future internet

MDPI

Article

A Lightweight Authentication Method for Industrial Internet of Things Based on Blockchain and Chebyshev Chaotic Maps

Zhonghao Zhai [1], Junyi Liu [1], Xinying Liu [1], Yanqin Mao [2], Xinjun Zhang [3], Jialin Ma [1] and Chunhua Jin [1,*]

[1] Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huai'an 223025, China; zhonghaozhai@hyit.edu.cn (Z.Z.); junyill@yeah.net (J.L.); lxyjjy@yeah.net (X.L.)
[2] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210049, China
[3] School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210049, China
* Correspondence: 2017070256@njupt.edu.cn

Abstract

The Industrial Internet of Things (IIoT), a key enabler of Industry 4.0, integrates advanced communication technologies with the industrial economy to enable intelligent manufacturing and interconnected systems. Secure and reliable identity authentication in the IIoT becomes essential as connectivity expands across devices, systems, and domains. Blockchain technology presents a promising solution due to its decentralized, tamper-resistant, and traceable characteristics, facilitating secure and transparent identity verification. However, current blockchain-based cross-domain authentication schemes often lack a lightweight design, rendering them unsuitable for latency-sensitive and resource-constrained industrial environments. This paper proposes a lightweight cross-domain authentication scheme that combines blockchain with Chebyshev chaotic mapping. Unlike existing schemes relying heavily on Elliptic Curve Cryptography or bilinear pairing, our design circumvents such computationally intensive primitives entirely through the algebraic structure of Chebyshev polynomials. A formal security analysis using the Real-Or-Random (ROR) model demonstrates the scheme's robustness. Furthermore, performance evaluations conducted with Hyperledger Fabric and the MIRACL cryptographic library validate the method's effectiveness and superiority over existing approaches in terms of both security and operational efficiency.

Keywords: Industrial Internet of Things; authentication; blockchain; Chebyshev chaotic maps

check for updates

Academic Editor: Paulo Ferreira

Received: 22 May 2025
Revised: 14 July 2025
Accepted: 22 July 2025
Published: 28 July 2025

Citation: Zhai, Z.; Liu, J.; Liu, X.; Mao, Y.; Zhang, X.; Ma, J.; Jin, C. A Lightweight Authentication Method for Industrial Internet of Things Based on Blockchain and Chebyshev Chaotic Maps. *Future Internet* **2025**, *17*, 338. https://doi.org/10.3390/fi17080338

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Industrial Internet of Things (IIoT) is an innovative infrastructure and ecosystem that combines new-generation communication technologies with the industrial economy [1]. It is a key enabler of Industry 4.0. Based on networks, with platforms at the core and data and security as key elements, the IIoT connects people, machines, objects, and systems. This enables the manufacturing sector to expand its industrial chain and create interconnectivity across devices, systems, factories, and regions. As a result, it boosts industrial productivity and drives the intelligent transformation of the manufacturing service system. Integrating the IIoT with manufacturing leads to intelligent production, networked collaboration, mass customization, and service extension upgrades. This shifts manufacturing from isolated models to more collaborative systems. As reported by MarketsandMarkets, the IIoT sector is expected to expand from USD 194.4 billion in 2024 to USD 286.3 billion by 2029, reflecting a compound annual growth rate (CAGR) of 8.1% [2].

In the collaborative process of the IIoT, ensuring the trusted identity of devices is crucial [3]. Malicious devices can fake their identity to join the collaboration, steal sensitive data, or disrupt tasks. Without a unified identity authentication mechanism, devices cannot establish mutual trust, which prevents effective collaboration across the domains. Currently, networks in different management domains face identity isolation. They use separate identity management systems, with inconsistent standards for identity formats and authentication policies. This makes it difficult for devices to exchange and verify credentials across domains. As a result, trust cannot be easily established, leading to significant identity fragmentation. In IIoT, devices often interact across different management domains, making secure cross-domain authentication essential. Traditional centralized methods face challenges such as single points of failure, poor scalability, and limited trust interoperability [3]. To address this, a distributed identity authentication mechanism across management domains is needed. This will enable trusted authentication and identity management for cross-domain devices, allowing seamless collaboration between networks [4].

The decentralized, tamper-resistant, and traceable characteristics of blockchain make it particularly suitable for identity authentication in cross-domain collaboration within the IIoT [5]. It enables secure, transparent, and efficient authentication while addressing trust and efficiency issues in traditional authentication methods. Blockchain's decentralization allows different administrative domains to reach consensus on a unified identity authentication mechanism without relying on a single centralized certification authority. This enables cross-domain identity information sharing and authentication. Its tamper-resistant property ensures that once identity information is recorded on-chain during cross-domain collaboration, it cannot be maliciously altered, thus guaranteeing the integrity and authenticity of the shared identity data. The traceability feature of blockchain enables the recording of all authentication operations in chronological order, allowing identity verification and access history to be traced at any time. This is particularly important for multi-party collaboration and security auditing. In addition, using smart contracts in blockchain technology can automate identity authentication processes, thereby reducing the complexity and cost of manual verification and improving collaboration efficiency.

However, existing blockchain-based cross-domain identity authentication schemes in IIoT scenarios lack a sufficient lightweight design. Industrial environments often have stringent latency constraints, with some time-critical applications requiring end-to-end delays in 10 to 100 milliseconds. Current blockchain-based cross-domain identity authentication schemes are mainly categorized into three types: authentication based on blockchain and Public Key Infrastructure (PKI) [6–17], authentication based on blockchain and Identity-Based Authentication (IBA) [18–27], and authentication based on blockchain and Certificateless Public Key Cryptography (CL-PKC) [28–34]. The hierarchical structure of most blockchain-based PKI schemes still poses a challenge. It increases interaction overhead during authentication and indirectly raises latency [7,12,14–17]. Moreover, most existing blockchain-based PKI schemes [7–17] rely on computationally intensive operations such as RSA exponentiation, bilinear pairings, and elliptic curve point multiplications. In addition, most blockchain-based IBA [18–27] and blockchain-based CL-PKC schemes [28–34] have the inherent privacy risk of using a user's identity as their public key. While their design eliminates the need for digital certificates, it also exposes identity-related information. Once written to the immutable blockchain ledger, such data becomes vulnerable to linkage attacks and long-term privacy compromises. To address these risks, researchers have proposed various privacy-preserving techniques. These include cryptographic obfuscation [19] and zero-knowledge proofs [20,21,32,34]. However, implementing these mechanisms often introduces significant computational overhead and increased protocol complexity. This is particularly problematic in resource-constrained environments such as IIoT. As a result,

while blockchain helps alleviate the trust and key escrow issues in traditional IBA by removing the need for a centralized KGC, it simultaneously necessitates more sophisticated and costly mechanisms to preserve user privacy.

To address this issue, this paper presents an efficient and lightweight cross-domain authentication scheme that integrates blockchain technology with Chebyshev chaotic mapping. By leveraging blockchain technology to achieve the trusted sharing of device identity information, the scheme significantly reduces the number of interactions required during cross-domain authentication. It simplifies the identity verification process for industrial devices. Furthermore, it employs the semigroup property of Chebyshev polynomials to construct session keys, effectively reducing the authentication process's computational complexity and enhancing the system's overall efficiency and security. Our scheme also assigns IoT devices pseudonyms that are periodically generated using Chebyshev chaotic maps, effectively mitigating traceability risks during cross-domain operations and preserving device privacy. To summarize, our contributions are the following:

- To address the complexity and single point of failure associated with third-party-dependent cross-domain identity authentication in traditional IIoT systems, we propose a blockchain-based cross-domain authentication scheme tailored for the IIoT. By integrating edge computing, the scheme effectively reduces the number of interactions and latency during device authentication.
- To reduce the high overhead and latency of existing blockchain-based authentication methods unsuitable for constrained devices, we propose a lightweight authentication method using Chebyshev chaotic maps and blockchain, significantly lowering computational cost and delay.
- We conduct a formal security analysis of the proposed method using the Real-Or-Random (ROR) model, demonstrating its security. Furthermore, we implement simulations using Hyperledger Fabric [35] and the MIRACL cryptographic library [36] to evaluate the performance of our scheme. Comparative analysis with related work confirms the superiority of our proposed method.

The remainder of this paper is structured as follows: Section 2 surveys the related literature. Section 3 covers the foundational concepts relevant to our scheme. In Section 4, we describe the system architecture. Section 5 defines the security objectives. Section 6 presents the proposed authentication protocol in detail. A thorough security evaluation is conducted in Section 7. Section 8 compares the computational and communication overhead of our method with existing solutions. Lastly, Section 9 summarizes the conclusions of this work.

2. Related Work

Given the advantages stated in the Section 1, many researchers and enterprises have begun researching the use of blockchain for cross-domain authentication and generating reliable cross-domain authentication without needing trusted third parties.

Existing blockchain-based cross-domain authentication schemes can be broadly categorized into three types: authentication based on blockchain and Public Key Infrastructure (PKI), authentication based on blockchain and IBA, and authentication based on blockchain and Certificateless Public Key Cryptography (CL-PKC).

2.1. Cross-Domain Authentication Based on PKI and Blockchain

Although traditional Public Key Infrastructure (PKI) has played a pivotal role in digital identity authentication, its reliance on centralized Certificate Authorities (CAs) exposes it to a series of inherent weaknesses [6]. As the sole trust anchors, CAs represent single points of failure—once compromised, either by attack, mismanagement, or negligence,

the entire authentication system becomes vulnerable. Moreover, PKI implementations vary widely across organizations and platforms, making cross-domain identity authentication prone to issues such as certificate incompatibility, inconsistent trust anchor configurations, and mismatched key management protocols. These inconsistencies often result in failed authentications, insecure fallback mechanisms, or increased administrative burden. A common approach to addressing the above issue is to involve a third-party Certificate Authority (CA) to handle authentication in cross-domain communications. However, this solution poses practical challenges, as it may introduce security risks like collusion, lack of fairness, and vulnerability to single points of failure.

To address these structural limitations, growing research interest has turned to blockchain as a foundation for decentralized authentication architectures. Due to its immutable and consensus-driven design, blockchain can serve as a shared ledger for recording identity information, thereby reducing dependence on any single CA and mitigating the systemic risks of centralized trust. Guided by this idea, many researchers have proposed blockchain-based cross-domain authentication schemes. For example, Wang et al. [7] designed a consortium-based CA collaboration model using blockchain to eliminate isolated trust silos. Similarly, Zhang et al. [8] proposed the BCAE scheme, which replaces traditional CA-signed X.509 certificates with blockchain-based credentials, improving identity consistency and interoperability across domains. Tong et al. [9] proposed CCAP, a complete cross-domain authentication based on consortium blockchain for the Internet of Things. They introduce verification servers to form a consortium blockchain, assisting authentication servers (i.e., CAs) in enabling secure cross-domain authentication between IoT domains with different configurations. Cui et al. [10,11] utilized blockchain-based mechanisms maintained by edge servers to allow for mutual authentication without central CAs and combine smart contracts and dynamic accumulators to optimize communication and computation during the authentication process. Zhang et al. [12] introduced smart contracts in vehicular networks to manage certificate lifecycles autonomously, reducing the administrative workload and improving the responsiveness of revocation and renewal operations. Saleem et al. [13] presented a blockchain-based Public Key Infrastructure (PKI) framework named ProofChain. It aims to decentralize the CA pool and ensure compatibility with X.509 standards. Yang et al. [14] presented a blockchain-enhanced hybrid authentication framework for vehicular networks. In their scheme, Certificate Authorities (CAs) handle initial identity issuance, while blockchain supports cross-domain credential verification and pseudonym lifecycle management. The framework enables real-time coordination among CAs via blockchain.

