scalability, surpassing ReCon by approximately 12.79% with equivalent nodes and transactions. In addition, as a combination of LRBCM, the proposed distributed lightweight authentication mechanism (ELAM) is rigorously evaluated against the security of various attacks, and its resilience is confirmed. Experiments show that ELAM has good efficiency while maintaining high security.

KEYWORDS

Blockchain, Identity Authentication, IoT, Lightweight, Reputation

1. INTRODUCTION

The internet of things (IoT) represents the concept of intelligent interaction, seamlessly connecting objects through intercommunication and information exchange. The industrial internet of things (IIoT) applies IoT technology to industrial production, integrating physical devices, sensors, and cloud computing to monitor, control, and optimize industrial processes (Sisinni et al., 2018; Sharma and Sharma, 2022; Yang et al., 2017; Hassija et al., 2019; Yao et al., 2021). In the modern industrial domain, IIoT has become an indispensable part, offering rich opportunities for machine-to-machine communication and automation. However, as devices and sensors become increasingly connected to networks, ensuring the authentication and data integrity of these devices is crucial (Mukherjee and Biswas, 2018; Wang et al., 2022; Nashwan, 2021; Raj and Prakash, 2022; Sengupta et al., 2020;

DOI: 10.4018/IJSWIS.334704 *Corresponding Author

Wang et al., 2019; Feng and Wang, 2022; Danish et al., 2020; Gupta et al., 2021). In the realm of IIoT security and authentication mechanisms, robust authentication mechanisms are urgently needed to protect industrial systems from malicious attacks and unauthorized access.

In recent years, numerous studies have focused on addressing security and authentication challenges in industrial IoT (Chen et al., 2021; Zhuang et al., 2019; Yuan et al., 2021; Yang et al., 2018; Pan et al., 2022; Shen et al., 2020; Esfahani et al., 2017; Xiong et al., 2020; Sadhukhan et al., 2021; Khalid et al., 2020; Stergiou et al., 2021; Wang et al., 2022; Mishra et al., 2022; Wang et al., 2019; Mohammadipanah and Sajedi, 2021; Fu et al., 2022). For example, research in machine-to-machine (M2M) communication has demonstrated outstanding performance compared to traditional methods (Nguyen et al., 2021). The rise of artificial intelligence and machine learning has also led to the proposal of various methods for detecting and preventing malicious software attacks (Zhang et al., 2023; Ling and Hao, 2022; Tembhurne et al., 2022; Xu et al., 2021; Gaurav et al., 2023; Lu et al., 2021; Ling and Hao, 2022; Sharma and Sharma, 2022; Devi and Bharti, 2022; Singh and Gupta, 2022).

Despite significant progress in recent years, device authentication in industrial IoT still faces many challenges. Existing authentication methods may not meet the growing needs of industrial IoT networks, especially in cases with a large number of devices, extensive network scale, and strict requirements for data integrity and confidentiality. Blockchain technology is widely considered a potential solution to address these challenges (Stergiou et al., 2021; Wang et al., 2022; Mishra et al., 2022; Wang et al., 2019; Mohammadipanah and Sajedi, 2021; Fu et al., 2022). Blockchain, as a scalable, distributed, and tamper-resistant ledger, exhibits unique advantages in maintaining consistent information records across different locations. Among these, the Reputation Proof-of-Work (PoR) blockchain proposed by Zhang et al. (2021) stands out for its security, resource efficiency, and decentralization. Additionally, ReCon (Reputation Consensus), incorporating a reputation module, is compatible with other consensus protocols. However, with the increasing interconnection of industrial devices, security threats correspondingly rise, necessitating a multi-layered security strategy to address challenges such as high resource consumption and low efficiency in cases with numerous devices.

This study aims to fill the research gap in the field of industrial IoT device authentication, addressing challenges such as a large number of devices, extensive network scale, and high requirements for data integrity and confidentiality. To tackle these issues, we introduce a lightweight reputation-based consensus algorithm, LRBCM, to achieve efficient consistency of authentication transaction data. The algorithm enhances the throughput and real-time capabilities of industrial IoT devices by reducing computational complexity and communication overhead. Subsequently, we propose a lightweight cross-domain authentication mechanism, ELAM, to ensure the security and efficiency of device authentication. The mechanism improves performance by reducing energy consumption and optimizing interoperability between devices.

The contributions of this paper include:

- Proposing the lightweight reputation-based consensus mechanism (LRBCM) to enhance authentication efficiency.
- Designing the distributed lightweight identity authentication mechanism (ELAM) for cross-domain trustworthy authentication.
- Conducting experiments and comparative analysis to evaluate the proposed consensus algorithm and identity authentication mechanism.

The paper is organized as follows: Section 2 summarizes related research, Section 3 presents the proposed lightweight consensus mechanism and the lightweight identity authentication mechanism, Section 4 presents experimental results and security analysis, and Section 5 provides the conclusion.

The data used to support the findings of this study are included within the article.

2. RELATED WORKS

1. **Blockchain:** Blockchain is a distributed ledger database widely deployed across distributed systems (Shen, 2022). It offers decentralized contract validation without the need for a trusted third party (Sober et al., 2023). This enhances trust in contract execution, reducing costs and alleviating operational traffic for central organizations (Liu et al., 2021). Moreover, all transactions within the blockchain are indisputable, as each network node maintains a ledger of executed transactions (Zafar et al., 2022). Encryption methods ensure the integrity of information blocks within the blockchain, ensuring the non-repudiation of communication. Additionally, through timestamp allocation, all users can track the progress of contract execution.
2. **Industrial Internet of Things (IIoT):** Emerging businesses worldwide face new standards, innovative trade methods, competitive pressures, and demands for timely goods transportation (Wan et al., 2019; Lloret and Parra, 2023). Therefore, many enterprises have turned to the industrial internet of things, a technology that collects information from thousands of interconnected machines, objects, and computers, aiding in business process modeling, monitoring, and improvement to achieve economic benefits. IIoT is a concept that connects and manages industrial equipment, objects, computers, and machines, bridging the physical and digital worlds (Dakhnovich et al., 2020).
3. **Trust and Reputation:** In social sciences, trust is at the core of interpersonal relationships, fostering interdependence. Luhmann defined trust as the foundation for simplifying interpersonal cooperation. Barbara Misztal pointed out in her work that trust makes social life predictable, creating a "sense of community" that facilitates collaboration. In information science, trust systems are built upon the trust concept from social sciences and, although devoid of subjective consciousness, they help derive trust relationships between nodes through reputation and context, promoting cooperation among distributed nodes.
4. **Gossip Protocol:** The gossip protocol is a crucial technology in P2P networks, widely used in distributed systems, functioning akin to the spread of rumors (Ishmaev, 2021). Similar to how someone in an office knows a rumor and shares it with those they know, who, in turn, share it with others (Abdi et al., 2023), eventually making everyone in the office aware of the rumor. In the gossip protocol, each node maintains its view, and in each communication round, each node selects several neighboring nodes to communicate with, using one of three communication methods.
5. **Elliptic Curve Cryptography (ECC):** Elliptic curve cryptography (ECC) is a public-key cryptography algorithm based on elliptic curve mathematics, with its security relying on the difficulty of the elliptic curve discrete logarithm problem.
6. **Combination of Blockchain and Industrial IoT:** Industrial IoT systems face multiple challenges, including weak interoperability, heterogeneity, resource constraints, trust, and security vulnerabilities. Blockchain technology can provide enhanced interoperability, trust, and security to balance industrial IoT systems. Furthermore, blockchain contributes to improving the reliability and scalability of industrial IoT systems (Jia et al., 2023).

3. METHODOLOGY

3.1 Basic Design Principles of the Lightweight Consensus Mechanism

3.1.1 Main Idea of the Method

In this study, we aim to address the critical challenges of security and efficiency in device authentication within the industrial internet of things (IIoT). To achieve this objective, we propose two novel mechanisms: a lightweight reputation-based consensus algorithm for authentication transaction data consistency (LRBCM) and a lightweight cross-domain identity authentication mechanism for efficient

and secure device authentication (ELAM). The selection of LRBCM and ELAM is primarily based on their lightweight design and strong real-time performance. LRBCM employs a mechanism cycle to ensure the trustworthiness of attestations, while ELAM leverages elliptic curve cryptography to swiftly establish trusted authentication channels across domains. These two methods combine security with higher efficiency and real-time capabilities. Furthermore, our choices also take into account the scalability and configurability of these methods in practical applications to ensure their wide adoption in the industrial IoT environment.

3.1.2 Reputation-Based Lightweight Consensus Mechanism Design

As depicted in Figure 1, the framework of the lightweight reputation-based consensus mechanism (LRBCM) comprises the following key components:

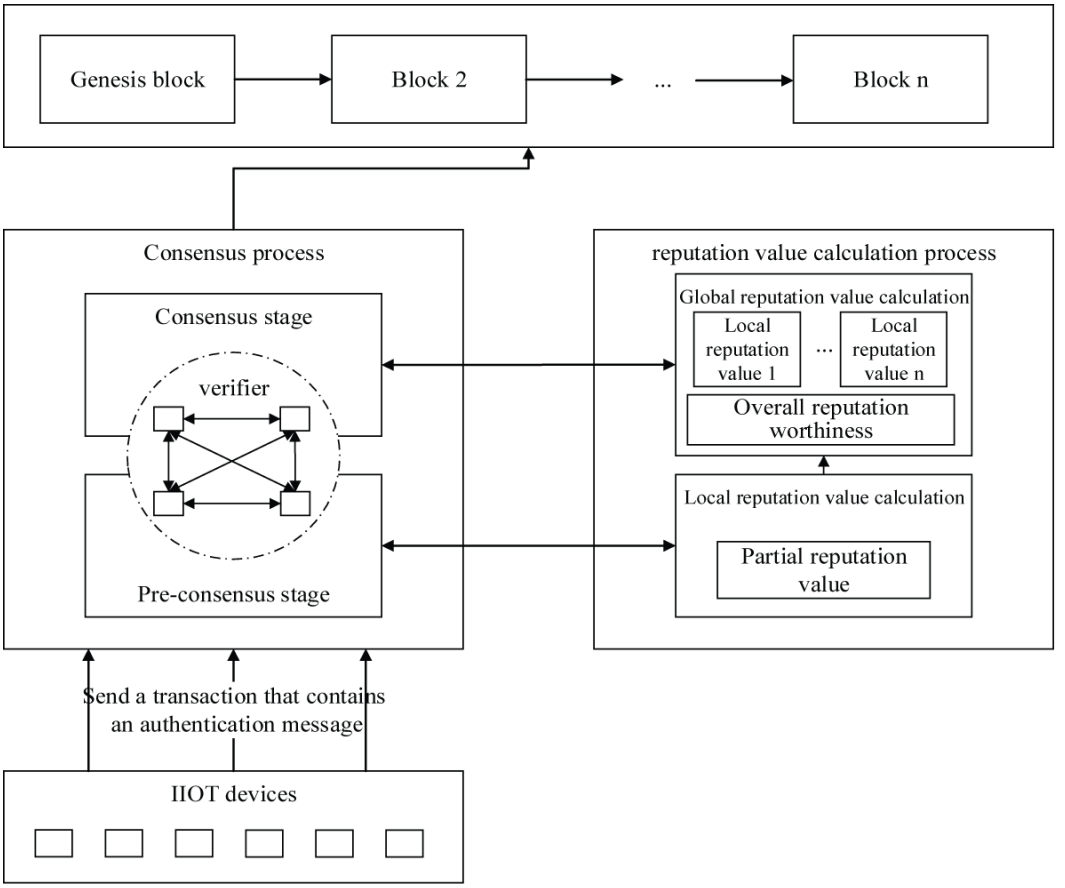
1. **Node Reputation Calculation Module:** Each network node possesses an associated reputation value reflecting its trustworthiness within the network. The reputation value is computed based on the node's historical behavior and performance in participating in the consensus process.
2. **Consensus Process Module:** LRBCM employs a consensus algorithm to determine which nodes are eligible to generate new blocks or validate transactions based on their reputation values. The consensus algorithm typically involves weighted random selection based on reputation scores.
3. **Distributed Ledger Module:** All reputation values and transaction histories are recorded on the blockchain's distributed ledger, ensuring data transparency and immutability.

The following steps outline the LRBCM framework proposed in this paper:
Step 1: Industrial internet of things (IIoT) devices send valid transactions containing authentication information within a specified time period.
Step 2: These transactions with authentication information enter the consensus process, which includes the pre-consensus and consensus phases. Validators in the consensus process are responsible for verifying the validity of transactions and placing them into the blockchain. Each cloud server can act as a validator.
Step 3: During the consensus process, validators examine the validity of transactions and include them in a block.
Step 4: After validation, validators reach pre-consensus to determine the accepted transactions and their order.
Step 5: After the pre-consensus phase, communication occurs with the reputation value calculation process. Each validator announces transactions and the number of transactions that can be recorded in the current block.
Step 6: In the local reputation calculation part of the reputation value calculation process, the local reputation of each validator is computed over a specific period.
Step 7: After calculating the local reputations, the global reputation calculation part calculates the overall reputation of each validator, representing its reputation over all periods.
Step 8: During the consensus phase, validators choose the validator with the highest global reputation value to create the current block and reach consensus, incorporating the recordable transactions into the block.
Step 9: The validator with the highest global reputation value publishes the current block.