However, despite these improvements, blockchain-based PKI systems also introduce new layers of complexity. First, existing consensus mechanisms (such as PoW (Proof of Work) [37], PoS (Proof of Stake) [38], or PBFT (Practical Byzantine Fault Tolerance) [39]) often bring significant computational and latency overhead, especially in high-frequency authentication scenarios. Second, blockchain's inherently transparent nature conflicts structurally with the need for privacy. Thirdly, blockchain's append-only nature leads to increased storage overhead. To solve these problems, Luo et al. [15] observed this bottleneck. They proposed a split-chain mechanism to accelerate write operations, though the trade-off between consistency and performance remains a challenge. Su et al. [16] employed decentralized oracles and zero-knowledge proofs to enable anonymous identity verification across heterogeneous domains, effectively preventing identity tracking. Likewise, Cui et al. [10,11] utilized pseudonym-based mechanisms distributed by edge servers to allow for mutual authentication. Tong et al. [9] proposed a complete cross-domain authentication based on consortium blockchain with a privacy protection scheme for the Internet of Things to preserve device privacy. Xue et al. [17] proposed integrating a blacklist Merkle

tree to support revocation while maintaining data integrity. However, this introduces additional computational and storage costs.

Although existing research has made notable progress in integrating blockchain with PKI, the hierarchical structure of PKI still poses a challenge. It increases interaction overhead during authentication and indirectly raises latency. Furthermore, few studies have explored optimizations of the computational and latency overhead from the perspective of cryptographic primitives employed in the authentication workflow. For example, related work [7,10–12,14,15,17] still relies heavily on traditional PKI mechanisms. In particular, the certificate-based signature verification in their scheme typically employs elliptic curve cryptography (ECC), which is computationally intensive for resource-constrained IIoT devices. Zhang et al. [8] claim lightweight key agreement, but the use of modular arithmetic over elliptic curves and multiple temporary key exchanges still results in resource-intensive cryptographic computations on the device side. Tong et al. [9] and Su et al. [16] rely on relatively complex cryptographic operations such as threshold cryptography, bilinear pairings, and non-interactive zero-knowledge proofs, which can impose significant computational overhead on the system.

We eliminate the complexity of traditional PKI hierarchical structures by leveraging blockchain as a decentralized and trusted authority for public key verification, thereby improving both authentication efficiency and system scalability. Moreover, most existing blockchain-based PKI schemes rely on computationally intensive operations such as RSA exponentiation, bilinear pairings, and elliptic curve point multiplications. To reduce this overhead, we propose an authentication scheme for IIoT based on Chebyshev chaotic maps. Chaotic-map-based authentication mechanisms have been proven to offer superior computational efficiency compared to conventional cryptographic techniques. According to [40–42], the Chebyshev polynomial computation operation takes one-third of the computational time of the ECC point multiplication operation.

2.2. Cross-domain authentication Based on IBA and Blockchain

Identity-Based Authentication (IBA) [18] is a method where a user's identity (e.g., email or username) serves as their public key, thereby eliminating the need for digital PKI certificates. In this approach, a trusted entity called the Key Generation Center (KGC) is responsible for generating the corresponding private keys of all users. During authentication, users demonstrate possession of their private keys by generating a valid cryptographic response, which can be verified by others using the public key derived from the user's identity. As a result, IBA significantly simplifies key management and reduces the overhead associated with certificate handling. Therefore, it is particularly suitable for distributed environments such as IoT and IIoT. However, since the KGC holds the power to generate any user's private key, IBA introduces potential key escrow and trust concerns.

To address these concerns, researchers have turned to blockchain technology, leveraging its decentralized, tamper-resistant architecture to reconstruct IBA frameworks without the need for a centralized KGC. For instance, Xiong et al. [19] proposed DIBRS-CE, a blockchain-based distributed identity-based ring signature scheme with identity abort, tailored for consumer electronics. Their design features a decentralized threshold identity-based ring signature protocol that removes reliance on a Key Generation Center (KGC). Zhang et al. [20] presented an identity-based data rights governance (IDRG) framework designed for blockchain-enabled, human-centric metaverse communication. By integrating blockchain technology with polynomial functions, their scheme supports access policies involving multiple users, thereby addressing the constraint of conventional identity-based encryption methods, which typically allow only single-user policies. Li et al. [21] presented a blockchain-assisted distributed identity-based signature scheme designed to enhance

security in resource-constrained IoT applications. By eliminating reliance on a centralized Key Generation Center (KGC), the scheme enables users to collaboratively generate master and signing keys through threshold protocols, addressing key escrow risks and single points of failure. Li et al. [22] introduced the Advanced Hierarchical Identity-Based Security Mechanism by Blockchain (AHISM-B) for Named Data Networking (NDN). Their approach leverages hierarchical identity-based cryptography to associate data names with public keys while utilizing blockchain to oversee public parameters, thereby mitigating the risk of single-point failures. Yang et al. [23] proposed an efficient identity-based aggregate signcryption scheme with blockchain (B-ID-ASC) for IoT-enabled maritime transportation systems (IMTSs). They design decentralized device authentication and tamper-proof transaction logging to replace centralized authorities, mitigating single-point failures. Suresh Babu et al. [24] introduced a decentralized Identity-Based Authentication framework for IoT devices, leveraging a permissioned blockchain. In their approach, the blockchain functions as a distributed Private Key Generator (PKG), effectively mitigating issues such as single points of failure and key escrow that are commonly associated with conventional Public Key Infrastructure (PKI) and IBA.

Despite these advancements, blockchain-based IBA systems are not without challenges. First of all, resource-constrained devices in IIoT may struggle with blockchain's computational and storage requirements, particularly when managing extensive data. To reduce computational overhead, Srivastava et al. [25] proposed a provably secure multivariate identity-based multi-signature scheme (MV-MSS) for the Internet of Vehicles (IoV) environment. The MV-MSS produces a single compact signature for multiple signers, reducing communication overhead. Zhang et al. [26] proposed two novel identity-based key agreement protocols tailored for the blockchain-powered intelligent edge. The first protocol ensures extended Canetti–Krawczyk (eCK) security, while the second protocol further achieves continuous after-the-fact leakage resilience (CAFL-eCK) security, resistant to side-channel attacks. Both protocols are lightweight and suitable for edge and end devices with limited computational resources. Li et al. [21] presented a blockchain-assisted distributed identity-based signature scheme for resource-constrained IoT applications. They propose a tree-based broadcasting strategy that reduces communication complexity from O (n^2) to O (nlogn), optimizing bandwidth efficiency for IoT devices. They further employ oblivious transfer protocols instead of homomorphic encryption for signature construction, achieving lightweight computational overhead without compromising security. To reduce storage overhead, Sharma et al. [27] proposed a blockchain-based IoT architecture for securing healthcare data using identity-based encryption (IBE). The system combines blockchain with Swarm off-chain storage to efficiently manage large-scale healthcare datasets. IBE secures data at rest, while Swarm enables decentralized data distribution, effectively addressing storage challenges. Second, privacy risks emerge from the immutable nature of blockchain, as identity or key-related metadata, once written to the ledger, may be susceptible to linkage attacks over time. Zhang et al. [20] proposed a privacy-preserving identity-based data rights governance scheme (IDRG) for blockchain-empowered human-centric metaverse communications. They protect user privacy by enabling encrypted identity-based data access policies that hide both policy content and size, ensuring data, identity, and policy privacy while supporting accountability and revocation via cryptographic techniques and blockchain.

Although prior studies have made notable progress in addressing the challenges introduced by integrating blockchain into IBA systems, several critical issues remain. One key concern is the inherent privacy risk of using a user's identity as their public key [22–27]. While this design eliminates the need for digital certificates, it also exposes identity-related information. Once written to the immutable blockchain ledger, such data

becomes vulnerable to linkage attacks and long-term privacy compromises. To address these risks, researchers have proposed various privacy-preserving techniques. These include cryptographic obfuscation [19] and zero-knowledge proofs [20,21]. However, implementing these mechanisms often introduces significant computational overhead and increased protocol complexity. This is particularly problematic in resource-constrained environments such as the Internet of Things (IoT) and Industrial Internet of Things (IIoT). As a result, while blockchain helps alleviate the trust and key escrow issues in traditional IBA by removing the need for a centralized KGC, it simultaneously necessitates more sophisticated and computationally intensive mechanisms to preserve user privacy.

Our scheme assigns IoT devices pseudonyms that are periodically generated using Chebyshev chaotic maps, effectively mitigating traceability risks during cross-domain operations and preserving device privacy. Furthermore, Chebyshev chaotic maps have demonstrated superior computational efficiency compared to traditional privacy-preserving techniques in most blockchain-based IBA frameworks.

2.3. Cross-Domain Authentication Based on CL-PKC and Blockchain

Certificateless Public Key Cryptography (CL-PKC) presents a compelling alternative to traditional PKI and identity-based encryption (IBE) by eliminating certificate management while preventing key escrow. In CL-PKC, a semi-trusted Key Generation Center (KGC) generates a partial private key based on the user's identity. This key is then combined with a user-chosen secret value to form a complete private key. Since the KGC lacks knowledge of this secret value, it cannot reconstruct the full private key, thereby mitigating the inherent trust risks associated with IBE. Additionally, CL-PKC-based authentication systems do not rely on digital certificates, reducing administrative complexity and improving scalability in large-scale distributed systems.

However, CL-PKC has its limitations. The partial trust assumption on the KGC still poses a security concern—particularly in adversarial or multi-domain environments. To overcome these shortcomings, researchers have explored a variety of blockchain-integrated CL-PKC frameworks that distribute trust and improve operational efficiency. For example, Yao et al. [28] introduced ECB-CLS, an authentication scheme for the automatic dependent surveillance broadcast (ADS-B) systems, combining blockchain and certificateless signatures to eliminate certificate management. It integrates blockchain for decentralized key management, mitigating single points of failure. Zhang et al. [29] developed an enhanced certificateless authentication and key agreement (CL-AKA) protocol based on blockchain technology in an Internet of Drones (IoD) environment. The protocol achieves resistance to key compromise impersonation attacks. Wang et al. [30] presented a revocable certificateless cross-domain authentication scheme leveraging a primary–secondary blockchain model. The scheme enhances cross-domain authentication efficiency and security by eliminating complex certificate management and mitigating centralized authority issues using the primary–secondary blockchain model. Feng et al. [31] proposed a cross-domain authentication method (CABC) that integrates blockchain with certificateless signatures for Industrial Internet of Things (IIoT) devices. CABC enables trusted authentication across different management domains (e.g., factories) and supports decentralized identity verification, thereby eliminating the reliance on trusted third parties and centralized servers. Wang et al. [32] proposed a blockchain-based certificateless conditional anonymous authentication scheme (BCCA) for the Industrial Internet of Things (IIoT). The BCCA enables traceability and user revocation with a chameleon hash algorithm for illegal information rectification on the evidence blockchain, aiming to mitigate security threats such as forgery, man-in-the-middle, and replay attacks. Dong et al. [33] developed a certificate-free, blockchain-enabled cross-domain authentication scheme tailored for the

Industrial Internet. Their method relies on an Ethereum consortium blockchain to serve as a trusted foundation across various regions. Within each region, industrial entities collaborate with a local Key Generation Center to produce users' private keys, thereby addressing the key escrow issue. Liu et al. [34] introduced a blockchain-assisted certificateless anonymous cross-domain authentication scheme for the Internet of Vehicles (IoVs). By leveraging blockchain, the approach minimizes redundant authentication overhead. The proposed scheme guarantees message integrity, supports traceability, and defends against multiple types of attacks.

Although existing research has made considerable progress in addressing the challenges introduced by integrating blockchain into CL-PKC systems, a fundamental issue remains. Similar to IBA, CL-PKC inherently uses the user's identity as part of the public key [28–34], which poses significant privacy risks. To mitigate these risks, additional privacy-preserving mechanisms are required. However, these measures inevitably introduce further computational overhead [32,34].

Likely, to enhance privacy and prevent traceability in cross-domain scenarios, our scheme uses Chebyshev chaotic maps to generate pseudonyms for IoT devices at regular intervals. This approach keeps device identities unlinkable over time and protects sensitive information. In addition, Chebyshev chaotic maps provide better computational efficiency than traditional methods like RSA, ECC, or bilinear pairing that are used in most blockchain-based CL-PKC methods.