3.1.3 Reputation-Based Lightweight Consensus Mechanism Algorithm

The credibility model of distributed networks lacks strict classification criteria. Based on the source of relevant information data when synthesizing node credibility values, the credibility model can be categorized into two types: global credibility model, local credibility model, and a combination of global credibility and local credibility models with confidence factors. In this paper, the reputation of each validator is calculated at two levels:

Figure 1. Depicts the framework of LRBCM



1. Local credibility calculation, as shown in Equation (1).

The steps involved in the LRBCM framework are as follows as Figure 1:

$$RL = \frac{NRT}{NRT + NUT} \tag{1}$$

In this context, RL denotes the local reputation of each validator. NRT represents the number of transactions recorded by validators in the current block, while NUT signifies the number of transactions that validators are unable to record in the current block.

2. The computation of global reputation is formulated as shown in Equation (2):

$$RG(n) = (\alpha)RL(n) + (1-\alpha)RG(n-1) \tag{2}$$

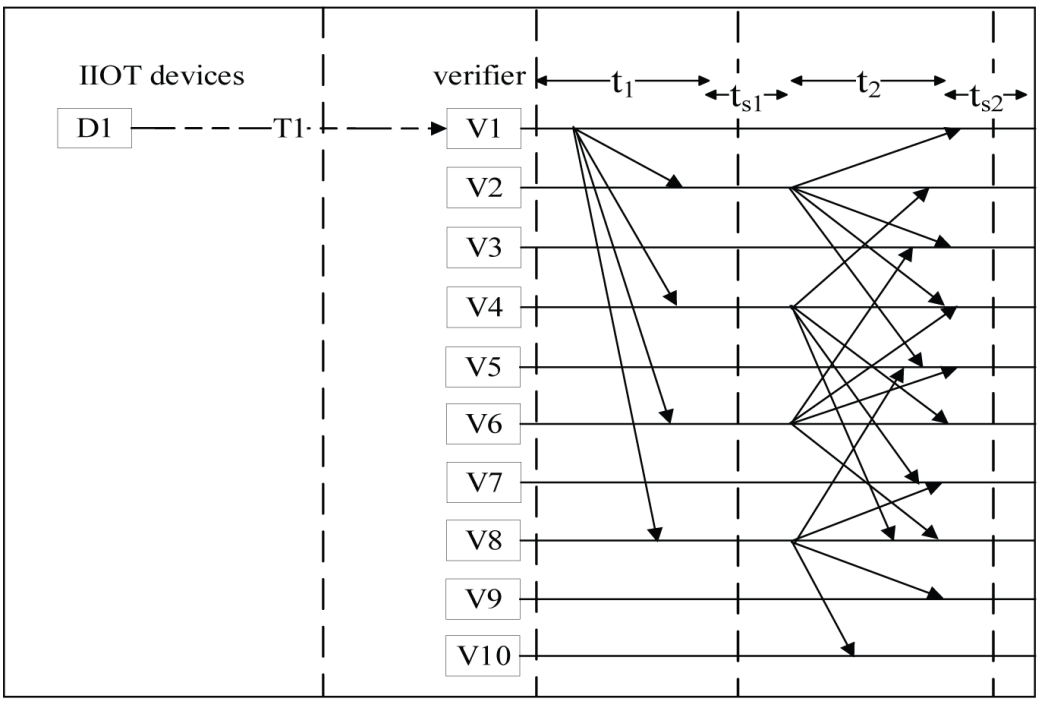
RG(n) and RL(n) denote the global reputation score and local reputation score, respectively, of each validator in the last block (current block). RG(n-1) represents the global reputation score of validators before the last block, serving as a parameter to assess the impact of time on calculating the reputation change of each validator over time.

The lightweight consensus mechanism consists of a pre-consensus phase and a consensus phase, both executed at each time interval, with the current block being created and published at the end of each time period.

1. Pre-Consensus Phase

In the pre-consensus phase, each validator signs the received transactions and propagates them to a randomly selected set of other x validators using the gossip protocol. The average pre-consensus time required for different values of x was evaluated through experiments, and this study set x=4. Figure 2 provides an overview of pre-consensus in LRBCM where over 60% of validators achieve consensus on the transactions after two rounds of propagation. industrial internet of things (IIoT) device D_1 creates one or more transactions, which are received and evaluated by validators $V_1, V_2, ..., V_{10}$. Pre-consensus is reached within the specified time period for transaction quantity and order. After each time period ends, validators synchronize an acceptable time for transactions, t_{s1}, t_{s2} are to create a block that achieves consensus. Here, $D_n T_m$ represents which IIoT device each transaction belongs to; for example, if IIoT device 1 creates three transactions, then $D_n T_m = \{D_1 T_1, D_1 T_2, D_1 T_3\}$.

Figure 2. Overview of the pre-consensus of the LRBCM



This paper employs the balance model to save records and customizes vector clocks based on transaction creation timestamp (t_c) and transaction reception timestamp (t_r). For transactions with the same creation timestamp, validators sort them based on the transaction reception timestamp. For transactions with different creation timestamps, validators sort them based on the transaction creation timestamp, as shown in Figures 3(a) and (b).

2. Consensus Phase

In the consensus phase, all validators with equal opportunities declare the transactions they can process and record them in the current block. The reputation of each validator is calculated at two levels: local reputation and global reputation. The formula for calculating local reputation is shown in Equation (3)

$$RL_i = \frac{\alpha p_r + \beta p_u}{p_r + p_u} \left(i = 1,2,3,\ldots,n\right) \tag{3}$$

where p_r represents transactions recorded in the block p and p_u represents transactions not recorded in the block p, with $\pm$ and ^{2} being weights for recorded and not recorded valid transactions, set to 1 and 0, respectively. The default reputation value is set to 0.5. Based on the aforementioned scenario, the local credibility calculation formula for each validator is presented in Equation (4).

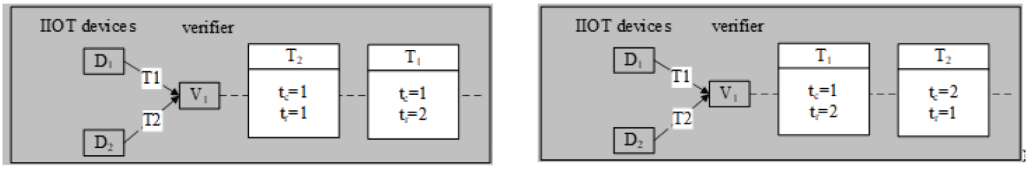
$$RL_i = \frac{p_r}{p_r + p_u} (i = 1,2,3,\ldots,n) \tag{4}$$

The formula for calculating global reputation (RG) is shown in Equation (5)

$$RG(n) = (\alpha)RL(n) + (1-\alpha)RG(n-1) \tag{5}$$

where RG(n) represents the global reputation value of each validator in the last block (current block) over a certain period, RG(n-1) represents the global reputation value of the validator before the last block, and RL(n) represents the local reputation value of each validator in the last block (current block). The initial global reputation value RG(1) is set to 0.5, and α is an adjustable parameter that determines the impact of time on reputation, set to 0.6 in this paper. The validator with the highest global reputation value is responsible for creating the current block. Any validator who obtains the highest global reputation value among other validators can create a block and append it to the blockchain to ensure that all validators hold the same copy of the latest version of the distributed

Figure 3. (a) Receiving the timestamp is different; (b) creating the timestamp is different



(a) (b)

ledger. To incentivize validators to improve efficiency and performance, a block creation reward (CBR) is introduced. The CBR is added as a numerical value to the validator's global reputation value. Based on the above content, the global reputation value is defined as shown in Equation (6)

$$RG(n) = \delta + (\alpha)RL(n) + (1-\alpha)RG(n-1) \tag{6}$$

where ′ is an adjustable weight parameter as a reward for the validator who creates the block. The computational time complexity of LRBCM is dependent on the number of validators (m) and the number of transactions (n). During the pre-consensus phase, each validator sends its received transactions to four other validators, resulting in a time complexity of 4mn. In the consensus phase, validators determine the block publisher based on the global highest reputation value, resulting in a time complexity assumed to be xm. Therefore, the overall time complexity of LRBCM is given by m(4n + xm).

In summary, the algorithm of LRBCM is shown in Table 1.

Table 1. The LRBCM algorithm

1: **input:** A transaction that contains authentication information for an industrial internet of things device
2: **output:** Publishes the current block containing authentication information transactions for industrial IOT devices
3: **begin**
4: **for** Each limited time period **do**
5: **begin**
6: Random verifiers receive new transactions
7: **begin**
8: **if** A transaction is a new transaction **then**
9: The validator creates a transaction timestamp based on the number of transactions
10: Sign the transaction
11: **if** Received transactions with the same creation time t_c **then**
12: Sign the transaction
13: **else**
14: SORT transactions by transaction creation time t_c
15: **if** Transactions are sent by other validators **then**
16: Synchronize the transaction timestamp according to the maximum value
17: SORT transactions
18: The number and order of inspection transactions
19: Check the d status
20: **if** d <60% then //less than 60% of validators agree on the number and order of transactions
21: **call** LRBCM
22: **else**//more than 60%
23: Return the number and order of transactions
24: **end**
25: **begin**
26: The verifier declares the number of transactions that can be recorded
27: Calculate local reputation //according to the formula 3
28: Calculate global reputation / /according to the formula 4
29: **if** Verifier obtains the highest global reputation value **then**
30: Add the CBR value to the global reputation value of the target verifier
31: Return to target verifier
32: **end**
33: Target verifier creates block
34: Target verifier publishes the current block and its distributed ledger
35: **end**
36: **end**

3.1.4 Performance Evaluation of LRBCM Network

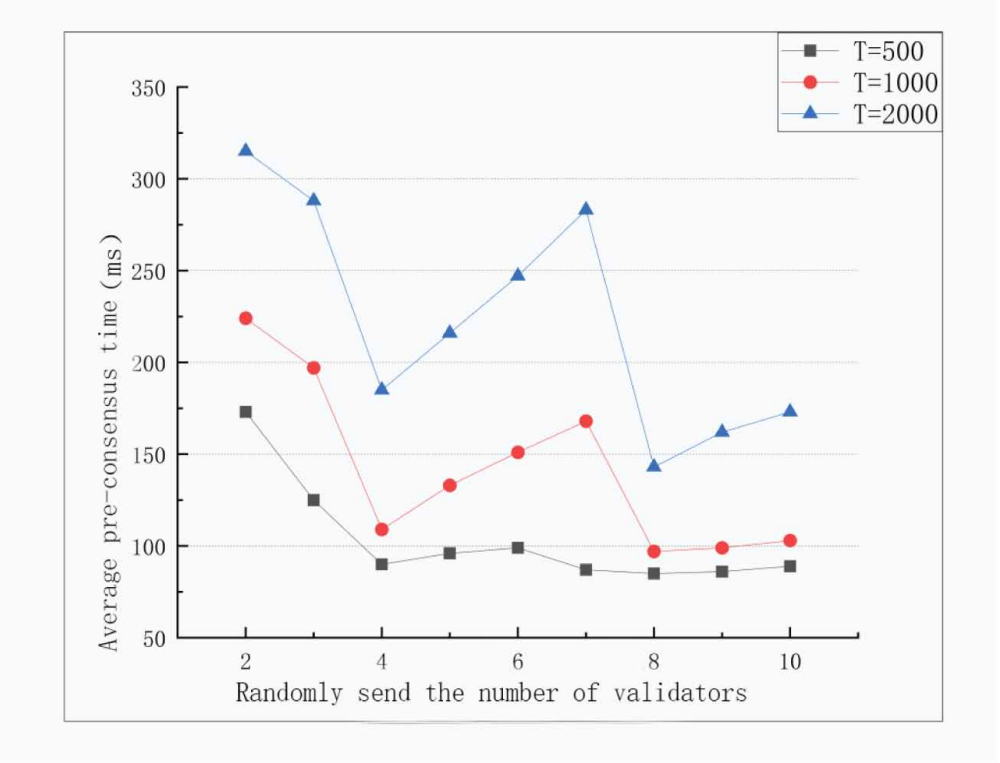
In the context of distributed networks for the industrial internet of things (IIoT), it is essential to minimize the computational cost of consensus algorithms while minimizing the occurrence of erroneous nodes. Additionally, achieving a higher transaction consensus rate within a given time frame is desired. To assess the computational overhead of the proposed LRBCM algorithm and evaluate its operational cost and complexity, this paper initially establishes a reasonably controlled experimental environment. The experiments were conducted on a computer running the Windows 10 operating system with hardware specifications comprising an Intel 2.5GHz i5 CPU and 8GB RAM. The simulations employ the Hyperledger Fabric component to emulate the consensus algorithm.

(1) Evaluation of LRBCM Average Pre-Consensus Time

In the process of achieving consensus among validators in the LRBCM algorithm, validators need to reach pre-consensus regarding the quantity and order of received transactions. During the pre-consensus phase, each validator is required to sign and transmit received transactions to a random subset of other validators. Consequently, this paper conducts an assessment of the average pre-consensus time required for transmission to randomly selected validators. In the course of the simulation experiments, varying numbers of validators and different transaction quantities are evaluated within a specified time frame for the assessment of the average pre-consensus time among validators. The experiment involves 1000 IIoT devices and 100 validators. The experimental results are illustrated in Figure 4.

From Figure 4, it is evident that the average pre-consensus time decreases with different transaction quantities until it slightly increases beyond a certain point. Notably, the variation in average pre-

Figure 4. Pre-consensus times for different numbers of validators were randomly sent



consensus time is minimal for different transaction quantities. Furthermore, considering the lightweight design for IIoT, this paper sets the number of validators randomly propagating transactions among themselves during the pre-consensus phase to be four.

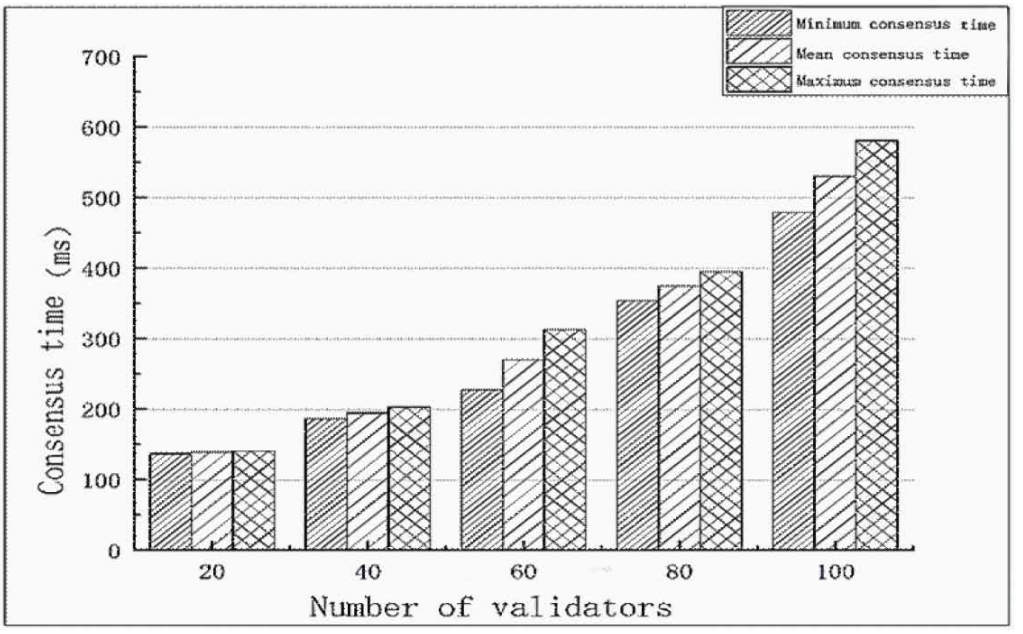
(2) LRBCM Consensus Time Evaluation

In this experiment, we investigated the consensus time in LRBCM under different numbers of validators, including the minimum consensus time, average consensus time, and maximum consensus time. Figure 5 illustrates the consensus time results for varying numbers of validators when the transaction count is 2000 and the number of IoT devices is 500. As the number of validators increases, the average time to achieve consensus increases due to the additional time required for transaction propagation among validators. To achieve preliminary consensus, each validator must transmit received transactions to four other validators.

(3) LRBCM Computational Time Complexity Assessment

LRBCM consists of two primary phases: the preliminary consensus phase and the consensus phase. In the consensus phase, after computing the local reputation values and global reputation values for validators, the validator with the highest global reputation is determined. Therefore, the computational time complexity of LRBCM depends on the number of transactions and validators, represented by "m" and "n," respectively. In the preliminary consensus phase, each validator transmits received transactions to four other validators, resulting in a computational time complexity of 4mn. In the consensus phase, validators determine the block producer based on the highest global reputation value, leading to a computational time complexity of 3m. Hence, the computational time complexity of LRBCM is given by m(4n+3).

Figure 5. Consensus time under different numbers of validators



3.2 Distributed Lightweight Identity Authentication Mechanism

3.2.1 Basic Idea of Distributed Lightweight Identity Authentication

To address the challenges of lightweighting memory and computation in industrial internet of things (IIoT) devices, as well as the susceptibility to malicious attacks and information leakage, we emphasize the need for a lightweight security identity authentication mechanism during sensitive information exchanges. Our proposed IIoT solution, ELAM, builds upon the lightweight reliable blockchain consensus mechanism (LRBCM) and utilizes elliptic curve cryptography (ECC) to streamline the authentication process. ELAM ensures secure information exchanges among authenticated IIoT devices, effectively reducing the potential impact of malicious entities on network security. As depicted in Figure 6, our distributed lightweight identity authentication framework includes fundamental modules for seamless implementation:

(1) Industrial Internet of Things Devices (IIoT Devices) and Key Generation Center (RA) Module: In this module, IIoT devices interact with the key generation center and the cloud server during the registration and authentication phases. The key generation center is responsible for selecting system parameters, generating the device's master key, and writing the device's credentials to the blockchain ledger.
(2) Cloud Server Module: This module encompasses all cloud service nodes (CS) and is responsible for verifying device credentials and signatures, generating session keys, and ensuring the smooth progression of the authentication process.
(3) Blockchain Ledger Module: This module is employed to store device credentials and authentication outcomes, guaranteeing data integrity and transparency.

3.2.2 Symbol Description

The symbols used in the proposed lightweight identity authentication mechanism for industrial internet of things (IIoT) are described as follows in Table 2.

3.2.3 Lightweight Identity Authentication Mechanism Based on Elliptic Curve Cryptography

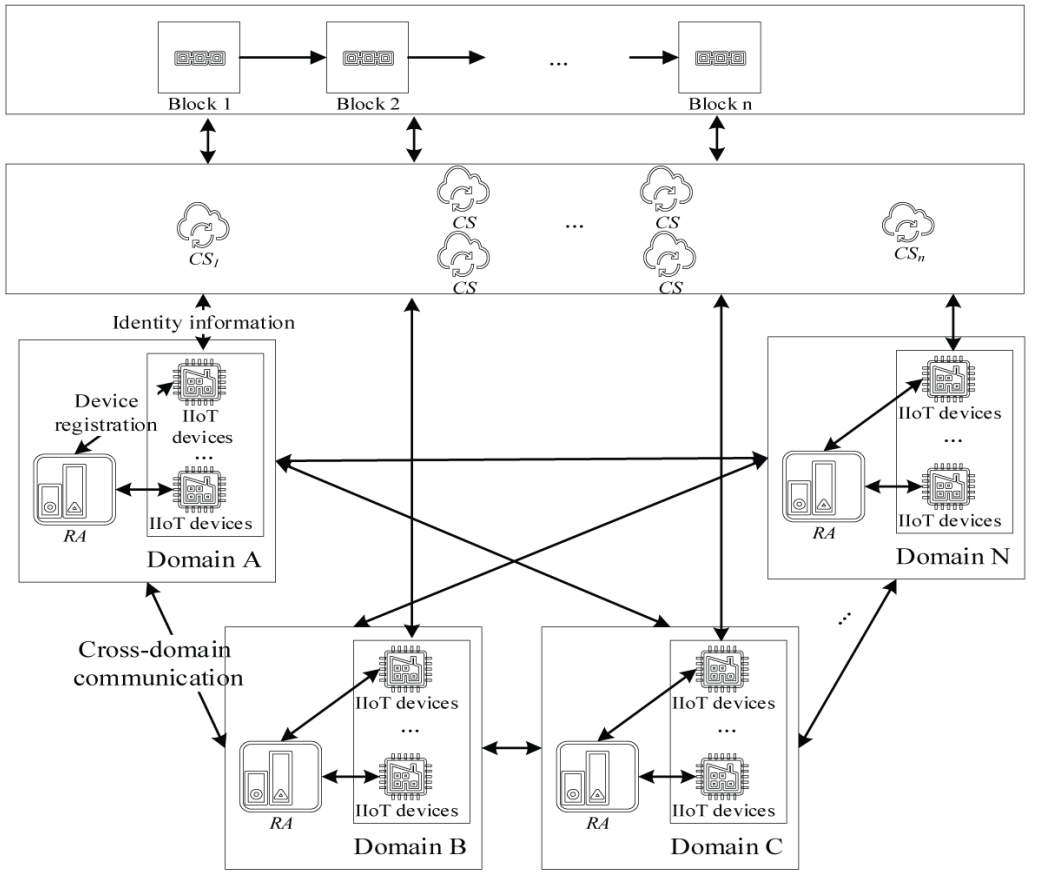
ELAM utilizes elliptic curve cryptography (ECC) for identity authentication through three modules. In the device-to-device (D2D) authentication phase, ELAM employs ECC for secure session key establishment via identity information and random secrets exchange. This involves message exchange and elliptic curve point calculations. During data transmission, ELAM ensures real-time data consistency using a lightweight reputation consensus mechanism, simplifying the process and reducing communication overhead. Ultimately, ELAM provides a secure environment for industrial internet of things (IIoT) devices to collaborate, exchange data, and maintain consistency and security in the network. The specific workflow of ELAM for trustworthy validation is outlined below:

(1) System Initialization Stage

In the system initialization stage, the key generation center (RA) selects system parameters through the following steps:

Step SIP_1: RA selects a non-singular elliptic curve $\mathrm{E}_q\left(a,b\right): y^2 = x^3 + ax + b\left(\mathrm{mod}\ q\right)$, in the finite field $\mathrm{GF}\left(q\right)$ with an "indeterminate point (zero point)" O, where constants $a,b \in Z_q = \left\{0,1,2,...,q-1\right\}$, satisfying $4a^3 + 27b^2 \neq 0\left(\mathrm{mod}\ q\right)$. RA chooses a base point $G \in E_q\left(a,b\right)$ of the same order as n_G, q. $n_G \cdot G = G + G + ... + G\left(n_G\right) = O$.

Figure 6. Lightweight identity authentication scheme architecture



Step SIP_2: RA selects a "collision-resistant one-way encryption hash function," such as $\mathrm{H}(\cdot)$ (using the SHA-256 hash algorithm), and the "LRBCM" algorithm for the consensus process in the blockchain cloud center.

Step SIP_3: Finally, RA selects its master key $\mathrm{mk}_{\mathrm{RA}}$ in $\mathrm{Z}_{\mathrm{q}}^{*}$ and publishes the domain parameters $\left\{\mathrm{E}_{\mathrm{q}}(\mathrm{a},\mathrm{b}),\mathrm{G},\mathrm{H}(\cdot)\right\}$ as the public key.

(2) Registration Stage

In the registration stage, the process for devices participating in the network is discussed. Figure 7 shows the process of the registration stage:

Step SDRE_1: Industrial IoT device SN sends a registration request to the key generation center (RA).