3. Preliminaries

This section describes the prerequisite knowledge for the proposed work.

3.1. Blockchain

Blockchain is a distributed ledger composed of a sequence of blocks $B_0, B_1, \ldots, B_n$, where each block contains a set of validated transactions. A blockchain system can be formally modeled as a state-based transition system $M = (S, I, \delta, s_0)$, where the following are true:

- S is the set of global states. The global state refers to the complete and shared snapshot of all relevant data that defines the current status of the blockchain network. This includes information such as account balances, smart contract storage, and other protocol-defined data.
- I is the set of valid inputs (e.g., transactions, blocks).
- $\delta : S \times I \to S$ is the deterministic state transition function.
- $s_0 \in S$ is the initial state.

The evolution of the blockchain system is described by the following transition sequence:

$$s_0 \xrightarrow{i_0} s_1 \xrightarrow{i_1} s_2 \ldots \xrightarrow{i_{n-1}} s_n$$

Each state s_k may represent the current ledger view, set of valid transactions, and configuration of participating nodes. Consensus protocols determine how a new input i_k is selected and verified before applying δ.

A block B can be defined generically as

$$B = (header, T)$$

where $T = \{tx_1, tx_2, ..., tx_m\}$ is the set of transactions and the *header* contains metadata such as the previous block hash h_{prev} timestamp t and consensus-specific proof π. The validity of a block is determined by a predicate:

$$Valid(B, s) \Leftrightarrow Verify(T, s) \wedge ConsensusCheck(\pi, s)$$

This model accommodates various consensus mechanisms. For example, in PoW, $ConsensusCheck(\pi, s)$ verifies that the proof satisfies $h(B) < D$, where D is the difficulty target. In PBFT, it verifies a quorum of signed messages from validator nodes.

Blockchains can be broadly classified into public, private, consortium, and hybrid types. This classification is based on factors such as access permissions, governance models, and intended applications.

Public blockchains are open and permissionless. Anyone can join the network, read data, submit transactions, and participate in consensus. These networks are fully decentralized and trustless. Public blockchains are well-suited for open systems where transparency, immutability, and user autonomy are essential.

Private blockchains, also known as permissioned blockchains, restrict access to a single organization or a specific group. Only authorized users can validate transactions, access records, or operate nodes. These blockchains are often used in enterprise environments. They enhance data integrity, enable traceability, and support process automation, while keeping sensitive information private.

Consortium blockchains sit between public and private models. They are jointly managed by a group of predefined organizations, creating a decentralized but controlled network. Each member operates a node and takes part in the consensus process. This model is effective for sectors like finance, supply chain, and healthcare, where multiple parties need to share data without depending on a single authority.

Hybrid blockchains combine features of both public and private systems. They support selective transparency—some data can be public, while other parts remain private or permissioned. This approach offers both flexibility and scalability. It is suitable for use cases that require public verification along with controlled access, such as government services, enterprise systems, and IoT platforms.

In the context of the IIoT, consortium blockchains offer a robust solution for device authentication by enabling a decentralized yet collaboratively governed registry of devices. This approach reduces dependence on a single centralized Certificate Authority while maintaining control within a trusted group of stakeholders. Consortium blockchains enhance resistance to spoofing and unauthorized access and support secure, auditable interactions among industrial entities. By integrating this model, industrial systems can achieve higher levels of trust, traceability, and operational resilience that are essential for secure and efficient performance in interconnected industrial environments.

3.2. Extended Chebyshev Chaotic Maps

Definition 1 (Chebyshev Chaotic Maps)**.** *Let n be an integer, and $x \in [-1, 1]$, the Chebyshev polynomial, denoted by $T_n(x)$, maps the interval $[-1, 1]$ to itself and is defined as follows:*

$$T_n(x) = \cos(n \times \cos^{-1}(x))$$

The recurrence formula defining the Chebyshev polynomial is as follows:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$$

where $n \geq 2$, $T_0(x) = 1$, and $T_1(x) = x$.

Definition 2 (Semigroup Property)**.** *The Chebyshev polynomials are closed under the semigroup operation, which is given as*

$$T_a(T_b(x)) = \cos\left(a \times \cos^{-1}\left(\cos\left(b \times \cos^{-1}(x)\right)\right)\right) = \cos\left(ab \times \cos^{-1}(x)\right) = T_{ab}(x)$$

where a, b *are integers and* $x \in [-1, 1]$.

Chebyshev polynomials also satisfy the semigroup property over the entire real line $(-\infty, \infty)$. The extended form of the Chebyshev polynomial is expressed as

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \ mod \ p$$

where $x \in (-\infty, \infty)$ and p is a large prime number.

Definition 3 (Chaotic Maps Discrete Logarithm Problem—CMDLP)**.** *Given a Chebyshev polynomial and a real number* $x \in [-\infty, \infty]$*, the CMDLP states that it is computationally infeasible to determine the value* a *such that* $y = T_a(x)$*. In other words, the advantage of a probabilistic polynomial-time (PPT) adversary* A *in solving CMDLP within time* t *is defined as* $\mathrm{ADV}_A^{\mathrm{CMDLP}}(t) = \Pr\left[A(x, y) = a : a \in \mathbb{Z}_p^*, y = T_a(x) \bmod p\right]$*, which is negligible. That is,* $ADV_A^{CMDLP}(t)$ *of a PPT adversary* A *within a time bound* t*, to solve CMDLP, is negligible. That means* $ADV_A^{CMDLP}(t) \leq \epsilon$*, where* ϵ *denotes a negligible function.*

4. System Model

In the system model of our authentication method, there are four kinds of entities, as shown in Figure 1: *industrial device*, *edge gateway*, *blockchain anchor node*, and *consortium blockchain network*.

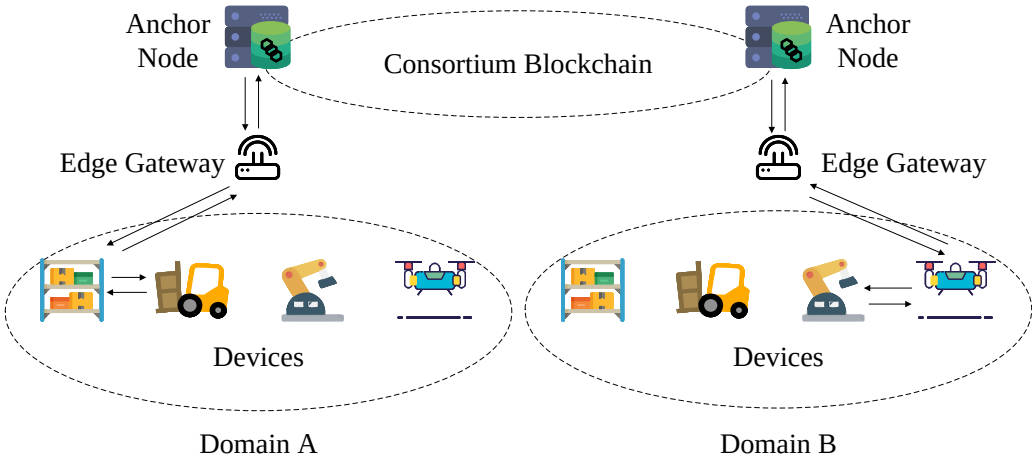


Figure 1. The system model of the proposed method.

- *Industrial devices* refer to smart machines, sensors, actuators, and control systems deployed within manufacturing or operational environments. Each device is uniquely identifiable and equipped with a digital identity. These devices typically possess limited computational resources and are often constrained in terms of connectivity. As such, they rely on nearby infrastructure, the edge gateways, for identity verification and secure network onboarding.
- *Edge gateways* act as intermediaries between industrial devices. Positioned close to the devices at the network edge, an edge gateway performs initial identity verification for devices within its administrative domain. It maintains local access control policies and authentication protocols. The edge gateway collaborates with blockchain anchor nodes in cross-domain scenarios to validate device identities from other domains.

- *Blockchain anchor nodes* are specialized entities participating directly in the consortium blockchain network. They are responsible for maintaining a synchronized ledger of authenticated device identities across different domains. Each anchor node represents a local domain or administrative zone and communicates with peer anchor nodes to exchange identity verification records. When a device seeks access in a foreign domain, the local edge gateway can query its associated anchor node, which in turn consults the blockchain to verify the authenticity of the device's identity as issued by another domain's anchor node. In the context of the Industrial Internet, a domain refers to a logical segment where devices, data, networks, applications, and services are managed in a distributed manner. The division of domains is typically based on functionality, geographic location, permissions, or management requirements. It aims to enhance the system's management efficiency, security, and controllability. The domain serves as a boundary for administrative tasks and resource management. Typically, different domains are independent of each other, especially the authentication service.
- *The consortium blockchain* network is a permissioned ledger infrastructure where only authorized anchor nodes are allowed to validate transactions and contribute to consensus. This network ensures decentralized trust and provides tamper-evident storage for device identity credentials. It supports smart contracts that encode identity registration, revocation, and cross-domain verification logic. The use of a consortium model balances scalability with security, avoiding the performance drawbacks of fully public chains while still achieving distributed consensus.

The authentication workflow is orchestrated through a multi-entity collaboration:

(1) Industrial devices request authentication from the local edge gateway.

(2) The edge gateway forwards the request to the anchor node for cross-domain verification.

(3) The anchor node queries the consortium blockchain network to check the validity of the device identity as registered by a remote anchor node.

This layered and federated architecture ensures that device identity is managed in a secure, decentralized, and scalable manner across the IIoT ecosystem.

The primary role of blockchain is to replace traditional trusted authorities in storing and managing identity information, thereby enabling a decentralized identity authentication mechanism. Unlike conventional identity systems that rely on centralized Certificate Authorities (CAs) or Key Generation Centers (KGCs), blockchain leverages consensus protocols and tamper-resistant ledger structures to enhance the security, transparency, and auditability of identity data. By integrating lightweight cryptographic techniques—Chebyshev chaotic mapping—it becomes possible to design authentication protocols that are both computationally efficient and resource-friendly. This is particularly beneficial for environments with constrained devices, such as the Internet of Things (IoT). The fusion of blockchain and lightweight cryptography paves the way for a next-generation identity authentication system characterized by high scalability, strong security, and decentralized autonomy.

In addition, our proposed scheme exhibits strong scalability and can support large-scale device authentication (e.g., thousands of devices across multiple management domains). As the number of devices within or across domains increases, additional edge gateways can be deployed in the corresponding domains. These new edge gateways can quickly join the consortium blockchain network and synchronize with existing gateways. Once synchronized, they can operate in parallel to handle intra-domain and cross-domain authentication requests, thereby significantly enhancing the overall scalability of the system.

5. Security Requirements

During the design of the authentication scheme, it is essential to ensure both the integrity and confidentiality of messages exchanged during transmission, as well as the protection of device identity information. To achieve robust security in an Industrial Internet environment, the protocol must satisfy the following security requirements:

(1) Mutual Authentication and Key Agreement

The protocol must ensure mutual authentication between the device and the authentication server (e.g., edge gateway or anchor node). Only after both parties have authenticated each other should they engage in a secure key agreement phase to derive a session key used for subsequent communication.

(2) Resistance to Man-in-the-Middle (MitM) Attacks

The protocol must be designed to prevent attackers from intercepting, modifying, or injecting messages during transmission over public or insecure channels.

(3) Resistance to Impersonation Attacks

The protocol should be resilient against adversaries attempting to impersonate a legitimate device or authentication entity. This requires robust identity verification methods, often involving cryptographic proofs bound to unique device credentials.

(4) Device Anonymity and Privacy Preservation

The protocol should preserve device anonymity, ensuring that a device does not expose its real identity during authentication. Techniques such as pseudonym-based identifiers or zero-knowledge proofs can be employed to achieve unlinkability and identity concealment.

(5) Resistance to Replay Attacks

The protocol must prevent attackers from reusing previously captured messages or authentication exchanges to gain unauthorized access. Common countermeasures include nonces, timestamps, and session tokens that ensure message freshness and temporal uniqueness.