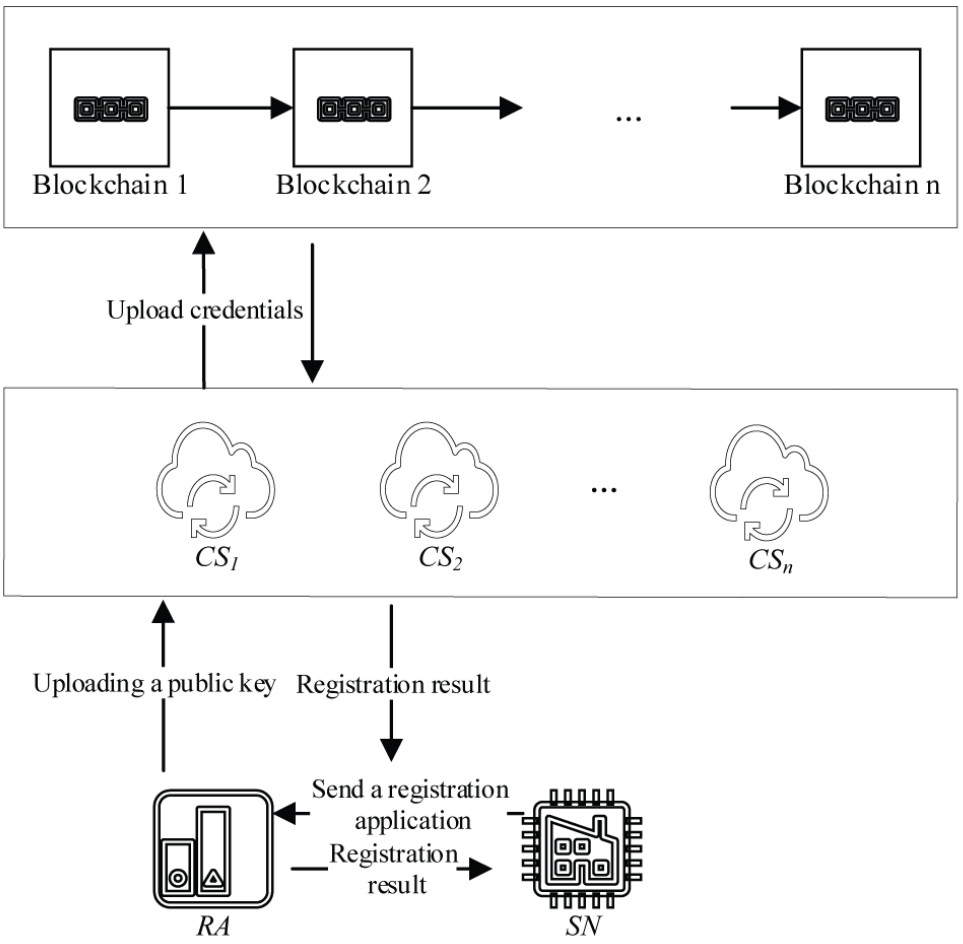
Step SDRE_2: RA selects a real identity ID_{S} and a temporary identity $\mathrm{TID}_{\mathrm{S}}$ for SN and uses a random secret $\mathrm{s}_1 \in \mathrm{Z}_{\mathrm{q}}^{*}$ to compute SN's pseudonymous identity $\mathrm{RID}_{\mathrm{S}} = \mathrm{H}\left(\mathrm{ID}_{\mathrm{S}} \parallel \mathrm{s}_1 \parallel \mathrm{mk}_{\mathrm{RA}}\right)$.

Table 2. Symbol description

Symbol	Description
$E_q\left(a,b\right)$	The form of a non upersingular elliptic curve: $\mathrm{y}^2 = \mathrm{x}^3 + \mathrm{ax} + \mathrm{b}\left(\mathrm{mod\ q}\right)$
G	One base point in $\mathrm{E_q}\left(\mathrm{a},\mathrm{b}\right)$. Its order is as large as $\mathrm{n_G}$ and q
$x \cdot G$	The point multiplication of an elliptic curve: $\mathrm{x} \cdot \mathrm{G} = \mathrm{G} + \mathrm{G} + ... + \mathrm{G}\left(\mathrm{xorder}\right)$
$P + Q$	Elliptic curve point addition: $\mathrm{P},\mathrm{Q} \in \mathrm{E_q}\left(\mathrm{a},\mathrm{b}\right)$
RA	Key generation center
SN	Industrial internet of things intelligent (sensor) equipment
CS	SERVER
RTS_X	The timestamp of registration with entity X for RA
TC_S	Temporary vouchers for SN
ID_X, TID_X, RID_X	Real, temporary, and pseudo identity equations for entity X
mk_{RA}	Master key for RA
pr_X, Pub_X	Private and public keys of entity X
s_1, g_1	Random secret of RA
r_{S1}, r_{S2}, p_S	Random secret of SN
$\|$	Concatenation
TS_X	The current timestamp generated by entity X
*	Modular multiplication in finite field $\mathrm{Z_q}$
ΔT	Maximum transmission delay related to messages
$H\left(.\right)$	Anti collision one-way encrypted hash function

Step $\mathrm{SDRE_3}$: RA randomly chooses a private key $\mathrm{pr_S} \in \mathrm{Z_q^*}$ and calculates the corresponding public key $\mathrm{Pub_S} = \mathrm{pr_S} \cdot \mathrm{G}$ and SN 's temporary credentials $\mathrm{TC_S} = \mathrm{H}\left(\mathrm{RID_S} \parallel \mathrm{pr_S} \parallel \mathrm{mk_{RA}} \parallel \mathrm{RTS_S}\right)$, where RTSS is the current registration timestamp for SN.

Figure 7. Registration phase



$\mathrm{StepSDRE}_4$: RA preloads SN with credentials $\left\{\left(\mathrm{RID_S}, \mathrm{TID_S}, \mathrm{TC_S}\right), \mathrm{H}(\cdot), \mathrm{E_q}\left(\mathrm{a}, \mathrm{b}\right), \mathrm{G}, \left(\mathrm{pr_S}, \mathrm{Pub_S}\right)\right\}$, and sends $\mathrm{Pub_S}$ as SN 's public key and $\left\{\left(\mathrm{RID_S}, \mathrm{TID_S}, \mathrm{TC_S}\right), \mathrm{H}(\cdot), \mathrm{E_q}\left(\mathrm{a}, \mathrm{b}\right), \mathrm{G}, \left(\mathrm{pr_S}, \mathrm{Pub_S}\right)\right\}$ as SN 's credentials $\mathrm{C_S}$ to the cloud server(CS).

Step $\mathrm{SDRE_5}$: The cloud server CS responds to RA 's request and writes SN 's credentials as a digital certificate into the blockchain ledger through the LRBCM using a smart contract.

Step $\mathrm{SDRE_6}$: After successful writing, CS sends a reply to RA , which then sends the registration result to SN , completing the registration process.

(3) Authentication and Key Agreement Stage

In the authentication and key agreement stage, the authentication process for device-to-device (D2D) is discussed, assuming that two devices have completed registration. Industrial IoT device $\mathrm{SN_1}$ needs to securely send its sensing data to another industrial IoT device $\mathrm{SN_2}$ in a different domain. The session key is established through the following steps:

Step D2D 1: Industrial IoT device SN_1, as the initiator, chooses a random secret $r_{S1} \in Z_q^*$ and the current timestamp TS_{S1}. It computes $x_{S_1} = H\left(RID_{S1} \parallel TID_{S1} \parallel TC_{S1} \parallel pr_{S1} \parallel TS_{S1} \parallel r_{S1}\right)$, $X_{S_1} = x_{S_1} \cdot G$, and the signature on rS1 as $Sig_{S1} = x_{S_1} + H\left(TID_{S1} \parallel Pub_{S1} \parallel TS_{S1}\right) * pr_{S1} \left(\text{mod } q\right)$. SN_1 sends the authentication request message $Msg_{D2D_1} = TID_{S1}, X_{S_1}, Sig_{S1}, Pub_{S1}, TS_{S1}$ to CS_2.

Step D2D 2: CS_2 receives the authentication request message Msg_{D2D_1} at the timestamp TS_{S1}^* and checks the validity of the timestamp with $\left|TS_{S1}^* - TS_{S1}\right| \leq \Delta T$. If valid, it verifies the signature through the smart contract. If successful, CS_2 generates the current timestamp TS_{S2} and sends the result back to SN_2.

Step D2D 3: SN_2, as the responder, receives Msg_{D2D_1} at the timestamp TS_{S2}^* and checks the validity of the timestamp with $\left|TS_{S2}^* - TS_{S2}\right| \leq \Delta T$. If valid, SN_2 chooses a random secret $r_{S2} \in Z_q^*$ and the current timestamp TS_{S3} to compute $y_{S_2} = H\left(RID_{S2} \parallel TID_{S2} \parallel TC_{S2} \parallel pr_{S2} \parallel TS_{S3} \parallel r_{S2}\right)$, $Y_{S_2} = y_{S_2} \cdot G$, and the shared secret (session key) with SN_1 as $SK_{S2S1} = y_{S_2} \cdot X_{S_1}$. The signature on the session key is $Sig_{S2} = y_{S_2} + H\left(TID_{S2} \parallel TID_{S1} \parallel Pub_{S2} \parallel SK_{S2S1} \parallel TS_{S3}\right) * pr_{S2} \left(\text{mod } q\right)$. SN_2 sends the authentication response message $Msg_{D2D_2} = TID_{S2}, Y_{S_2}, Sig_{S2}, Pub_{S2}, TS_{S2}$ to CS_1.

Step D2D 4: CS_1 receives Msg_{D2D_2} at the timestamp TS_{S3}^* and checks the validity of the timestamp with $\left|TS_{S3}^* - TS_{S3}\right| \leq \Delta T$. If valid, it verifies the signature through the smart contract. If successful, CS_1 generates the current timestamp TS_{S4} and sends the result back to SN_1.

Step D2D 5: If SN_1 receives Msg_{D2D_2} at the timestamp TS_{S4}, it checks the validity of the timestamp with $\left|TS_{S4}^* - TS_{S4}\right| \leq \Delta T$. If valid, SN_1 computes the shared secret (session key) with SN_2 as $SK_{S1S2} = x_{S1} \cdot Y_{S2}$. Then, SN_1 creates a new timestamp TS_{S5}, computes the session key verifier as $SKV_{S1S2} = H\left(SK_{S1S2} \parallel TS_{S5}\right)$, and sends the verification confirmation message $Msg_{D2D_3} = SKV_{S1S2}, TS_{S5}$ to SN_2.

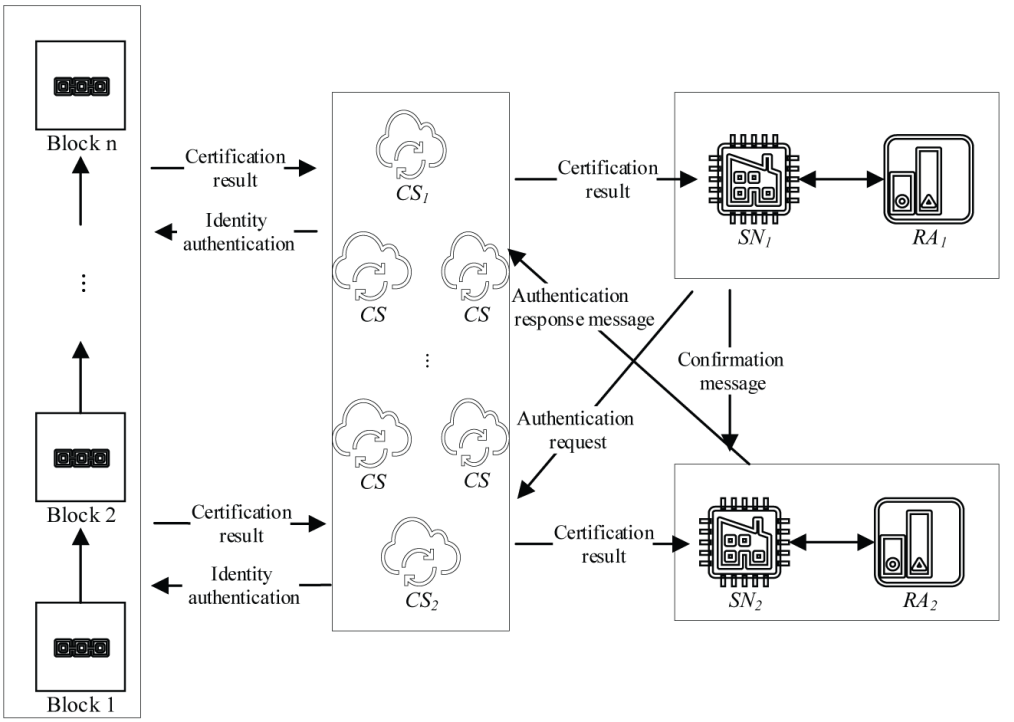
Step D2D 6: If SN_2 receives Msg_{D2D_3} at the timestamp TS_{S5}^*, it checks the validity of the timestamp with $\left|TS_{S5}^* - TS_{S5}\right| \leq \Delta T$. If valid, SN_2 computes the session key verifier as $SKV_{S2S1} = H\left(SK_{S2S1} \parallel TS_{S5}\right)$. SN_2 checks if SKV_{S2S1} is equal to SKV_{S1S2}. If valid, SN_1 and SN_2 share the same secret key $SKV_{S2S1} = SKV_{S1S2}$. The authentication phase is shown in Figure 8.

(4) Dynamic Smart Node Addition Stage

In this stage, when an existing industrial IoT device needs replacement due to failure or security issues, the key registration center (RA) deploys a new industrial IoT device SN^{new} to a specific area of the industrial domain in a temporary mode, following the steps below:

Step DSNA1: RA selects a real identity ID_S^{new} a temporary identity TID_S^{new}, and a random $S_1^{new} \in Z_q^*$. Then, for SN^{new}, it computes a pseudonymous identity RID $RID_S^{new} = H\left(ID_S^{new} \parallel S_1^{new} \parallel mk_{RA}\right)$ and selects a random private key $pr_1^{new} \in Z_q^*$. It calculates the corresponding public key $Pub_S^{new} = pr_S^{new} \cdot G$ and SN^{new}'s temporary credentials

Figure 8. Authentication phase



$\mathrm{TC}_{\mathrm{S}}^{\mathrm{new}} = \mathrm{H}\left(\mathrm{RID}_{\mathrm{S}}^{\mathrm{new}} \parallel \mathrm{pr}_{\mathrm{S}}^{\mathrm{new}} \parallel \mathrm{mk}_{\mathrm{RA}} \parallel \mathrm{RTS}_{\mathrm{S}}^{\mathrm{new}}\right)$, where $\mathrm{RTS}_{\mathrm{S}}^{\mathrm{new}}$ is the current registration timestamp for $\mathrm{SN}^{\mathrm{new}}$.

StepDSNA2: RA preloads $\mathrm{SN}^{\mathrm{new}}$ with credentials $\{\left(\mathrm{RID}_{\mathrm{S}}^{\mathrm{new}}, \mathrm{TID}_{\mathrm{S}}^{\mathrm{new}}, \mathrm{TC}_{\mathrm{S}}^{\mathrm{new}}\right), \mathrm{H}(\cdot), \mathrm{E}_{\mathrm{q}}(\mathrm{a}, \mathrm{b}), \mathrm{G}, (\mathrm{pr}_{\mathrm{S}}^{\mathrm{new}}, \mathrm{Pub}_{\mathrm{S}}^{\mathrm{new}}\}$, and sends $\mathrm{Pub}_{\mathrm{S}}^{\mathrm{new}}$ as $\mathrm{SN}^{\mathrm{new}}$'s public key.

3.2.4 Lightweight Identity Authentication Mechanism's Smart Contract Design

The execution logic of the smart contract is shown in Figure 9. When an IoT device initiates an authentication request transaction, the smart contract independently and automatically executes the contract code based on the data in the transaction, records the authentication execution result in the blockchain ledger through LRBCM consensus, and feeds back the authentication result to the applicant, thereby completing the authentication of the IoT device.

(1) Registration Smart Contract

When an industrial IoT device joins the network for the first time, it needs to register on the blockchain. The device submits a registration request to the key generation center and obtains credentials and a public key, which is then stored in the blockchain ledger. After receiving the confirmation message, the device is successfully registered and becomes a known device, and the registration process is completed.

(2) Authentication Smart Contract

Figure 9. Smart contract execution logic

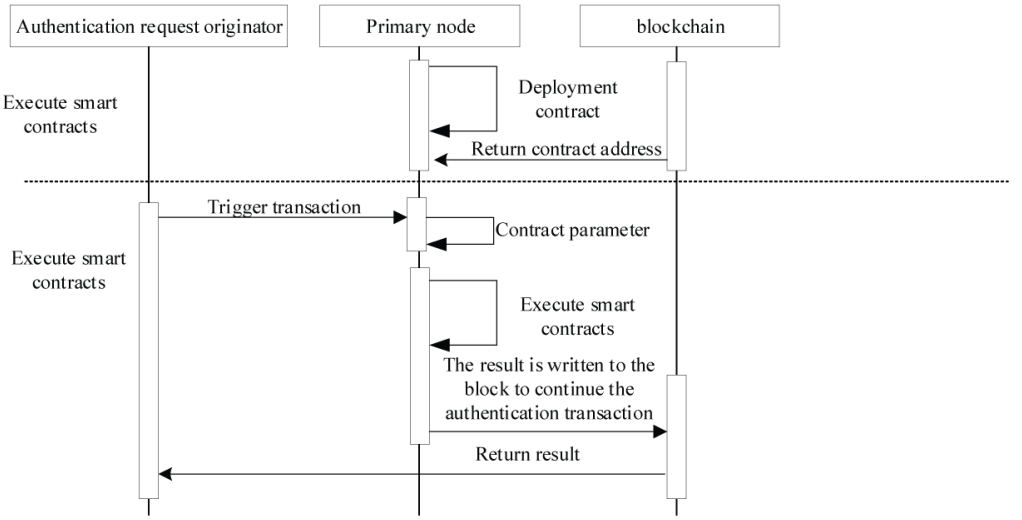


Table 3. Register for IIoT devices

1**: input:** ID_S , TID_S , mk_{RA} , ID_i /* ID_S : The true identity of the device; TID_S : Temporary identity of the device; mk_{RA} : Master key of the key registration center; ID_i : device identifier*/
2**: output:** industrial internet of things devices are registered or unregistered
3**: begin**
4**:** RA generate s_1
5: RA count RID_S
6: $SN \leftarrow RID_S$
7: RA select private key pr_S
8: RA count $Pub_S = pr_S \cdot G$
9: generate SN current timestamp
10: RA count TC_S
11: Generate Voucher C_S
12: Send credentials t C_S to CS
13: CS obtain the identifier of the device ID_i
14: **if** $ID_i =$ **true then //**the device is legal, can be connected
15: (C_S ,*timestamp*)consensus to CS *//using* TID_S *as the key value to store digital vouchers in a distributed ledger*
16: return industrial internet of things equipment has been registered
17: **else**
18: **return industrial internet of things equipment not registered**
19: **end if**
20: **end**

In the authentication process of industrial IoT devices, the industrial IoT device initiates an authentication request. The cloud server verifies the signature of the industrial IoT device based on its credentials. If the verification is successful, the cloud server responds with an authentication

Table 4. IIoT devices verification

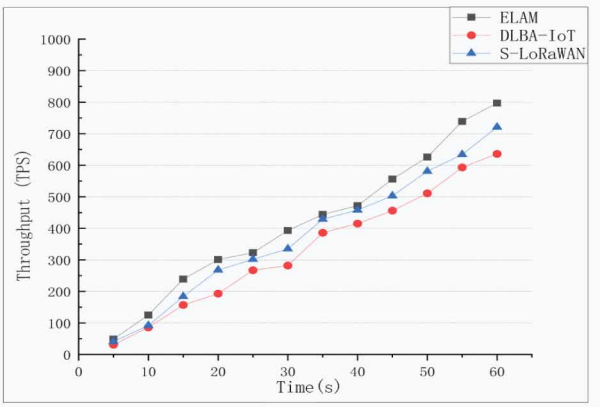
1: **input:** Msg , Sig /* Msg[*device verification message*; Sig[**Signature of the device***/
2: **output:** Successful or unsuccessful certification of industrial internet of things equipment
3: **begin**
4: SN_1 select random secret r_{S1} ,**generate current timestamp** TS_{S1}
5: count x_{S_1} , X_{S_1}
6: **Generate signature** Sig_{S1}
7: Send authentication request message ($TID_{S1}, X_{S_1}, Sig_{S1}, Pub_{S1}, TS_{S1}$)to CS_2
8: **if** $\left|TS^*_{S1} - TS_{S1}\right| \leq \Delta T$ **then**
9: **if** $Sig_{S1} \cdot G = X_{S_1} + H\left(TID_{S1} \parallel pub_{S1} \parallel TS_{S1}\right) \cdot pub_{S1}$ **then**
10: result consensus to CS **then //**store consensus authentication results in the block chain ledger**//**
11: CS_2 generate current timestamp TS_{S2}
12: Send verification results to SN_2
13: **if** $\left|TS^*_{S2} - TS_{S2}\right| \leq \Delta T$ **then**
14: SN_2 select random secret r_{S2} ,**generate current timestamp** TS_{S3}
15: count y_{S_2} , Y_{S_2} ,session key $SK_{S2S1} = y_{S_2} \cdot X_{S_1}$
16: Generate session key signature Sig_{S2}
17: Send authentication response message($TID_{S2}, Y_{S_2}, Sig_{S2}, Pub_{S2}, TS_{S2}$) CS_1
18: **if** $Sig_{S2} \cdot G \leftarrow Y_{S_2} + H\left(TID_{S2} \parallel TID_{S1} \parallel pub_{S2} \parallel SK_{S2S1} \parallel TS_{S3}\right) \cdot pub_{S2}$ **then**
19: result consensus to CS **then //**store authentication results in the block chain ledger**//**
20: CS_1 generate current timestamp TS_{S4}
21: Send verification results to SN_1
22: **if** $\left|TS^*_{S4} - TS_{S4}\right| \leq \Delta T$ **then**
23: SN_1 calculate session key $SK_{S1S2} = x_{S1} \cdot Y_{S2}$,generate current timestamp TS_{S5}
24: Calculate session key verification SKV_{S1S2}
25: Send verification confirmation message (SKV_{S1S2}, TS_{S5})to SN_2
26: **if** $\left|TS^*_{S5} - TS_{S5}\right| \leq \Delta T$ **then**
27: SN_2 calculate session key verification SKV_{S2S1}
28: **if** $SKV_{S2S1} \leftarrow SKV_{S1S2}$ **then**
29: return successful certification of industrial internet of things equipment
30: **else**
31: return industrial internet of things equipment certification failed
32: **end if**
33: **end**

success message, indicating that the identity authentication of the IoT device is successful. The smart contract algorithm for the IoT device authentication stage is shown in Table 4:

3.2.5 ELAM Performance Analysis

ELAM authentication mechanism is designed to accommodate the limited hardware capabilities and energy resources of industrial IoT devices, thereby reducing energy consumption. In the ELAM

Figure 10. Displays the throughput at different runtimes



authentication phase, identity and random secrets each require 160 bytes, the hash function outputs 256 bytes and 128 bytes, and the coordinates of points on the elliptic curve require 320 bytes. The timestamp is represented by 32 bytes. Consequently, during ELAM's D2D authentication phase, messages $\mathrm{Msg}_{\mathrm{D2D}_1}$, $\mathrm{Msg}_{\mathrm{D2D}_2}$, and $\mathrm{Msg}_{\mathrm{D2D}_3}$ require 992, 992, and 288 bytes, respectively, totaling 4256 bytes. In comparison to literature (Sadhukhan et al., 2021), ELAM requires fewer message exchanges, resulting in a communication overhead of 5248 bytes. ELAM's algorithm exhibits low computational complexity and communication cost, making it suitable for industrial IoT scenarios.

To compare the average delay between ELAM and existing schemes DLBA-IoT (Khalid et al., 2020) and S-LoRaWAN (Danish et al., 2020), throughput and average delay tests were conducted with 100 cloud server nodes and 100 devices. The experimental results are illustrated in Figure 10.

Figure 10 indicates that ELAM's rate of processing authentication requests per second increases with runtime and consistently surpasses the other two methods. This is achieved by utilizing elliptic curve cryptographic algorithms with shorter key lengths, improving processing and calculation speed, reducing processing delays, enhancing scalability, and utilizing the gossip protocol to distribute and propagate transactions among nodes, thereby increasing throughput and system performance. Compared to S-LoRaWAN, ELAM achieves approximately 11.35% higher throughput.

Figure 11. Average delay for different execution times

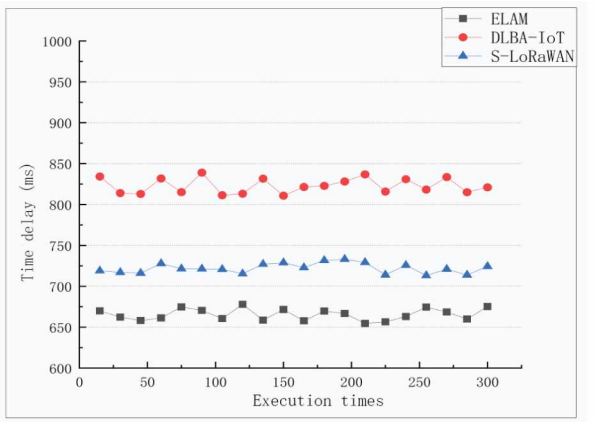


Figure 11 presents the average delay at different execution times. The average delay of DLBA-IoT is approximately 823 milliseconds, about 155 milliseconds higher than ELAM. Compared to S-LoRaWAN, ELAM exhibits approximately 7.83% slower delay. This is attributed to ELAM's theoretical research based on the discrete logarithm problem on elliptic curves, resulting in low algorithmic complexity and fast key generation. Additionally, ELAM optimizes the interactions between industrial IoT devices by offloading low-complexity calculations to the devices, reducing the burden on the devices. This approach decreases the interaction time for cross-domain authentication among industrial IoT devices, thereby improving authentication delay. The reduced authentication time enhances device security and ensures efficient and secure authentication in industrial IoT environments.

4. EXPERIMENTAL RESULTS AND COMPARATIVE ANALYSIS

To investigate the performance of the LRBCM lightweight consensus algorithm and the ELAM authentication mechanism, we established an experimental environment. We employed a computer running the Windows 10 operating system, equipped with an Intel 2.5GHz i5 CPU and 8GB RAM to simulate our experiments. Simultaneously, we utilized Hyperledger Fabric components for simulating the consensus algorithm to measure crucial performance metrics of LRBCM, such as average pre-consensus time, consensus time, throughput, consensus success rate, and average latency.

4.1 LRBCMD Throughput Level Comparison

This section aims to evaluate the performance and effectiveness of LRBCM by comparing it with two other consensus mechanisms, PoR, and ReCon. These two mechanisms were chosen for comparison due to their structural similarity with LRBCM, making them suitable as baselines for performance comparison.