(6) Resistance to Ephemeral Key Leakage

Even if an adversary obtains temporary (ephemeral) session-specific keys, they should not be able to derive the session key or any other sensitive long-term credentials. This property, often referred to as ephemeral key compromise resilience, ensures the confidentiality of session keys under partial exposure scenarios.

(7) Forward Secrecy (Perfect Forward Secrecy, PFS)

The protocol must ensure that the exposure of long-term private keys does not affect the confidentiality of either past or future session keys. Forward secrecy protects earlier session keys from being compromised, even if a device's long-term credentials are revealed at a later point in time.

6. Proposed Cross-Domain Authentication Method

The proposed authentication method is explained in detail in this section. First, the system generates essential parameters (e.g., secret key, shared key, and public key) for the IIoT devices. Then, the proposed method and its detailed procedures for both intra-domain and cross-domain authentication of IIoT devices are thoroughly described. The notations of the proposed scheme are listed in Table 1.

Table 1. NOTATIONS IN THIS PAPER.

Notation	Description
ANR	Blockchain Anchor Node Representative
PK_A	Public Key of the Entity A
SK_A	Secret Key of the Entity A
S	Shared Key

Table 1. *Cont.*

Notation	Description
x	A Random Integer
p	Large Prime Number
$h(\bullet)$	Hash Function
D_i^X	The ith Device of Domain X
DID_i^X	ID of the ith Device of Domain X
$PDID_i^X$	The Pseudonymous ID of the ith Device of Domain X
EG_i^X	The ith Edge Gateway of Domain X
EID_i^X	ID of the ith Edge Gateway of Domain X
$T_y(x)$	The Chebyshev Polynomials
T_i	ith Timestamp
$\|\|$	OR Operation
$\oplus$	XOR Operation

6.1. System Initialization Phase

In the consortium blockchain, blockchain anchor nodes from different domains collaboratively generate a random integer $x \in (-\infty, \infty)$ using a distributed random number generation algorithm. A representative anchor node from the consortium blockchain generates the secret key SK_{ANR}, the shared key S, and a large prime number p. It then computes the public key:

$$PK_{ANR} = T_{SK_{ANR}}(x) \ mod \ p$$

The representative anchor node securely transmits the shared key S to the blockchain anchor nodes of each domain via a secure channel. It then selects a one-way hash function $h(\bullet)$ and publishes the system parameters

$$\{x, p, PK_{ANR}, h(\bullet)\}$$

on the blockchain. Besides the shared key S, the initialization parameters of the system are recorded in the blockchain's genesis block.

Subsequently, the consortium blockchain network, through a consensus mechanism, assigns a unique identifier EID_i^X to each Domain $X's$ Edge Gateway EG_i^X. Each Edge Gateway then locally generates its own private key $SK_{EG_i^X}$ and computes the corresponding public key:

$$PK_{EG_i^X} = T_{SK_{EG_i^X}}(x) \ mod \ p$$

The identity and public key pair $\{EID_i^X, PK_{EG_i^X}\}$ are submitted to the blockchain through the respective local blockchain anchor node, ensuring that each gateway is verifiably registered and authenticated within its domain.

The consortium blockchain network leverages the Industrial Internet Identification System to generate or retrieve a unique identifier DID_i^X for each Device D_i^X of each Domain X. Based on DID_i^X, the device generates a private key $SK_{D_i^X}$ and computes its corresponding public key as

$$PK_{D_i^X} = T_{SK_{D_i^X}}(x) \ mod \ p$$

The device then sends its identifier DID_i^X along with the public key $PK_{D_i^X}$ to Edge Gateway EG_i^X in its Domain X. Upon receiving the message, EG_i^X first verifies the validity

of DID_i^X using the Industrial Internet Identification System. If valid, it computes the pseudonymous identity $PDID_i^X = h(DID_i^X || SK_{EG_i^X})$ for the device D_i^X. The edge gateway then uploads $\{PDID_i^X, PK_{D_i^X}\}$ to the blockchain via its associated anchor node AN_i^X. This allows anchor nodes in other domains to retrieve the registration information of the device using its pseudonymous identifier. The pseudonymous identity is periodically updated to prevent continuous tracking by potential attackers. The update interval can be adjusted flexibly based on the specific context.

Edge Gateway EG_i^X then sends the pseudonymous identity $PDID_i^X$ back to Device D_i^X. Upon receiving the response, the device locally stores the tuple $\{SK_{D_i^X}, PK_{D_i^X}, PDID_i^X\}$.

This initialization phase establishes the trust foundation for subsequent mutual authentication and secure communication between industrial devices, edge gateways, and cross-domain nodes.

6.2. Intra-Domain Device Mutual Authentication

After the registration phase of Device D_i^A is completed, it can perform mutual authentication with Edge Gateway EG_i^A in the same Domain A. Here, we use Domain A as a concrete example of Domain X. As shown in Figure 2, the authentication process is as follows:

(1) Initial authentication message from the device to the edge gateway. Device D_i^A retrieves the registration information of Edge Gateway EG_i^A from the blockchain through the blockchain anchor node, generates a random number a_i and a timestamp T_1, and then computes

$$B_{it} = T_{SK_{D_i^A}}(PK_{EG_i^A})$$

$$E_i = T_{a_i}(x)$$

$$M_1 = PDID_i^A \oplus h(EID_i^A || B_{it})$$

$$M_2 = h(PDID_i^A || B_{it} || E_i || T_1)$$

Device D_i sends $(M_1, M_2, PK_{D_i^A}, E_i, T_1)$ to EG_i^A, where EID_i^A is the identifier of Edge Gateway EG_i^A.

(2) Authentication verification by the edge gateway. Upon receiving the message, Edge Gateway EG_i^A verifies whether the timestamp is within the valid range, i.e., $|T. - T._1;| < \Delta_t$, where T is the current timestamp and Δ_t is the valid time that represents the maximum allowable round-trip time for messages under normal conditions. Its value should be determined through statistical analysis based on the specific scenario. If the timestamp is valid, EG_i^A computes

$$B_{it} = T_{SK_{EG_i}}(PK_{D_i^A})$$

$$PDID_i^A = M_1 \oplus h(EID_i^A || B_{it})$$

Edge Gateway EG_i^A checks whether $\{PDID_i^A, PK_{D_i^A}\}$ exists on the blockchain through the anchor node. If $\{PDID_i^A, PK_{D_i^A}\}$ exists on the blockchain and $M_2 = h(PDID_i^A || B_{it} || E_i || T_1)$, then D_i^A is successfully authenticated. Edge Gateway EG_i^A then generates two random numbers a_t and b_t, along with a timestamp T_2, and computes

$$U_{it} = T_{a_t}(E_i)$$

$$V_t = T_{a_t}(x)$$

$$TID_i = h(b_t||EID_i^A||PDID_i^A)$$

$$M_3 = TID_i \oplus h(U_{it}||PDID_i^A)$$

$$SK_{it} = h(U_{it}||TID_i||PDID_i^A)$$

$$M_4 = h(SK_{it}||T_2)$$

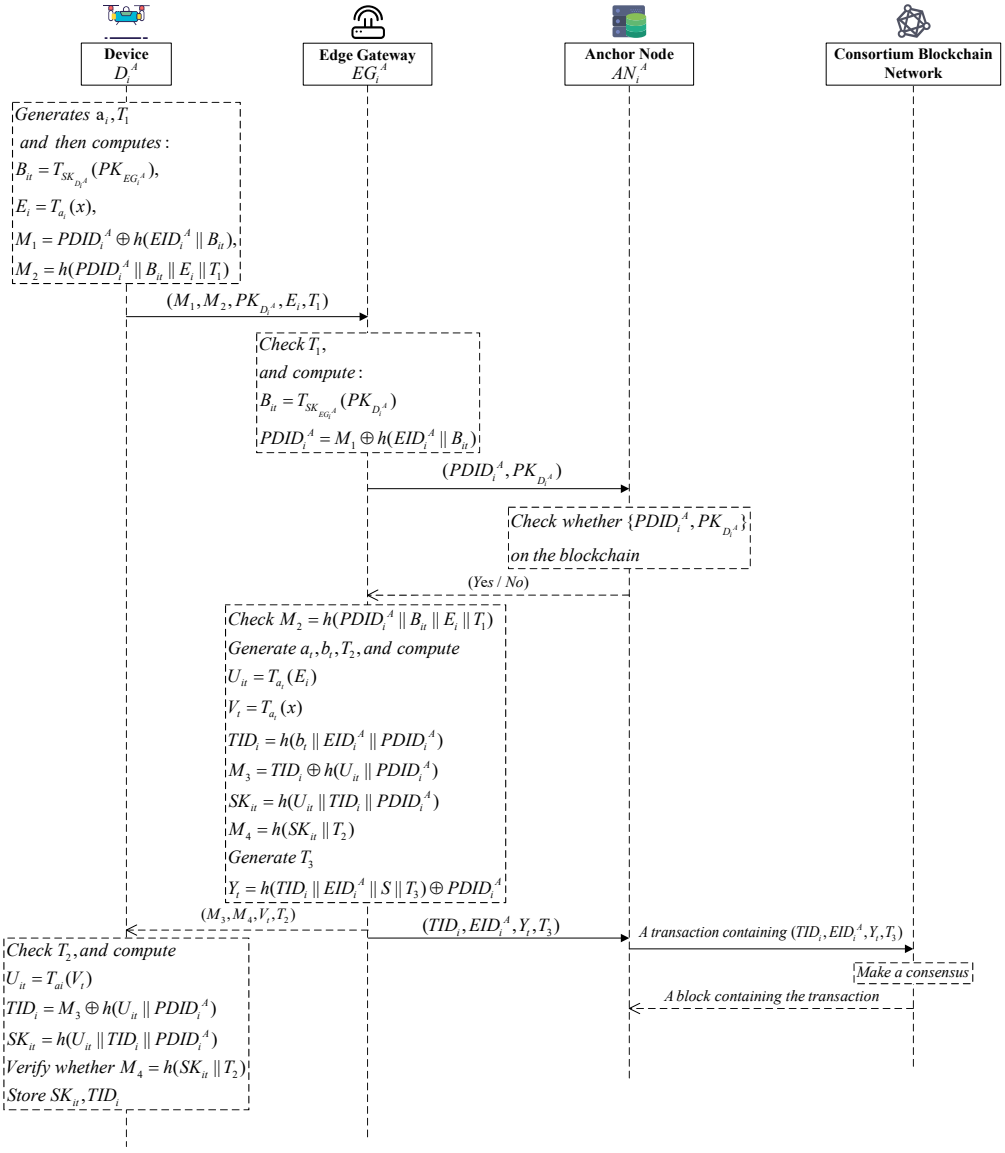


Figure 2. The workflow of intra-domain device mutual authentication.

EG_i sends (M_3, M_4, V_t, T_2) to D_i. Then, EG_i^A generates a new timestamp T_3 and computes

$$Y_t = h(TID_i||EID_i^A||S||T_3) \oplus PDID_i^A$$

Edge Gateway EG_i^A uploads TID_i, EID_i^A, Y_t, T_3 to the blockchain with the help of the associated anchor node. The successful recording of the message on the blockchain indicates that Device D_i^A has successfully passed authentication by EG_i^A at time T_3. Leveraging the immutability and transparency of the blockchain, edge gateways in other domains can quickly perform handover authentication for device Device D_i^A via anchor nodes based on its initial authentication record stored on the blockchain.

(3) Authentication verification by the device. Upon receiving the message, Device D_i^A first checks the validity of the timestamp T_2, ensuring that $|T - T_2| < \Delta_t$, where T is the current timestamp.

$$U_{it} = T_{a_i}(V_t)$$

$$TID_i = M_3 \oplus h(U_{it}||PDID_i^A)$$

$$SK_{it} = h(U_{it}||TID_i||PDID_i^A)$$

Device D_i^A verifies whether $M_4 = h(SK_{it}||T_2)$. If the values match, the authentication is successful, and the vehicle stores the session key SK_{it} and the temporary identity TID_i.