Throughput is an important metric to evaluate the performance of a consensus algorithm. In this section, the throughput of LRBCM, PoR, and ReCon is compared. In the first experiment, the relationship between throughput and the number of nodes was studied. The transaction quantity was set to 2000, and the number of nodes was increased from 20 to 100.

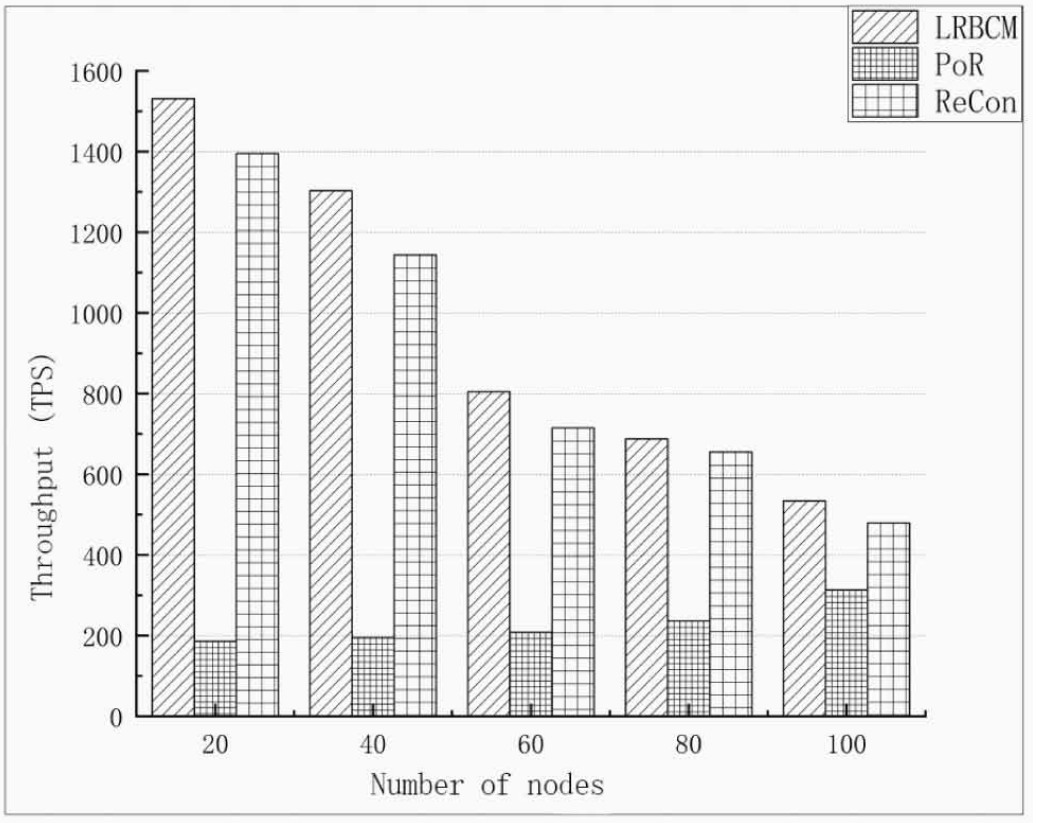
As shown in Figure 12, by increasing the number of participating nodes in the consensus mechanism, the throughput in both LRBCM and ReCon mechanisms slightly decreased. In LRBCM, as transactions need to circulate to four other nodes, and nodes synchronize all data after connecting to each other, the throughput decreases with an increase in the number of nodes. In the PoR mechanism, the throughput increases with an increase in the number of nodes but remains much lower than LRBCM, especially when the number of nodes participating in consensus is low. When the number of nodes is the same, LRBCM's throughput is approximately 10.78% higher than ReCon.

In the second experiment, the relationship between throughput and runtime was evaluated for the three algorithms, considering 100 nodes and 1000 transactions. As shown in Figure 13, with an increase in runtime, the performance gap between the three algorithms gradually increased. In LRBCM, using the reputation calculation model, the speed of processing and computation was increased, reducing processing delays, and enhancing scalability. The use of the gossip protocol to distribute and propagate transactions among validators helps increase throughput and improve system performance. When the number of nodes and transactions is the same, LRBCM's throughput is approximately 12.79% higher than ReCon.

4.2 Comparison Analysis of LRBCM Consensus Latency

Consensus delay is another important metric for evaluating the consensus algorithm. Figure 14 shows the relationship between the number of consensus nodes and the average consensus delay for different consensus mechanisms. With 1000 transactions, LRBCM and ReCon algorithms showed similar average delays with 20 to 100 participating nodes, but LRBCM's growth was slower. LRBCM's consensus delay decreased at a slower rate due to transactions being randomly sent to other validators

Figure 12. Throughput comparison at different numbers of nodes



using the gossip protocol, leading to a slower increase in consensus delay compared to ReCon. However, in the PoR algorithm, each node can individually generate a block, and increasing the number of consensus nodes resulted in more transactions and rapidly increasing network overhead, thus increasing the delay.

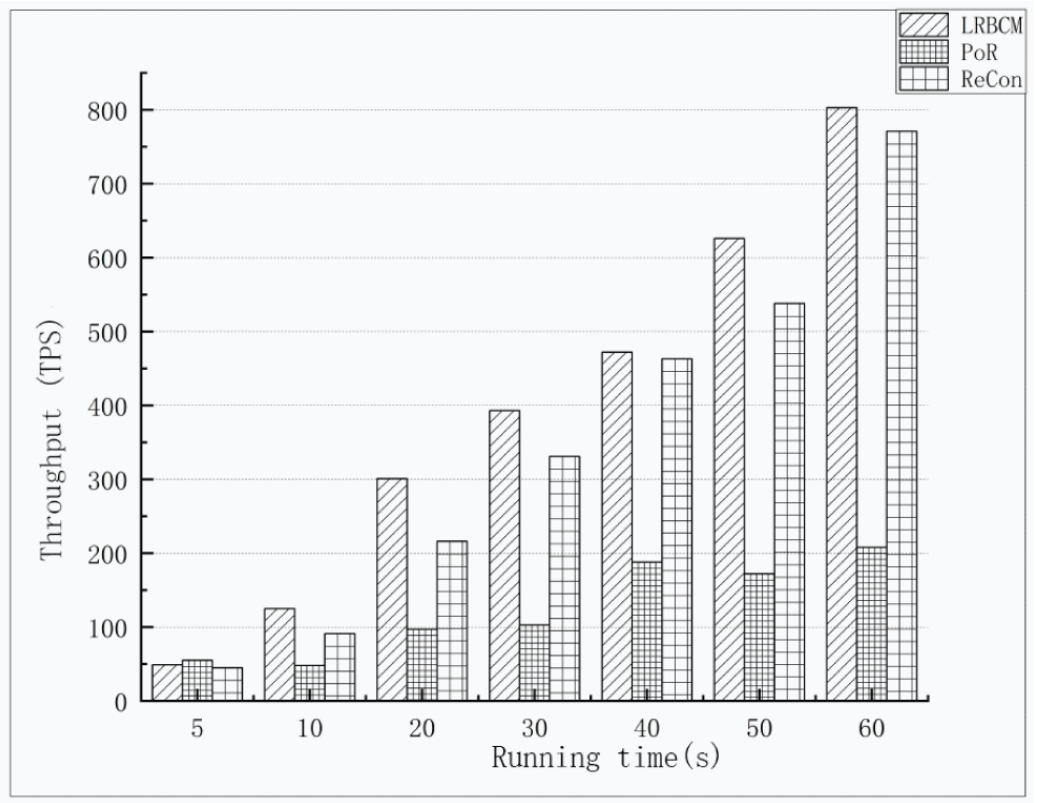
4.3 Security Analysis

In this section, we analyze the security of the session key under the real-or-random (ROR) model (Abdalla et al., 2005). In the D2D authentication phase of ELAM, a session key is established between two industrial IoT devices, SN_1 and SN_2. The security of this session key is proven based on the semantic security concept defined in Definition 1, and the security theorem is stated in Theorem 1. All entities involved have access to a "one-way encryption function H(.)", which is treated as a random oracle. Table 5 lists the queries available to the adversary.

Definition 1: Semantic Security: Let $Adv_A^{ELAS}\left(t_p\right)$ denote the adversary A's advantage in breaking the semantic security of ELAM within polynomial time t_p, to derive the session key $SK_{S1S2}\left(=SK_{S2S1}\right)$ between two industrial IoT devices, SN_1 and SN_2, during the D2D authentication phase.

Theorem 1: Assuming that the adversary A attempts to obtain the session key $SK_{S1S2}\left(=SK_{S2S1}\right)$ between SN_1 and SN_2 during the D2D authentication phase within polynomial time t_p, if q_h,

Figure 13. Throughput at different runtimes



$\left|\mathrm{Hash}\right|$, and $\mathrm{Adv}_{\mathrm{A}}^{\mathrm{ECDDHP}}\left(\mathrm{t}_{\mathrm{p}}\right)$ represent the number of hash queries, the range of the one-way collision-resistant hash function H(.), and the advantage in solving the elliptic curve decisional Diffie-Hellman problem (ECDDHP), respectively, then we have Equation (7).

$$\mathrm{Adv}_{\mathrm{A}}^{\mathrm{ELAS}}\left(\mathrm{t}_{\mathrm{p}}\right) \le \frac{\mathrm{q}_{\mathrm{h}}^{2}}{\left|\mathrm{Hash}\right|} + 2\mathrm{Adv}_{\mathrm{A}}^{\mathrm{ECDDHP}}\left(\mathrm{t}_{\mathrm{p}}\right) \tag{7}$$

Proof: In proving Theorem 1, we design three games. $\mathrm{Game}_{\mathrm{l}}^{\mathrm{A}}$, $\left(\mathrm{l}=0,1,2\right)$ in which the adversary A performs the execution. Let $\mathrm{Suc}_{\mathrm{Game}_{\mathrm{l}}}^{\mathrm{A}}$ represent the adversary A's advantage in correctly guessing a random number b in $\mathrm{Game}_{\mathrm{l}}^{\mathrm{A}}$, i.e., the probability of adversary A winning $\mathrm{Game}_{\mathrm{l}}^{\mathrm{A}}$ is $\mathrm{Adv}_{\mathrm{A,Game}_{\mathrm{l}}}^{\mathrm{ELAS}} = \Pr\left[\mathrm{Suc}_{\mathrm{Game}_{\mathrm{l}}}^{\mathrm{A}}\right]$. The adversary A interacts with ELAM in the following games:

(1) $\mathrm{Game}_{0}^{\mathrm{A}}$: In this game, before the start of $\mathrm{Game}_{0}^{\mathrm{A}}$, the adversary A chooses a random number to launch an actual attack on ELAM. Based on the semantic security defined in Definition 1, we get the Equation (8).

Figure 14. Average consensus delay at the different number of nodes

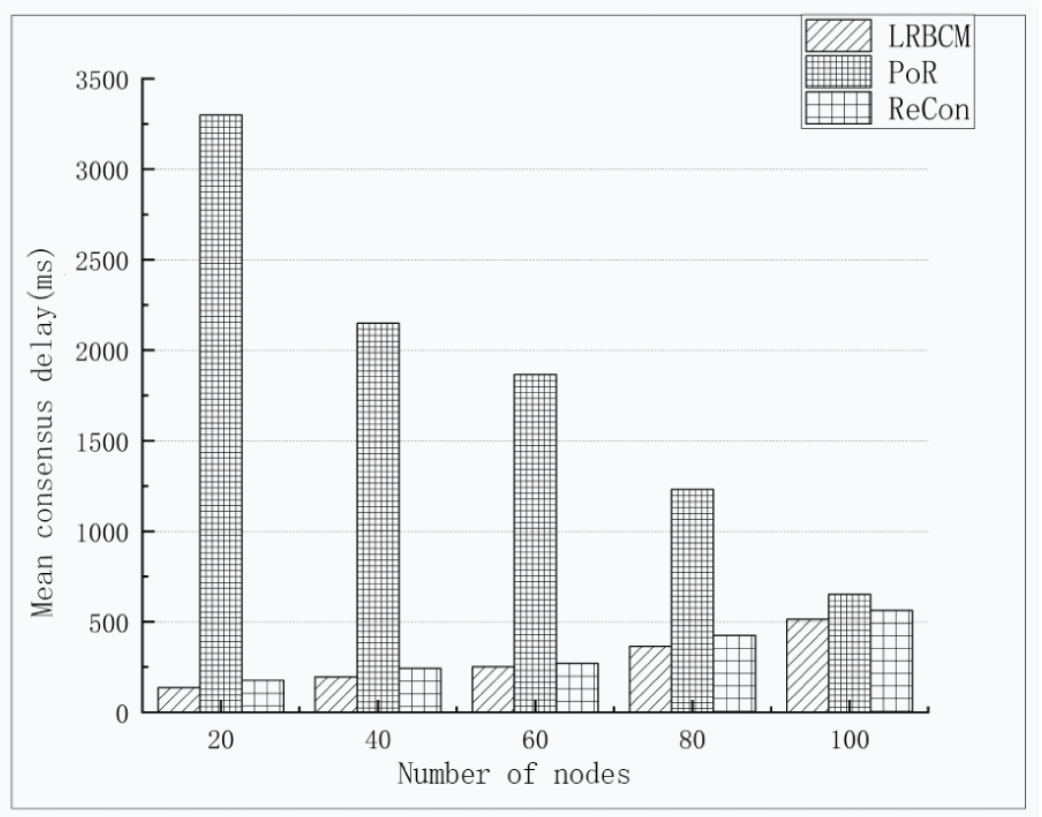


Table 5. Available queries and their explanations

Queries	Explanations
Execute $\left(\ddot{}^{c_1}_{SN_1}, \ddot{}^{c_2}_{SN_2}\right)$	Opponent A uses this query to eavesdrop on communication messages between SN_1 and
CorruptSD $\left(\ddot{}^{c}_{SN_1}\right)$	Opponent A can obtain all pre stored private vouchers in any damaged industrial internet of things device SN through this query
Reveal $\left(\ddot{}^{c}\right)$	Opponent A uses this query to obtain the shared session key between IoT devices
Test $\left(\ddot{}^{c}\right)$	Opponent A uses this query to verify whether the session key between SN_1 and SN_2 is an original key or a random key

$$Adv_A^{ELAS}(t_p) = \left|2Adv_{A,Game_i}^{ELAS} - 1\right| \tag{8}$$

(2) $Game_1^A$: In this game, the adversary A launches an eavesdropping attack by running the Execute query and the Test query. The result of the Test query determines whether the adversary A extracts the original key or some random keys from the Reveal query. The adversary A intercepts the messages Msg_{D2D_1} `

$\mathrm{Msg}_{\mathrm{D2D}_2}$ and $\mathrm{Msg}_{\mathrm{D2D}_3}$ during the D2D authentication phase by executing the Execute query. The session key between two industrial IoT devices "SN_1" and "SN_2" is derived as $\mathrm{SK}_{\mathrm{S1S2}} = \mathrm{x}_{\mathrm{S1}} \cdot \mathrm{Y}_{\mathrm{S2}} = \mathrm{SK}_{\mathrm{S2S1}} = \mathrm{y}_{\mathrm{S}_2} \cdot \mathrm{X}_{\mathrm{S}_1}$, where $\mathrm{Y}_{\mathrm{S}_2} = \mathrm{y}_{\mathrm{S}_2} \cdot \mathrm{G}$, $\mathrm{y}_{\mathrm{S}_2} = \mathrm{H}\left(\mathrm{RID}_{\mathrm{S2}} \parallel \mathrm{TID}_{\mathrm{S2}} \parallel \mathrm{TC}_{\mathrm{S2}} \parallel \mathrm{pr}_{\mathrm{S2}} \parallel \mathrm{TS}_{\mathrm{S3}} \parallel \mathrm{r}_{\mathrm{S2}}\right)$, $\mathrm{X}_{\mathrm{S}_1} = \mathrm{x}_{\mathrm{S}_1} \cdot \mathrm{G}$, $\mathrm{x}_{\mathrm{S}_1} = \mathrm{H}\left(\mathrm{RID}_{\mathrm{S1}} \parallel \mathrm{TID}_{\mathrm{S1}} \parallel \mathrm{TC}_{\mathrm{S1}} \parallel \mathrm{pr}_{\mathrm{S1}} \parallel \mathrm{TS}_{\mathrm{S1}} \parallel \mathrm{r}_{\mathrm{S1}}\right)$. The session key depends on short-term secrets $\left(\mathrm{r}_{\mathrm{S1}}, \mathrm{r}_{\mathrm{S2}}\right)$ and long-term secrets $\left(\mathrm{RID}_{\mathrm{S1}}, \mathrm{RID}_{\mathrm{S2}}, \mathrm{TC}_{\mathrm{S1}}, \mathrm{TC}_{\mathrm{S2}}, \mathrm{pr}_{\mathrm{S1}}, \mathrm{pr}_{\mathrm{S2}}\right)$. To enhance security, a one-way collision-resistant hash function $\mathrm{H}(.)$ is used to protect the secret parameters. This indicates that the success rate of the adversary A cannot be simply improved by capturing the session key $\mathrm{SK}_{\mathrm{S1S2}} \left(= \mathrm{SK}_{\mathrm{S2S1}}\right)$. Thus, $\mathrm{Game}_0^{\mathrm{A}}$ and $\mathrm{Game}_1^{\mathrm{A}}$ are indistinguishable under eavesdropping attacks, leading to Equation (9).

$$Adv_{A,Game_0}^{ELAS} = Adv_{A,Game_1}^{ELAS} \tag{9}$$

(3) $\mathrm{Game}_2^{\mathrm{A}}$: In this game, the adversary A launches a proactive attack by simulating hash queries and performing ECDDHP computations. In the D2D authentication phase, the session key is derived by SN_1 as $\mathrm{SK}_{\mathrm{S2S1}} = \mathrm{y}_{\mathrm{S}_2} \cdot \mathrm{X}_{\mathrm{S}_1}$ and by SN_2 as $\mathrm{SK}_{\mathrm{S1S2}} = \mathrm{x}_{\mathrm{S1}} \cdot \mathrm{Y}_{\mathrm{S2}}$. The adversary A can obtain $\mathrm{X}_{\mathrm{S}_1}$, Y_{S2} from $\mathrm{Msg}_{\mathrm{D2D}_1}$, $\mathrm{Msg}_{\mathrm{D2D}_2}$ during the transmission process. To derive the session key, the adversary A needs to solve the ECDDHP problem to calculate the private $\mathrm{X}_{\mathrm{S}_1}$, Y_{S2} based on unknown secrets ($\mathrm{r}_{\mathrm{S1}}, \mathrm{r}_{\mathrm{S2}}$). Then, it needs to simulate hash queries to compute $\mathrm{x}_{\mathrm{S}_1}$, $\mathrm{y}_{\mathrm{S}_2}$, but the private $\mathrm{x}_{\mathrm{S}_1}$, $\mathrm{y}_{\mathrm{S}_2}$ are also protected by the one-way collision-resistant hash function $\mathrm{H}(.)$. Thus, in the D2D authentication phase, the adversary A can derive the session key only when it can solve both the hash queries and the ECDDHP problem simultaneously. By excluding the simulation of hash queries and ECDDHP computations in $\mathrm{Game}_2^{\mathrm{A}}$, $\mathrm{Game}_1^{\mathrm{A}}$ and $\mathrm{Game}_2^{\mathrm{A}}$ become indistinguishable. The relation is derived as Equation (10).

$$\left|Adv_{A,Game_1}^{ELAS} - Adv_{A,Game_2}^{ELAS}\right| \le \frac{q_h^2}{2\left|Hash\right|} + Adv_A^{ECDDHP}(t_p) \tag{10}$$

The adversary A has executed all the previous queries except for guessing the random point to win $\mathrm{Game}_2^{\mathrm{A}}$, resulting in AdvA, Game 2ELAS=0.5. Utilizing the triangle inequality, Equations (7), (8), and (9) are derived as Equation (10). Finally, by multiplying both sides by two, we obtain the final result as Equation (11).

$$\frac{1}{2}Adv_A^{ELAS}(t_p) = \left|Adv_{A,Game_0}^{ELAS} - \frac{1}{2}\right| = \left|Adv_{A,Game_1}^{ELAS} - Adv_{A,Game_2}^{ELAS}\right| \le \frac{q_h^2}{2\left|Hash\right|} + Adv_A^{ECDDHP}(t_p) \tag{11}$$

Finally, by multiplying both sides by 2, we obtain the final result of Equation (12):

$$Adv_A^{ELAS}(t_p) \leq \frac{q_h^2}{|Hash|} + 2Adv_A^{ECDDHP}(t_p) \quad (12)$$

Using the AVISPA tool for formal security verification, a non-mathematical security analysis demonstrates that ELAM can withstand some known attacks. The experimental results are presented the Figure 15.

(1) Replay Attack: Assuming an adversary, such as A, intercepts messages Msg_{D2D_1}, Msg_{D2D_2} and Msg_{D2D_3} during the $D2D$ authentication phase. It is evident that each message includes a timestamp or a random secret or both. Each receiver validates these values before processing. If the timestamp is not validated, the receiver discards the received message without any further processing. This prevents A from replaying previous messages, indicating that ELAM is resilient against replay attacks.

(2) Man-in-the-Middle Attack: Suppose adversary A intercepts the information exchanged during the authentication phase, i.e., Msg_{D2D_1}, Msg_{D2D_2} and Msg_{D2D_3}, and attempts to forward them to the intended recipients after tampering with the message content. In the $D2D$ authentication phase, Sig_{S1} employs the private credential r_{S1} based on SN_1 and x_{S_1}, which is recorded on the blockchain ledger and hence cannot be tampered with. Similarly, Sig_{S2} uses the private credential r_{S2} based on SN_2 and y_{S_2}, also recorded on the blockchain ledger. Consequently, the proposed ELAM architecture demonstrates resilience against "man-in-the-middle" attacks.

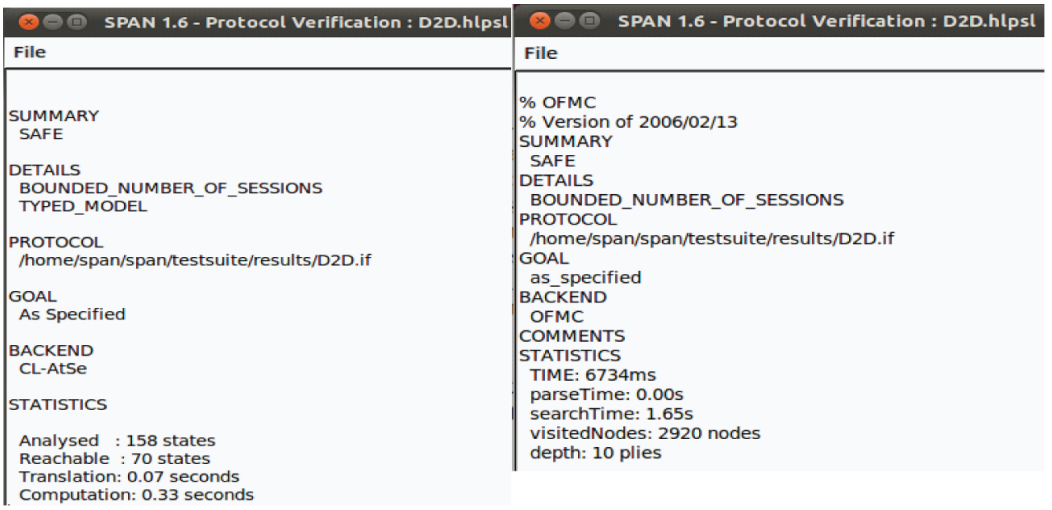
(3) Denial of Service (DoS) Attack: Using the current timestamp in each exchanged message ensures that multiple messages from an adversary can be easily detected by checking the receiver's timestamp, and such messages will not be further processed. Therefore, the resources utilized by the entity cannot be consumed by the adversary because the computation is based on lightweight cryptographic operations such as hashing and ECC point addition/multiplication. Hence, ELAM is resilient against DoS attacks.

(4) Anonymity and Untraceability: During the D2D authentication phase, the messages exchanged between two industrial internet of things devices, SN_1 and SN_2, are Msg_{D2D_1}, Msg_{D2D_2} and Msg_{D2D_3}. All messages use only temporal identities, not the actual or pseudo identities of SN. Moreover, due to their unique and random components, these messages are distinct. Therefore, adversaries cannot identify or trace the entities participating in communication during consecutive sessions. Hence, in ELAM, both anonymity and untraceability are preserved.

5. CONCLUSION

Compared to other methods, LRBCM consistently outperforms with approximately 10.78% higher throughput and about 12.79% lower consensus latency than ReCon. ELAM demonstrates increasing throughput over time, surpassing DLBA-IoT and S-LoRaWAN. During peak operation, ELAM achieves about 11.35% higher throughput than S-LoRaWAN, and an average latency about 7.83% lower than DLBA-IoT, highlighting its efficiency in reducing authentication delays. Security analysis confirms ELAM's resilience to known attacks, ensuring secure authentication for industrial internet of things (IIoT) devices. While security analysis has been conducted on ELAM, unknown attack vectors may exist in practical applications. LRBCM and ELAM's resistance to emerging network threats requires continuous updates and validation. The integration effectiveness of LRBCM and ELAM in

Figure 15. Safety simulation results



large-scale manufacturing networks warrants further research. In summary, our implementation of LRBCM and ELAM significantly advances IIoT device authentication, enhancing performance and ensuring the security, reliability, and energy efficiency of IIoT applications across various industries. Our research lays the foundation for future improvements in consensus efficiency, strengthened data security, and exploration of efficient cross-domain identity authentication solutions to meet the evolving security needs of the industrial internet of things sector.