6.3. Cross-Domain Device Mutual Authentication

When Device D_i^A moves into Domain B, Device D_i^A and Edge Gateway EG_j^B should perform mutual authentication.

At this time, as shown in Figure 3, the authentication process is as follows:

(1) Initial authentication message from the device to the edge gateway of another edge gateway. Device D_i^A generates a random number c_i and a timestamp T_4 and then computes

$$W_i = T_{c_i}(x)$$

$$M_5 = h(EID_j^B||PDID_i^A||TID_i||T_4)$$

Afterwards, Device D_i^A sends (TID_i, W_i, M_5, T_4) to Edge Gateway EG_j^B.

(2) Authentication verification by the edge gateway. After receiving the message, Edge Gateway EG_j^B checks the validity of the timestamp T_4 by verifying C where T is the current timestamp. If the timestamp is valid, Edge Gateway EG_j^B then retrieves the authentication record TID_i, EID_i^A, Y_t, T_3 from the blockchain through the blockchain anchor node using TID_i and computes

$$h(TID_i||EID_i^A||S||T_3) \oplus Y_t = PDID_i^A$$

Edge Gateway EG_j^B verifies whether $M_5 = h(EG_j^B||PDID_i^A||TID_i||T_4)$. If they are equal, Device D_i^A is successfully authenticated. Then, Edge Gateway EG_j^B generates c_m and a timestamp T_5 and then computes

$$X_m = T_{c_m}(x)$$

$$Y_{im} = T_{c_m}(W_i)$$

$$SK_{im} = h(Y_{im}||TID_i||PDID_i^A)$$

$$M_6 = h(SK_{im}||T_5)$$

Edge Gateway EG_j^B sends $\{M_6, X_m, T_5\}$ to Device D_i^A.

(3) Authentication verification by the device. After receiving the information, Device D_i^A checks the validity of the timestamp T_5 by verifying whether $|T - T_5| < \Delta_t$. If the timestamp is valid, Device D_i^A then computes

$$Y_{im} = T_{c_i}(X_m)$$

$$SK_{im} = h(Y_{im}||ID_i||PDID_i^A)$$

Device D_i^A verifies whether $M_6 = h(SK_{im}||T_5)$. If they are equal, the device stores the session key SK_{im}.

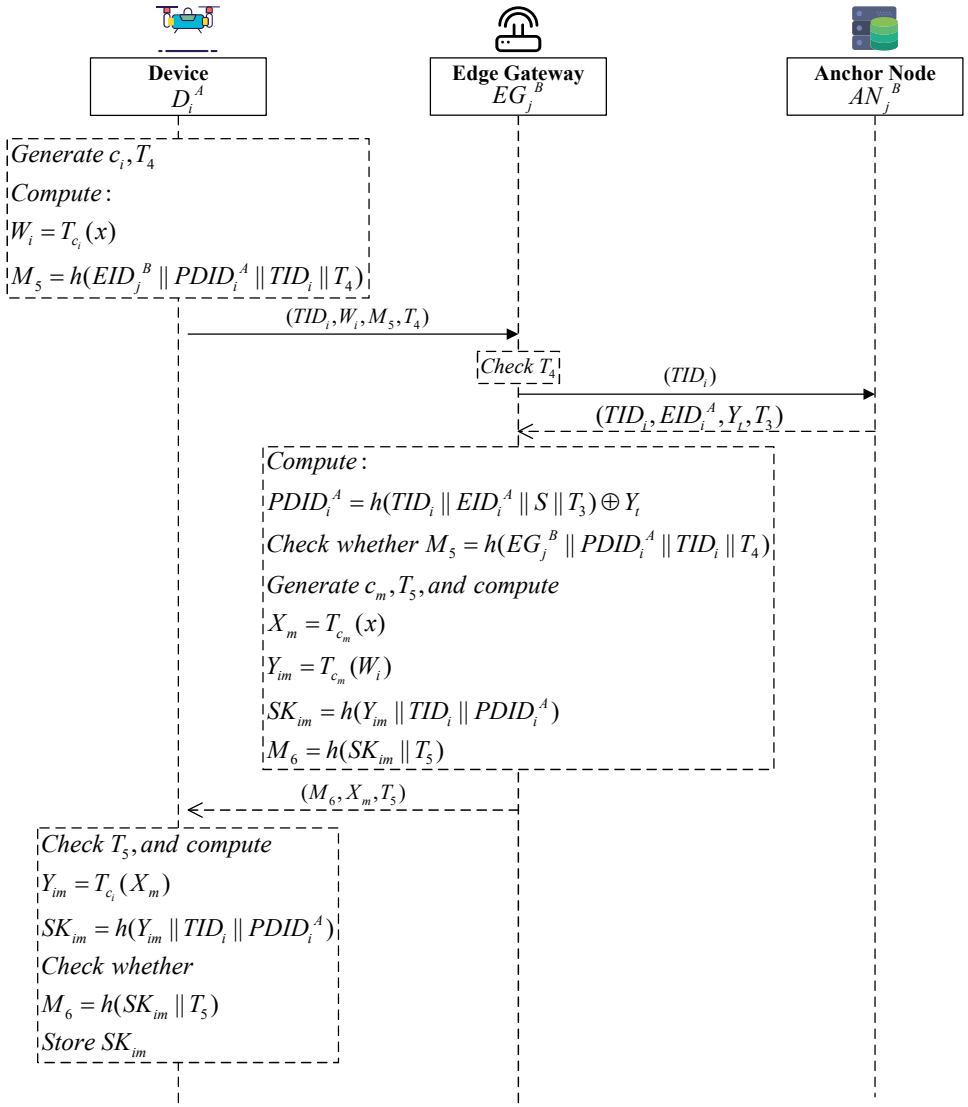


Figure 3. The workflow of cross-domain device mutual authentication.

7. Security Analysis

We have demonstrated the security of the proposed method using both informal and formal approaches.

7.1. Informal Security Analysis

(1) Mutual Authentication: Edge Gateway EG_i^X can obtain $PDID_i^X$ and the public key $PK_{D_i^X}$ from the message sent by Device D_i^X and retrieve the device's registration information from the blockchain through the anchor node. Edge Gateway EG_j^Y in a different domain can also retrieve the verification record containing $PDID_i^X$ from the blockchain through the anchor node. By using $PDID_i^X$ and the verification record, both EG_i^X and EG_j^Y can authenticate Device D_i^X. Device D_i^X can receive M_4 during the intra-domain authentication phase and M_6 during the cross-domain handover authentication phase. By utilizing M_4 and M_6, Device D_i^X can confirm that the messages are from Edge Gateway EG_i^X and Edge Gateway EG_j^Y, respectively. As a result, the proposed protocol supports mutual authentication.

(2) Session Key Agreement: Device D_i^X generates session keys SK_{it} and SK_{im} during intra-domain authentication and cross-domain handover authentication, respectively. An attacker may attempt to compute the session keys; however, without solving the discrete logarithm problem, the attacker cannot compute U_{it} and Y_{im}. Therefore, the attacker is unable to obtain the session keys SK_{it} and SK_{im}.

(3) Replay Attack: Each authentication message contains a timestamp. The receiver verifies the timestamp before performing any processing. If the timestamp is invalid, the receiver will discard the received message. This mechanism prevents attackers from replaying previously captured messages.

(4) Man-in-the-Middle Attack: Even if an attacker captures messages transmitted over public channels, they are unable to forge or modify the messages, because the attacker cannot obtain the valid parameters contained in the hash values of $\{M_2, M_4, M_5, M_6\}$. Therefore, the proposed scheme can effectively defend against man-in-the-middle attacks.

(5) Impersonation Attack: A malicious Device D_A may attempt to impersonate the legitimate Device D_i^X. However, during intra-domain authentication, D_A cannot obtain $PDID_i^X$ and the private key $SK_{D_i^X}$ of D_i^X. Therefore, it is unable to impersonate D_i^X or generate a legitimate authentication request message during cross-domain authentication.

(6) Anonymity: During the authentication phase, Device D_i^X uses a pseudonym $PDID_i^X$ for verification; therefore, its real identity is not exposed during the authentication process. In addition, the temporary identity TID_i contains a random number b_t, making it impossible for an attacker to obtain any identity information about Device D_i^X through TID_i. Thus, the proposed protocol can ensure the anonymity of the device.

(7) Short-Term Key Exposure: Even if the random numbers $\{a_i, a_t, b_t, c_i, c_m\}$ are exposed to an attacker, the attacker still cannot obtain $PDID_i^X$. Since $SK_{it} = h(U_{it}||TID_i||PDID_i^X)$ and $SK_{im} = h(Y_{im}||TID_i||PDID_i^X)$, the attacker is unable to compute the session keys.

(8) Forward Security: In this protocol, the generation of session keys SK_{it} and SK_{im} requires U_{it} and Y_{im}, which are generated by the device and the edge gateway during each authentication process based on random numbers. Even if an attacker knows all the long-term keys, they still cannot obtain or compute previous or current session keys. Therefore, the proposed protocol ensures forward security.

(9) Malicious Message Tracing: In the protocol proposed in this paper, the pseudonym $PDID_i^X$ of a legitimate device is assigned by the edge gateway, where $PDID_i^X = h(DID_i^X||SK_{EG_i^X})$, with DID_i^X being the real identity of the device and $SK_{EG_i^X}$ being the private key of Edge Gateway EG_i^X. Therefore, $PDID_i^X$ is unforgeable. When a legitimate user sends malicious messages, the edge gateway can trace back to the user's real identity DID_i^X by decrypting $PDID_i^X$.

7.2. Formal Security Analysis

During the authentication phase, another session key is established between the device and the edge gateway. In this section, it will be proven that the established session key is secure under the ROR (Real-Or-Random) model. Definition 1 provides the security definition of session keys within the ROR model. In the proposed cross-domain authentication model, there are three types of entities: Device D_i^X, Edge Gateway EG_i^X, and Edge Gateway EG_j^Y. Each type of entity contains multiple instances. Let Π^t denote the t-th instance of an entity. Then, $\Pi_{D_i^X}^{t_1}$, $\Pi_{EG_i^X}^{t_2}$, and $\Pi_{EG_j^Y}^{t_3}$ represent instances of D_i^X, EG_i^X, and EG_j^Y, respectively. All instances are treated as random oracles. Additionally, the adversary A is allowed to make the following queries:

(1) $EXECUTE(\Pi_{D_i^X}^{t_1}, \Pi_{EG_i^X}^{t_2}, \Pi_{EG_j^Y}^{t_3})$: The adversary A can perform this query to simulate an eavesdropping attack and obtain all the information exchanged between entities.

(2) $SEND(\Pi^t, m)$: By performing this query, the adversary A can simulate an active attack by sending a message m to the entity Π^t and obtaining the response information from that entity.

(3) $REVEAL(\Pi^t)$: The adversary A performs this query to obtain the session key of Entity Π^t. If Π^t does not have a session key, the query returns an undefined symbol $\perp$; otherwise, it returns the session key of Π^t.

(4) $TEST(\Pi^t)$: This query simulates the semantic security of the session key between entities. When the adversary A performs this query, if Entity Π^t does not have a defined session key, or if A has previously issued a REVEAL query to Π^t or any of its partners, the query returns an undefined symbol $\perp$. Otherwise, Π^t randomly generates a bit c, and the output is kept secret from the adversary A. If $c = 1$, the real session key is returned; if $c = 0$, a random number of the same length as the session key is returned.

Next, we will use these queries to prove the semantic security of the proposed method. In an authentication protocol, the semantic security proof plays a crucial role by providing formal guarantees of confidentiality and resistance to attacks in the presence of adversaries.