AUTHOR CONTRIBUTIONS

Conceptualization, Mingrui zhao; Data curation, Formal analysis, Chunjing Shi; Investigation, Mingrui zhao; Methodology, Mingrui zhao; Resources, Mingrui zhao; Software, Yixiao Yuan, Mingrui zhao, and Chunjing Shi; Supervision, Chunjing Shi, Yixiao Yuan; Validation, Chunjing Shi; Visualization, Chunjing Shi; Writing – review & editing, Mingrui zhao.

FUNDING

This research was funded by the Basic Scientific Research Project of Colleges and Universities from the Educational Department of Liaoning Province (LJKZ0258) and; the Liaoning Doctor Scientific Research Initial Fund from the Department of Science & Technology of Liaoning Province (2022-BS-187).

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Abdi, G. H., Sheikhani, A. H. R., Kordrostami, S., Ghane, A., & Babaie, S. (2023). A novel selfish node detection based on reputation and game theory in internet of things. *Computing*. Advance online publication. doi:10.1007/s00607-023-01184-8

Biryukov, A., & Feher, D. (2020). ReCon: Sybil-resistant consensus from reputation. *Pervasive and Mobile Computing*, *61*, 101109. doi:10.1016/j.pmcj.2019.101109

Chen, P., Han, D., Weng, T. H., Li, K.-C., & Castiglione, A. (2021). A novel Byzantine fault tolerance consensus for green IoT with intelligence based on reinforcement. *Journal of Information Security and Applications*, *59*, 102821. doi:10.1016/j.jisa.2021.102821

Dakhnovich, A. D., Moskvin, D. A., & Ivanov, D. V. (2020). A technique for safely transforming the infrastructure of industrial control systems to the industrial internet of things. *Automatic Control and Computer Sciences*, *54*(8), 841–849. doi:10.3103/S0146411620080106

Danish, S. M., Lestas, M., Qureshi, H. K., Zhang, K., Asif, W., & Rajarajan, M. (2020). Securing the LoRaWAN join procedure using blockchains. *Cluster Computing*, *23*(3), 2123–2138. doi:10.1007/s10586-020-03064-8

Devi, S., & Bharti, T. S. (2022). A review on detection and mitigation analysis of distributed denial of service attacks and their effects on the cloud. *International Journal of Cloud Applications and Computing*, *12*(1), 1–21. doi:10.4018/IJCAC.311036

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Tauber, M. G., Schmittner, C., & Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. *IEEE Internet of Things Journal*, *6*(1), 288–296. doi:10.1109/JIOT.2017.2737630

Feng, Y., Wang, X. (2022). Data privacy protection scheme of industrial internet of things based on elliptic curve encryption algorithm. *Intelligent Computer and Application, 12*(12), 110-113+121. 10.1109/JIOT.2021.3128528

Fu, X., Wang, H., Shi, P., Ma, X., & Zhang, X. (2022). Teegraph: Trusted execution environment and directed acyclic graph-based consensus algorithm for IoT blockchains. *Science China. Information Sciences*, *65*(3), 1–3. doi:10.1007/s11432-019-1516-3

Gaurav, A., Gupta, B. B., & Panigrahi, P. K. (2023). A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. *Enterprise Information Systems*, *17*(3), 2023764. doi:10.1080/17517575.2021.2023764

Gupta, B. B., Li, K. C., & Leung, V. C. M. (2021). Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. *IEEE/CAA Journal of Automatica Sinica, 8*(12), 1877-1890. 10.1371/journal.pone.0279429

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 82721–82743. doi:10.1109/ACCESS.2019.2924045

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*, *23*(3), 239–252. doi:10.1007/s10676-020-09563-x PMID:33281497

Jia, D., Yang, G., Huang, M., Xin, J., Wang, G., & Yuan, G. Y. (2023). An efficient privacy-preserving blockchain storage method for internet of things environment. *World Wide Web (Bussum)*, *26*(5), 2709–2726. doi:10.1007/s11280-023-01172-0 PMID:37361140

Khalid, U., Asim, M., Baker, T., Hung, P. C. K., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), 2067–2087. doi:10.1007/s10586-020-03058-6

Ling, Z., & Hao, Z. J. (2022a). An intrusion detection system based on normalized mutual information antibodies feature selection and adaptive quantum artificial immune system. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–25. doi:10.4018/IJSWIS.308469

Ling, Z., & Hao, Z. J. (2022b). Intrusion detection using normalized mutual information feature selection and parallel quantum genetic algorithm. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–24. doi:10.4018/IJSWIS.307324

Liu, T., Yuan, Y., & Yu, Z. (2021). The service architecture of internet of things terminal connection based on blockchain technology. *The Journal of Supercomputing*, *77*(11), 12690–12710. doi:10.1007/s11227-021-03774-9

Lloret, J., & Parra, L. (2023). Industrial internet of things. *Mobile Networks and Applications*, *28*(1), 1–3. doi:10.1007/s11036-022-02014-5

Lu, J., Shen, J., Vijayakumar, P., & Gupta, B. B. (2021). Blockchain-based secure data storage protocol for sensors in the industrial internet of things. *IEEE Transactions on Industrial Informatics*, *18*(8), 5422–5431. doi:10.1109/TII.2021.3112601

Mishra, A., Joshi, B. K., Arya, V., Gupta, A. K., & Chui, K. T. (2022). Detection of distributed denial of service (DDoS) attacks using computational intelligence and majority vote-based ensemble approach. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–10. doi:10.4018/IJSSCI.309707

Mohammadipanah, F., & Sajedi, H. (2021). Potential of blockchain approach on development and security of microbial databases. *Biological Procedures Online*, *23*(1), 3. doi:10.1186/s12575-020-00139-z PMID:33517878

Mukherjee, S., & Biswas, G. P. (2018). Networking for IoT and applications using existing communication technology. *Egyptian Informatics Journal*, *19*(2), 107–127. doi:10.1016/j.eij.2017.11.002

Nashwan, S. (2021). AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. *Egyptian Informatics Journal*, *22*(1), 15–26. doi:10.1016/j.eij.2020.02.005

Nguyen, G. N., Le Viet, N. H., & Elhoseny, M. (2021). Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of Parallel and Distributed Computing*, *153*, 150–160. doi:10.1016/j.jpdc.2021.03.011

Pan, Q., Wu, J., Bashir, A. K., Li, J., Vashisht, S., & Nawaz, R. (2022). Blockchain and AI enabled configurable reflection resource allocation for IRS-aided coexisting drone-terrestrial networks. *IEEE Wireless Communications*, *29*(6), 46–54. doi:10.1109/MWC.001.2200099

Raj, A., & Prakash, S. (2022). A privacy-preserving authentic healthcare monitoring system using blockchain. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–23. doi:10.4018/IJSSCI.310942

Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, *77*(2), 1114–1151. doi:10.1007/s11227-020-03318-7

Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, *149*, 102481. doi:10.1016/j.jnca.2019.102481

Sharma, R., & Sharma, N. (2022). Attacks on resource-constrained IoT devices and security solutions. *International Journal of Software Science and Computational Intelligence*, *14*(1), 1–21. doi:10.4018/IJSSCI.310943

Shen, C. (2022). Overview of research on blockchain cross-chain technology. *Journal of Internet of Things*, *6*(04), 183–196. doi:10.11959/j.issn.2096-3750.2022.00301

Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-assisted secure device authentication for cross-domain industrial IoT. *IEEE Journal on Selected Areas in Communications*, *38*(5), 942–954. doi:10.1109/JSAC.2020.2980916

Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–43. doi:10.4018/IJSWIS.297143

Sisinni, E., Saifullah, A., Han, S., Jennehag, U., & Gidlund, M. (2018). Industrial internet of things: Challenges, opportunities, and directions. *IEEE Transactions on Industrial Informatics*, *14*(11), 4724–4734. doi:10.1109/TII.2018.2852491

Sober, M., Scaffino, G., Schulte, S., & Kanhere, S. S. (2023). A blockchain-based IoT data marketplace. *Cluster Computing*, *26*(6), 3523–3545. doi:10.1007/s10586-022-03745-6

Stergiou, C. L., Psannis, K. E., & Gupta, B. B. (2021). InFeMo: Flexible big data management through a federated cloud system. *ACM Transactions on Internet Technology*, *22*(2), 1–22. doi:10.1145/3426972

Tembhurne, J. V., Almin, M. M., & Diwan, T. (2022). Mc-DNN: Fake news detection using multi-channel deep neural networks. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–20. doi:10.4018/IJSWIS.295553

Wan, J., Li, J., Imran, M., Li, D., & Fazal-e-Amin, . (2019). A blockchain-based solution for enhancing security and privacy in smart factory. *IEEE Transactions on Industrial Informatics*, *15*(6), 3652–3660. doi:10.1109/TII.2019.2894573

Wang, J., Wu, L., Choo, K. K. R., & He, D. (2019a). Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Transactions on Industrial Informatics*, *16*(3), 1984–1992. doi:10.1109/TII.2019.2936278

Wang, T., Pan, Z., Hu, G., Duan, Y., & Pan, Y. (2022b). Understanding universal adversarial attack and defense on graph. *International Journal on Semantic Web and Information Systems*, *18*(1), 1–21. doi:10.4018/IJSWIS.308812

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019b). Survey on blockchain for internet of things. *Computer Communications*, *136*, 10–29. doi:10.1016/j.comcom.2019.01.006

Wang, Y., Chen, L., & Zhong, M. (2022a). Research progress of blockchain scheme based on zero-knowledge proof. *Netinfo Security*, *22*(12), 47–56. doi:10.1155/2022/3186112

Xiong, H., Wu, Y., Jin, C., & Kumari, S. (2020). Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT. *IEEE Internet of Things Journal*, *7*(12), 11713–11724. doi:10.1109/JIOT.2020.2999510

Xu, Z., He, D., & Vijayakumar, P. (2021). Certificateless public auditing scheme with data privacy and dynamics in group user model of cloud-assisted medical WSNs. *IEEE Journal of Biomedical and Health Informatics*. Advance online publication. doi:10.1109/JBHI.2021.3128775 PMID:34788225

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal*, *4*(5), 1250–1258. doi:10.1109/JIOT.2017.2694844

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. M. (2018). Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet of Things Journal*, *6*(2), 1495–1505. doi:10.1109/JIOT.2018.2836144

Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., & Ning, H. (2021). Security and privacy issues of physical objects in the IoT: Challenges and opportunities. *Digital Communications and Networks*, *7*(3), 373–384. doi:10.1016/j.dcan.2020.09.001

Yuan, X., Luo, F., Haider, M. Z., Chen, Z., & Li, Y. (2021). Efficient Byzantine consensus mechanism based on reputation in IoT blockchain. *Wireless Communications and Mobile Computing*, *9952218*, 1–14. Advance online publication. doi:10.1155/2021/9952218

Zafar, S., Bhatti, K. M., Shabbir, M., Hashmat, F., & Akbar, A. H. (2022). Integration of blockchain and internet of things: Challenges and solutions. *Annales des Télécommunications*, *77*(1-2), 13–32. doi:10.1007/s12243-021-00858-8

Zhang, J., Huang, Y., Ye, F., & Yang, Y. (2021). A novel proof-of-reputation consensus for storage allocation in edge blockchain systems. *IEEE/ACM 29th International Symposium on Quality of Service (IWQOS)*. doi:10.1109/IWQOS52092.2021.9521348

Zhang, Q., Guo, Z., Zhu, Y., Vijayakumar, P., Castiglione, A., & Gupta, B. B. (2023). A deep learning-based fast fake news detection model for cyber-physical social services. *Pattern Recognition Letters*, *168*, 31–38. doi:10.1016/j.patrec.2023.02.026

Zhuang, Q., Liu, Y., & Chen, L. (2019). Proof of reputation: A reputation-based consensus protocol for blockchain based systems. *Proceedings of the 2019 International Electronics Communication Conference*. doi:10.1145/3343147.3343169

Mingrui Zhao is a graduate student at Shenyang University of Technology, specializing in mechanical manufacturing and automation. Focused on research in artificial intelligence and computer vision, I have published several journal articles and actively participated in provincial and national research projects.

Chunjing Shi's fields of workshop production management, networked manufacturing technologies, and enterprise information systems and modeling. With an extensive research background, Chunjing Shi has led or participated in over 10 projects, including national-level initiatives. He has also authored more than 10 academic papers published in both domestic and international journals and conferences. Additionally, Chunjing Shi has contributed to the academic community by co-authoring two textbooks.

Yixiao Yuan is a Ph.D. candidate at Northeastern University and specializes in several research areas, including the optimization of microgrid operations, mechanical manufacturing and automation, hydraulic transmission, and control systems, as well as automation control. Yuan Yixiao has made significant contributions to the field with multiple journal publications and articles, alongside holding two invention patents. Furthermore, Yuan Yixiao actively participates in various provincial and national-level research projects.