Theorem 1 (Semantic Security)**.** *Let $ADV_A(tp)$ denote the semantic security advantage of adversary A in breaking the proposed protocol within polynomial time tp, in order to obtain the session key $SK_{im} = SK_{mi}$ between D_i^X and EG_i^X during the initial authentication phase and the session key $SK_{it} = SK_{ti}$ between D_i^X and EG_j^Y during the handover authentication phase. Let q_h,$|Hash|$, and ADV_A^{CMDLP} represent, respectively, the number of hash queries made, the output space of the one-way collision-resistant hash function $H(*)$, and the adversary's advantage in solving the chaotic map-based discrete logarithm problem. Then,*

$$ADV_A \leq \frac{q_h^2}{|Hash|} + 2ADV_A^{CMDLP}$$

Proof. The adversary A can engage in three independent games G_i (where $i \in [0, 2]$) using the allowed queries. At the end of each game, if A can correctly guess whether the bit c in game G_i corresponds to the real session key or a random number, then A is considered to have won the game. Let $Success_{G_i}^A$ denote the event that A wins game G_i. Therefore, the advantage of A in winning game G_i is defined as

$$ADV_{G_i}^A = Pr\left[Success_{G_i}^A\right]$$

Here, $Pr[E]$ denotes the probability of event E. The games conducted by adversary A are as follows:

G_0: Game G_0 simulates a real attack launched by adversary A against the protocol under the ROR model. Since the probability that A correctly guesses the bit c is equal to the probability that A successfully breaks the real scheme, it follows from the definition of semantic security that

$$ADV_A = |2ADV_{G_0}^A - 1| \quad (1)$$

G_1: Within the game, adversary A carries out an eavesdropping attack through the EXECUTE query. The adversary A can obtain the messages $(M_1, M_2, PK_{D_i^X}, E_i, T_1)$ and (M_3, M_4, V_t, T_2) exchanged during the initial authentication phase, as well as the messages (TID_i, W_i, M_5, T_5) and (M_6, X_m, T_5) exchanged during the handover authentication phase.

Subsequently, A may also perform REVEAL and TEST queries to determine whether the returned bit c corresponds to a real session key or a random function. However, the values $E_i = T_{a_i}(x), V_t = T_{a_t}(x), W_i = T_{c_i}(m)$ contain random parameters (a_i, a_t, c_i, c_m), which A cannot obtain. Therefore, A is unable to extract any useful information. In this

round of the game, A's winning probability does not increase. Thus, A's advantage in winning game G_0 is equal to that in G_1:

$$ADV_{G_1}^{A} = ADV_{G_0}^{A} \tag{2}$$

G_2: In this game, the adversary A simulates an active attack by performing hash and SEND queries, attempting to forge messages that deceive the protocol participants into believing they are legitimate authentication messages. The game terminates only if A successfully constructs a valid message. During the initial authentication phase, A attempts to forge the message $\{M_1, M_2, PK_{v_i}, E_i, T_1\}$, where $M_1 = PDID_i^X \oplus h(EID_i^X||B_{it})$, $M_2 = h(PDID_i^X||B_{it}||E_i||T_1)$. To obtain the parameters $PDID_i^X$ and B_{it}, A must solve the CMDLP problem to compute B_{it} or, alternatively, find a hash collision to forge the message. Similarly, in the cross-domain handover authentication phase, A also needs to solve the CMDLP problem or find a hash collision. If hash collisions and CMDLP-solving capabilities are excluded in game G_2, A's advantage in winning G_2 is the same as in G_1. Based on the birthday paradox, the likelihood of a hash collision can be estimated as $\frac{q_h^2}{|Hash|}$. Therefore, A's advantage in winning game G_2 is given by

$$|ADV_{G_2}^{A} - ADV_{G_1}^{A}| \leq \frac{q_h^2}{2|Hash|} + ADV_A^{CMDLP} \tag{3}$$

At this point, A has completed all queries. In order to win game G_2, A performs the TEST query and then randomly guesses the bit c. Therefore,

$$ADV_{G_2}^{A} = 1/2 \tag{4}$$

By using Equations (1)–(4), the following equation can be derived:

$$\frac{1}{2}ADV_A = |ADV_{G_1}^{A} - 1/2| = |ADV_{G_2}^{A} - ADV_{G_1}^{A}| \leq \frac{q_h^2}{2|Hash|} + ADV_A^{CMDLP} \tag{5}$$

By multiplying both sides of Equation (5) by 2, we obtain

$$ADV_A \leq \frac{q_h^2}{|Hash|} + ADV_A^{CMDLP} \tag{6}$$

Theorem 1 is thus proved, and the advantage of adversary A is negligible. Therefore, the session key in the proposed protocol is semantically secure under the ROR model. □

8. Result Analysis

This paper compares the proposed protocol's computational and communication overhead with existing cross-domain authentication protocols that are currently the most efficient and cost-effective works. For a fair evaluation, the compared schemes are all assumed to have security levels equivalent to the Advanced Encryption Standard (AES) 128-bit. Specifically, the key length for symmetric encryption and decryption is 128 bits, the key length for elliptic curve encryption is 256 bits, the hash function output is 256 bits, and the lengths of random numbers and identity identifiers are 128 bits. The timestamp length is 32 bits. According to reference [43], since the Chebyshev discrete logarithm problem can only be solved through exhaustive search, this paper assumes that the key length of the Chebyshev polynomial is 128 bits.

8.1. Computation Cost

This section evaluates the computational overhead of the proposed cross-domain handover authentication protocol and compares it with other protocols. The experiments were conducted in an environment with a quad-core Intel(R) Core(TM) i7-8750H 2.20GHz CPU, 16GB RAM (Intel, Santa Clara, CA, USA), and the operating system Ubuntu-22.04.4-desktop-amd64. Various cryptographic primitives were implemented using the MIRACL cryptographic library. In addition, the matrix iteration algorithm was used to write the corresponding C language code for testing the computation time of Chebyshev polynomials. Since the execution time of the XOR operation is negligible, it was ignored in the evaluation. The data is generated from the experiments implemented by MIRACL cryptographic library and Hyperledger Fabric frameworks. Table 2 and Figure 4 present the execution times of various cryptographic primitives.

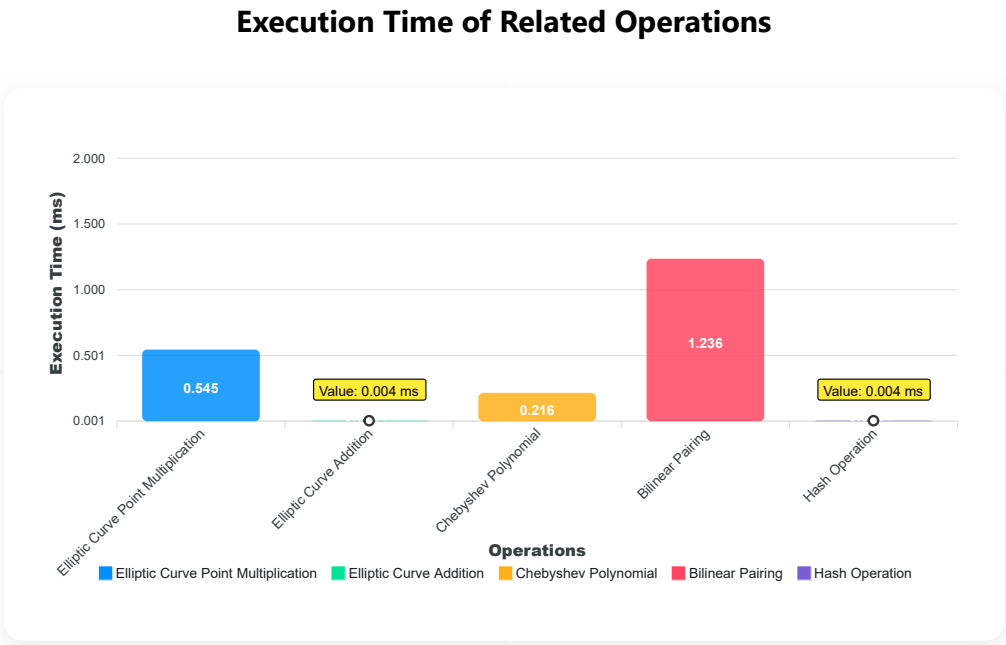


Figure 4. Execution time of related operations.

Table 2. Execution time of related operations.

Computational Operation	Definition	Execution Time (ms)
T_{mul}	Elliptic Curve Point Multiplication	0.545
T_{add}	Elliptic Curve Addition	0.004
T_c	Chebyshev Polynomial	0.216
T_{bp}	Bilinear Pairing	1.236
T_h	Hash Operation	0.004

In the cross-domain handover authentication protocol proposed in this paper, the device side performs three hash operations and two Chebyshev chaotic map computations, with an execution time of $3T_h + 2T_c = 0.468$ ms. On the edge gateway side, four hash operations and two Chebyshev polynomial computations are carried out, resulting in an execution time of $4T_h + 2T_c = 0.456$ ms. Therefore, the total computational overhead is 0.924 ms.

According to the computational overhead comparison in Table 3, bilinear pairing operations incur significantly higher costs. As shown in Figure 5, the scheme in Reference [44]

exhibits the highest computational overhead, while the proposed protocol incurs the lowest. This efficiency stems from the use of the semigroup property of Chebyshev polynomials to establish session keys, thereby avoiding computationally intensive operations such as bilinear pairing and elliptic curve point multiplication.

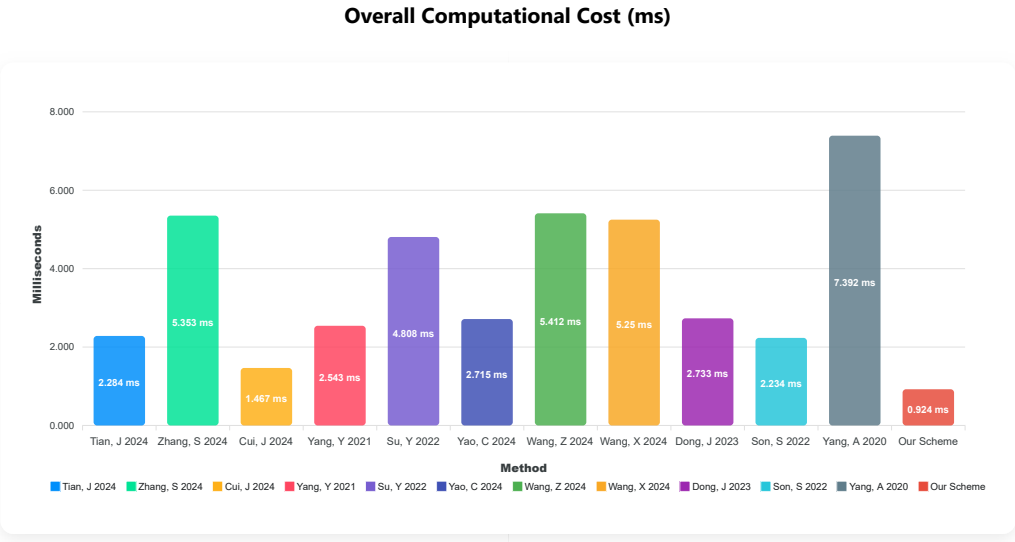


Figure 5. Comparison of computational cost with schemes Tian, J 2024 [4], Zhang, S 2024 [8], Cui, J 2024 [10], Yang, Y 2021 [14], Su, Y 2022 [16], Yao, C 2024 [28], Wang, Z 2024 [30], Wang, X 2024 [32], Dong, J 2023 [33], Son, S 2022 [45], and Yang, A 2020 [44].

Table 3. Comparison of computational overhead with related work.

Method	Device Side	Edge Gateway Side	Overall Computational Cost (ms)
Tian, J et al. [4]	$4T_h + 2T_{mul}$	$5T_h + 2T_{mul}$	2.284
Zhang, S et al. [8]	$7T_h + 5T_{mul}$	–	5.353
Cui, J et al. [10]	$3T_h + 3T_{mul}$	$4T_h + 5T_{mul} + 3T_{add}$	1.467
Yang, Y et al. [14]	$4T_h + 6T_{mul} + 4T_{add}$	–	2.543
Su, Y et al. [16]	$5T_h + 9T_{mul} + 4T_{add}$	$5T_h + 7T_{mul} + 3T_{add}$	4.808
Yao, C et al. [28]	$2T_h + 3T_{mul} + 3T_{add}$	–	2.715
Wang, Z et al. [30]	$4T_h + 6T_{mul} + 3T_{add}$	–	5.412
Wang, X et al. [32]	$4T_{mul} + 3T_{add}$	–	5.250
Dong, J et al. [33]	$5T_{mul} + 2T_{add}$	–	2.733
Son, S et al. [45]	$6T_h$	$12T_h + 4T_{mul} + T_{add}$	2.234
Yang, A et al. [44]	$3T_h + 4T_{mul}$	$2T_h + 2T_{mul} + 3T_{add}$	7.392
Our Method	$3T_h + 2T_{mul}$	$4T_h + 2T_c$	0.924

The proposed protocol thus achieves low computational overhead while ensuring security, making it a lightweight and efficient solution.

8.2. Communication Cost

Table 4 lists the communication overhead between the device and the edge gateway for the proposed cross-domain handover authentication protocol and the comparison schemes. It is worth noting that Table 4 does not cover all methods listed in Table 3, as not all of the related works conducted experiments on communication overhead. As shown in Table 4, the proposed protocol involves the exchange of two messages. Specifically, the device sends the message $\{TID_i, W_i, M_5, T_4\}$ to the edge gateway, resulting in a communication overhead of 660 bits on the device side. In response, the edge gateway sends the message

$\{M_6, X_m, T_5\}$ to the device, with a corresponding overhead of 410 bits. Therefore, the total communication overhead is 1070 bits. While our method may not be the most optimal in terms of communication cost, as shown in Figure 6, it provides a superior trade-off by achieving the best computational efficiency, making it highly suitable for resource-constrained IIoT environments.

Table 4. Comparison of communication cost with related work.

Method	Device Side (bits)	Edge Gateway Side (bits)	Overall Communication Cost (bits)
Tian, J et al. [4]	672	800	1472
Cui, J et al. [10]	613	613	1226
Yang, Y et al. [14]	584	584	1168
Su, Y et al. [16]	240	236	476
Wang, Z et al. [30]	1376	—	1376
Dong, J et al. [33]	536	536	1072
Son, S et al. [45]	800	800	1600
Yang, A et al. [44]	832	-	832
Our Method	660	410	1070

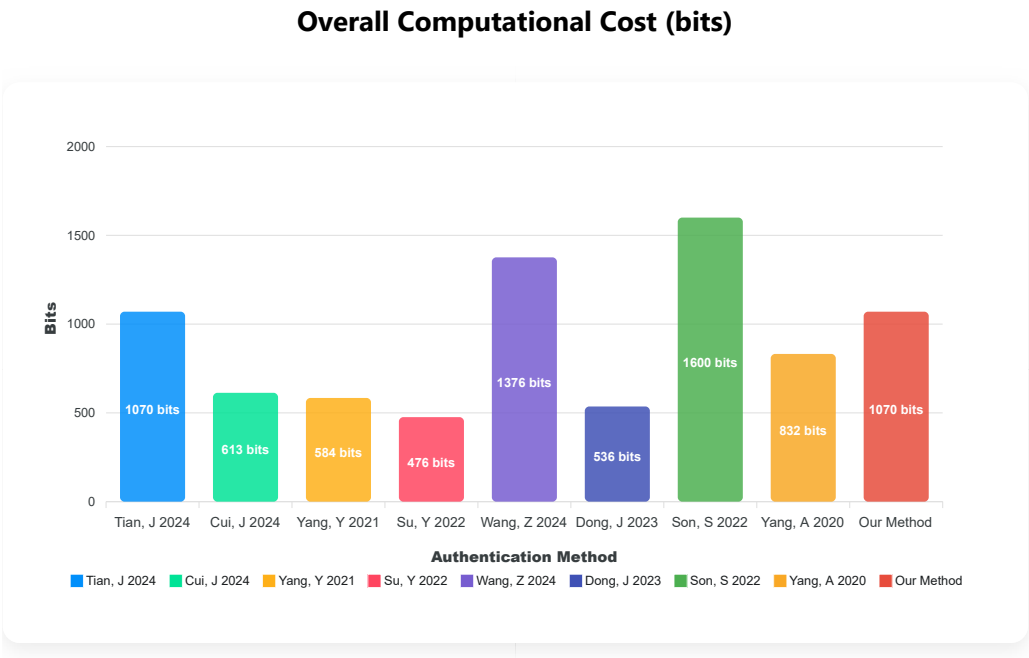


Figure 6. Comparison of communication cost with schemes Tian, J 2024 [4], Cui, J 2024 [10], Yang, Y 2021 [14], Su, Y 2022 [16], Wang, Z 2024 [30], Dong, J 2023 [33], Son, S 2022 [45], and Yang, A 2020 [44].

8.3. Authentication Latency

Authentication latency means the delay was caused by the mutual authentication, which contains the computation time both on device and edge gateway and the message propagation time.

From the device's perspective, as the number of cross-domain authentications m increases, the local computation delay can be expressed as $3T_c + 5T_h + m(3T_h + 2T_c)$, where $3T_c + 5T_h$ represents the computation time required during the initialization phase and $3T_h + 2T_c$ denotes the computation delay incurred during mutual authentication with edge gateways in different domains. In contrast, the local computation delays of the device for the scheme [4,10,17,44,45] are $2T_{mul} + 4T_h + m(2T_{mul} + 4T_h)$,

$2T_{mul} + 2T_h + m(3T_{mul} + 3T_h)$, $3T_{mul} + 2T_h + m(9T_{mul} + 5T_h + 4T_{add})$, $6T_h + m6T_h$, and $6T_p + (4m-1)T_{mul} + (m+6)T_h$, respectively. As illustrated in Figure 7a, the scheme [45] exhibits the lowest computation delay, as it relies solely on hash operations for device-to-gateway authentication. Our scheme achieves the second-lowest computation overhead by replacing computationally intensive elliptic curve scalar multiplication and addition with Chebyshev chaotic map operations.

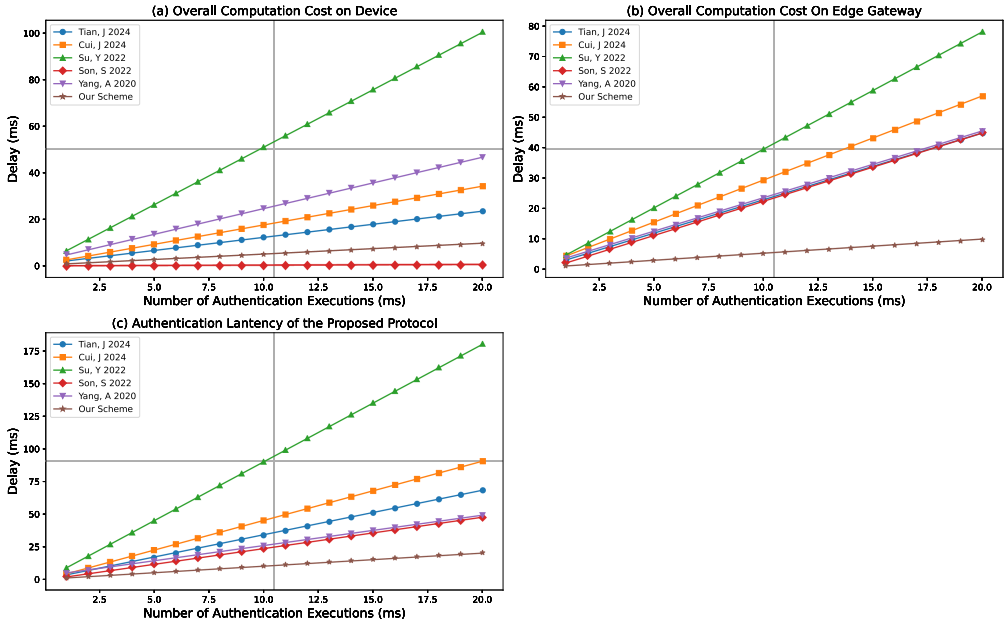


Figure 7. Performance evaluation and comparison of the authentication latency with schemes Tian, J 2024 [4], Cui, J 2024 [10], Su, Y 2022 [16], Son, S 2022 [45], and Yang, A 2020 [44].

From the perspective of the edge gateway, as the number of cross-domain authentications m increases, the local computation delay can be expressed as $3T_c + 6T_h + m(4T_h + 2T_c)$, where $3T_c + 6T_h$ represents the computation time required during the initialization phase and $4T_h + 2T_c$ denotes the computation delay incurred during mutual authentication with devices from other domains. In comparison, the local computation delays of the edge gateway for the scheme [4,10,17,44,45] are $2T_{mul} + 5T_h + m(2T_{mul} + 5T_c)$, $3T_{mul} + 3T_h + m(4T_h + 5T_{mul} + 3T_{add})$, $2T_{mul} + 2T_h + m(7T_{mul} + 5T_h + 3T_{add})$, $12T_h + m(4T_{mul} + 12T_h + T_{add})$, and $(3m+1)T_p + (m+2)T_{mul} + (m+3)T_h$, respectively. As illustrated in Figure 7b, our proposed scheme achieves the lowest computation delay on the edge gateway side, outperforming scheme [45]. This is because scheme [45] offloads the computationally intensive elliptic curve operations required for device authentication onto the more powerful edge gateway, whereas our scheme avoids such operations entirely by adopting lightweight Chebyshev chaotic map-based computations.

Above all, the overall authentication latency can be approximated as $m(3T_h + 2T_c) + m(4T_h + 2T_c) + m(T_{DE} + T_{BQ})$, where T_{DE} denotes the message transmission delay from the device to the edge gateway and T_{BQ} represents the latency associated with querying the blockchain. According to [44], T_{DE} is approximately 100 ms, and based on our experimental results, T_{BQ} is around 15 ms. In comparison, the total authentication latencies of schemes [4,10,17,44,45] are $m(2T_{mul} + 4T_h) + m(2T_{mul} + 5T_c) + m(T_{DE} + T_{BQ})$, $m(3T_{mul} + 3T_h) + m(4T_h + 5T_{mul} + 3T_{add}) + m(T_{DE} + T_{BQ})$, $m(9T_{mul} + 5T_h + 4T_{add}) + m(7T_{mul} + 5T_h + 3T_{add}) + m(2T_{DE} + T_{BQ})$, $6mT_h + m(4T_{mul} + 12T_h + T_{add}) + m(T_{DE} + T_{BQ})$, and $6T_p + (4m-1)T_{mul} + (m+6)T_h + m(T_{DE} + T_{BQ})$, respectively. As illustrated in Figure 7c, our proposed scheme achieves the lowest overall authentication latency,

benefiting from the use of lightweight Chebyshev chaotic map operations in place of computationally expensive elliptic curve operations.

9. Conclusions

In this paper, we propose a lightweight and secure cross-domain authentication scheme for the Industrial Internet of Things (IIoT) by integrating blockchain technology with Chebyshev chaotic maps. The proposed method effectively addresses the critical challenges of identity fragmentation, computational complexity, and communication latency that plague traditional blockchain-based authentication frameworks. By leveraging the decentralized and tamper-resistant nature of blockchain for device identity management and employing the semigroup property of Chebyshev polynomials to facilitate efficient session key generation, our scheme ensures both robustness and performance in resource-constrained and latency-sensitive industrial environments. A formal security analysis based on the Real-Or-Random (ROR) model confirms that the protocol satisfies key security requirements, including mutual authentication, resistance to various attacks, anonymity, and forward secrecy. Furthermore, empirical evaluations using the Hyperledger Fabric platform and the MIRACL cryptographic library demonstrate that our scheme achieves lower computational and communication overhead compared to existing solutions, without compromising on security. Overall, the proposed authentication framework presents a promising direction for enhancing trust and efficiency in cross-domain collaborations within IIoT systems. Future work may explore the integration of privacy-preserving techniques and scalability optimizations to further adapt the scheme to emerging industrial scenarios and large-scale deployments.

Author Contributions: Conceptualization, Z.Z.; methodology, Z.Z.; software, J.L.; validation, Z.Z. and X.L.; formal analysis, X.Z.; investigation, Z.Z.; resources, J.M.; data curation, Z.Z.; writing—original draft preparation, Z.Z. and J.L.; writing—review and editing, C.J. and Y.M.; visualization, X.L.; supervision, C.J.; project administration, Z.Z.; funding acquisition, Z.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Huaian Science and Technology Plan Project Natural Science Research grant number HAB2024048.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors report no conflicts of interest. The funding sources did not influence the study's design, data collection, analysis, interpretation, or manuscript preparation or the decision to publish the findings.

Abbreviations

The following abbreviations are used in this manuscript:

ROR	Real-Or-Random
CAGR	compound annual growth rate
PKI	Public Key Infrastructure
IBC	identity-based cryptography
CL-PKC	Certificateless Public Key Cryptography
ECC	elliptic curve cryptography
IIoT	Industrial Internet of Things
CA	Certificate Authority
KGC	Key Generation Center
CMDDHP	Chaotic Maps Decisional Diffie–Hellman Problem
PoW	Proof of Work

PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance

References

1. Hu, Y.; Jia, Q.; Yao, Y.; Lee, Y.; Lee, M.; Wang, C.; Zhou, X.; Xie, R.; Yu, F. Industrial internet of things intelligence empowering smart manufacturing: A literature review. *IEEE Internet Things J.* **2024**, *11*, 19143–19167. [CrossRef]
2. Industrial IoT Industry Worth $286.3 Billion by 2029. Available online: https://www.marketsandmarkets.com/PressReleases/industrial-internet-of-things.asp (accessed on 18 June 2025).
3. Alsheavi, A.; Hawbani, A.; Othman, W.; Wang, X.; Qaid, G.; Zhao, L.; Al-Dubai, A.; Zhi, L.; Ismail, A.; Jhaver, R.; et al. IoT Authentication Protocols: Challenges, and Comparative Analysis. *ACM Comput. Surv.* **2025**, *57*, 1–43. [CrossRef]
4. Tian, J.; Shen, Y.; Wang, Y. Blockchain-based fast handover authentication protocol for Internet of Vehicles in small industrial parks. *Veh. Commun.* **2024**, *50*, 100848. [CrossRef]
5. Liu, Y.; Liu, A.; Xia, Y.; Hu, B.; Liu, J.; Wu, Q.; Tiwari, P. A Blockchain-Based Cross-Domain Authentication Management System for IoT Devices. *IEEE Trans. Netw. Sci. Eng.* **2023**, *11*, 115–127. [CrossRef]
6. Khan, S.; Luo, F.; Zhang, Z.; Ullah, F.; Amin, F.; Qadri, S.; Heyat, M.; Ruby, R.; Wang, L.; Ullah, S.; et al. A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. *IEEE Commun. Surv. Tutorials* **2023**, *25*, 2529–2568. [CrossRef]
7. Wang, M.; Rui, L.; Yang, Y.; Gao, Z.; Chen, X. A Blockchain-Based Multi-CA Cross-Domain Authentication Scheme in Decentralized Autonomous Network. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2664–2676. [CrossRef]
8. Zhang, S.; Yan, Z.; Liang, W.; Li, K.; Martino, B. BCAE: A Blockchain-Based Cross Domain Authentication Scheme for Edge Computing. *IEEE Internet Things J.* **2024**, *11*, 24035–24048. [CrossRef]
9. Tong, F.; Chen, X.; Wang, K.; Zhang, Y. CCAP: A complete cross-domain authentication based on blockchain for Internet of Things. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 3789–3800. [CrossRef]
10. Cui, J.; Zhu, Y.; Zhong, H.; Zhang, Q.; Gu, C.; He, D. Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT. *IEEE Internet Things J.* **2024**, *11*, 16325–16338. [CrossRef]
11. Cui, J.; Liu, N.; Zhang, Q.; He, D.; Gu, C.; Zhong, H. Efficient and anonymous cross-domain authentication for IIoT based on blockchain. *IEEE Trans. Netw. Sci. Eng.* **2024**, *10*, 899–910. [CrossRef]
12. Zhang, H.; Zhao, F. Cross-domain identity authentication scheme based on blockchain and PKI system. *High-Confid. Comput.* **2023**, *3*, 100096. [CrossRef]
13. Saleem, T.; Janjua, M.U.; Hassan, M.; Ahmad, T.; Tariq, F.; Hafeez, K.; Salal, M.A.; Bilal, M.D. ProofChain: An X. 509-compatible blockchain-based PKI framework with decentralized trust. *Comput. Networks* **2022**, *213*, 109069. [CrossRef]
14. Yang, Y.; Wei, L.; Wu, J.; Long, C.; Li, B. A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network. *IEEE Internet Things J.* **2021**, *9*, 8078–8090. [CrossRef]
15. Luo, D.; Cai, Q.; Sun, G.; Yu, H.; Niyato, D. Split-chain based efficient blockchain-assisted cross-domain authentication for IoT. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 3209–3223. [CrossRef]
16. Su, Y.; Wang, Y.; Li, J.; Su, Z.; Pedrycz, W.; Hu, Q. Oracle based privacy-preserving cross-domain authentication scheme. *IEEE Trans. Sustain. Comput.* **2024**, *9*, 602–614. [CrossRef]
17. Xue, L.; Huang, H.; Xiao, F.; Wang, W. A cross-domain authentication scheme based on cooperative blockchains functioning with revocation for medical consortiums. *IEEE Trans. Sustain. Comput.* **2022**, *19*, 2409–2420. [CrossRef]
18. Manasrah, A.; Yaseen, Q.; Al-Aqrabi, H.; Liu, L. Identity-Based Authentication in VANETs: A Review. *IEEE Trans. Intell. Transp. Syst.* **2025**, *26*, 4260–4282. [CrossRef]
19. Xiong, H.; Gong, L.; Li, R.; Kumari, S.; Chen, C.; Amoon, M. Blockchain-enabled distributed identity-based ring signature with identity abort for consumer electronics. *IEEE Trans. Consum. Electron.* **2024**, *70*, 5340–5352. [CrossRef]
20. Zhang, C.; Zhao, M.; Zhang, W.; Fan, Q.; Ni, J.; Zhu, L. Privacy-preserving identity-based data rights governance for blockchain-empowered human-centric metaverse communications. *IEEE J. Sel. Areas Commun.* **2023**, *42*, 963–977. [CrossRef]
21. Li, R.; Wang, Z.; Fang, L.; Peng, C.; Wang, W.; Xiong, H. Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse. *IEEE Trans. Consum. Electron.* **2024**, *70*, 3770–3780. [CrossRef]
22. Li, B.; Ma, M. An advanced hierarchical identity-based security mechanism by blockchain in named data networking. *J. Netw. Syst. Manag.* **2023**, *31*, 13. [CrossRef]
23. Yang, Y.; He, D.; Vijayakumar, P.; Gupta, B.; Xie, Q. An efficient identity-based aggregate signcryption scheme with blockchain for IoT-enabled maritime transportation system. *IEEE Trans. Green Commun. Netw.* **2022**, *6*, 1520–1531. [CrossRef]
24. Babu, E.; Dadi, A.; Singh, K.; Nayak, S.; Bhoi, A.; Singh, A. A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system. *Expert Syst.* **2022**, *39*, e12941. [CrossRef]
25. Srivastava, V.; Debnath, S.; Bera, B.; Das, A.; Park, Y.; Lorenz, P. Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for Internet of Vehicles environment. *IEEE Trans. Veh. Technol.* **2022**, *71*, 9853–9867. [CrossRef]

26. Zhang, J.; Zhang, F. Identity-Based Key Agreement for Blockchain-Powered Intelligent Edge. *IEEE Internet Things J.* **2021**, *9*, 6688–6702. [CrossRef]
27. Sharma, P.; Moparthi, N.; Namasudra, S.; Shanmuganathan, V.; Hsu, C. Blockchain-based IoT architecture to secure healthcare system using identity-based encryption. *Expert Syst.* **2022**, *39*, e12915. [CrossRef]
28. Yao, C.; Zhang, X.; Liu, Y.; Zhao, B.; Wu, Q.; Susilo, W. Blockchain-Based Secure and Efficient ADS-B Authentication via Certificateless Signature With Packet Loss Tolerance. *IEEE Internet Things J.* **2024**, *12*, 10574–10588. [CrossRef]
29. Zhang, J.; Chen, X.; Cheng, Q.; Chen, X.; Luo, X. An Enhanced Certificateless Blockchain-Assisted Authentication and Key Agreement Protocol for Internet of Drones. *IEEE Trans. Netw. Sci. Eng.* **2025**, *12*, 3065–3081. [CrossRef]
30. Wang, Z.; Zong, Z.; Li, F.; Sun, S.; Zhao, P. Revocable Certificateless Cross-Domain Authentication Scheme Based on Primary—Secondary Blockchain. *IEEE Trans. Comput. Soc. Syst.* **2024**, *11*, 5880–5891. [CrossRef]
31. Feng, L.; Qiu, F.; Hu, K.; Yu, B.; Lin, J.; Yao, S. CABC: A Cross-Domain Authentication Method Combining Blockchain with Certificateless Signature for IIoT. *Future Gener. Comput. Syst.* **2024**, *158*, 516–529. [CrossRef]
32. Wang, X.; Wang, W.; Huang, C.; Cao, P.; Zhu, Y.; Wu, Q. Blockchain-based certificateless conditional anonymous authentication for IIoT. *IEEE Syst. J.* **2024**, *18*, 656–667. [CrossRef]
33. Dong, J.; Xu, G.; Ma, C.; Liu, J.; Cliff, U. Blockchain-based certificate-free cross-domain authentication mechanism for industrial internet. *IEEE Internet Things J.* **2023**, *11*, 3316–3330. [CrossRef]
34. Liu, X.; Wang, L.; Li, L.; Zhang, X.; Shufen, N. Certificateless Anonymous Cross-Domain Authentication Scheme Assisted by Blockchain for Internet of Vehicles. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 3488977. [CrossRef]
35. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proc. Thirteen. Eurosys Conf.* **2018**, 1–15.. [CrossRef]
36. Pigatto, D.; Silva, N.; Branco, K. Performance evaluation and comparison of algorithms for elliptic curve cryptography with El-Gamal based on MIRACL and RELIC libraries. *J. Appl. Comput. Res.* **2011**, *1*, 95–103. [CrossRef]
37. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 18 June 2025).
38. Gavin, W. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2008**, *151*, 1–32.
39. Miguel, C.; Liskov, B. Practical byzantine fault tolerance. *OsDI* **1999**, *99*, 173–186.
40. Abbasinezhad-Mood, D.; Nikooghadam, M. Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of NanoPi fire. *IEEE Trans. Reliab.* **2018**, *67*, 1328–1339. [CrossRef]
41. Zhu, H.; Zhang, Y.; Xia, Y.; Li, H. Password-Authenticated Key Exchange Scheme Using Chaotic Maps towards a New Architecture in Standard Model. *Int. J. Netw. Secur.* **2016**, *18*, 326–334.
42. Abbasinezhad-Mood, D.; Ostad-Sharif, A.; Mazinani, S.; Nikooghadam, M. Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection. *IEEE Trans. Ind. Inform.* **2020**, *16*, 7287–7294. [CrossRef]
43. Ma, R.; Cao, J.; Feng, D.; Li, H.; Li, X.; Xu, Y. A robust authentication scheme for remote diagnosis and maintenance in 5G V2N. *Veh. Commun.* **2022**, *198*, 103281. [CrossRef]
44. Yang, A.; Weng, J.; Yang, K.; Huang, C.; Shen, X. Delegating authentication to edge: A decentralized authentication architecture for vehicular networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *23*, 1284–1298. [CrossRef]
45. Son, S.; Lee, J.; Park, Y.; Park, Y.; Das, A. Design of blockchain-based lightweight V2I handover authentication protocol for VANET. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 1346–1358. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.