DPS-IIoT: Non-Interactive Zero-Knowledge Poof-inspired Access Control towards Information-Centric Industrial Internet of Things

Dun Li, Noel Crespi, Roberto Minerva, Wei Liang, Kuan-Ching Li, Joanna Kolodziejczyk

DPS-IIoT: Non-Interactive Zero-Knowledge Poof-inspired Access Control towards Information-Centric Industrial Internet of Things

Dun Li[a,b], Noel Crespi[b,*], Roberto Minerva[b], Wei Liang[c], Kuan-Ching Li[d,*] and Joanna Kołodziej[e]

[a]The Department of Industrial Engineering, Tsinghua University, Beijing 100084, P. R. China.
[b]Samovar, Telecom SudParis, Institut Polytechnique de Paris, 91120 Palaiseau, France.
[c]School of Computer Science and Engineering, Hunan University of Science and Technology, and Hunan Key Laboratory for Service Computing and Novel Software Technology, China.
[d]Dept. of Computer Science and Information Engineering, Providence University, Taiwan.
[e]Dept. of Computer Science, Cracow University of Technology, and NASK-PIB, ul. Kolska 12, 01-045 Warsaw, Poland.

ARTICLE INFO

Keywords:
Industrial Internet of Things
Information-Centric Network
Zero-Knowledge Proof
CP-ABE
Blockchain

ABSTRACT

The advancements in 5G/6G communication technologies have enabled the rapid development and broader application of the Industrial Internet of Things (IIoT). However, the limitations of traditional host-centric networks are becoming more apparent, especially in meeting the growing demands of the IIoT for higher data speeds, enhanced privacy protections, and greater resilience to disruptions. In this work, we present the ZK-CP-ABE algorithm, a novel security framework designed to enhance security and efficiency in distributing content within the IIoT. By integrating a non-interactive zero-knowledge proof (ZKP) protocol for user authentication and data validation into the existing Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the ZK-CP-ABE algorithm substantially improves privacy protections while efficiently managing bandwidth usage. Furthermore, we propose the Distributed Publish-Subscribe Industrial Internet of Things (DPS-IIoT) system, which uses Hyperledger Fabric blockchain technology to safeguard access policies and ensure the integrity of ZKP from tampering and cyber-attacks, thereby enhancing the security and reliability of IIoT networks. To validate the effectiveness of our approach, extensive experiments were conducted, demonstrating that the proposed ZK-CP-ABE algorithm significantly reduces bandwidth consumption, while maintaining robust security against unauthorized access. Experimental evaluation shows that the ZK-CP-ABE algorithm and DPS-IIoT system significantly enhance bandwidth efficiency and overall throughput in IIoT environments.

1. Introduction

The development of the Industrial Internet of Things (IIoT) has fundamentally reshaped industrial operations [1], highlighting the need for more efficient data management. In this context, the Information-Centric Network (ICN) emerges as a strategic solution, advancing data localization to enhance information flow within the IIoT. It emphasizes the necessity of complex security measures, especially in access management [2, 3, 4, 5]. Given the dynamic and multifaceted nature of IIoT networks, traditional host-centric access control approaches are increasingly insufficient [6]. Therefore, to accommodate the decentralized and content-centric nature of the IIoT, there is an urgent need for a more flexible, scalable, and security-driven approach built on the ICN framework.

However, as real-time data services become increasingly prevalent in the IIoT, traditional peer-to-peer packet transfer methods face significant challenges, including: 1) the heightened risk of a single point of failure, which can precipitate informational redundancy and squandering resources within clustered networks [7, 8, 9], 2) reduced system throughput attributable to the limitations imposed by bandwidth and computational capacity, severely hinder operational efficiency [10, 11, 12, 13, 14, 15, 16], 3) compromised data security, stemming from encryption protocols that fail to meet the demanding standards of contemporary IIoT frameworks [17, 18, 19], and 4) a sub-optimal tolerance for network disruptions, reflecting the inherent volatility of IIoT communication infrastructures [20, 21].

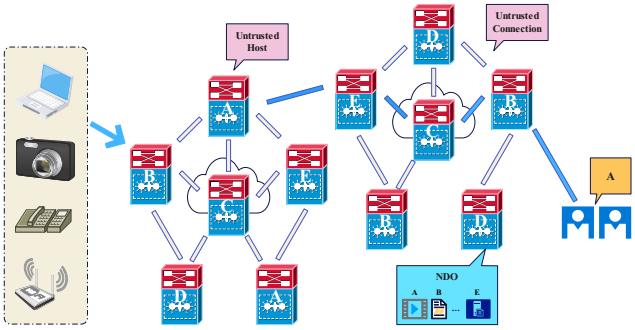


Figure 1: ICN structure

In this context, the content-centric focus of many IIoT applications introduces complexity, requiring a critical review of traditional communication protocols due to the shift towards ICN architecture to ensure they meet the evolving demands of the IIoT ecosystem. Thus, ICN has been adopted

*Corresponding author
lidunshmtu@outlook.com (D. Li); noel.crespi@mines-telecom.fr (N. Crespi); roberto.minerva@telecom-sudparis.eu (R. Minerva); wliang@hnust.edu.cn (W. Liang); kuancli@pu.edu.tw (K. Li); joanna.kolodziej@pk.edu.pl, joanna.kolodziej@nask.pl (J. Kołodziej)
ORCID(s):

in IIoT implementations for its efficient data distribution capabilities for high-demand content [22]. As shown in Fig 1, ICN employs the principle of Named Data Objects (NDOs), incorporates caching at routers, and adopts multicast communication combined with the decoupling of senders and receivers to improve the efficiency of data distribution. Existing ICN-based solutions face notable limitations, including the difficulty of implementing efficient access control mechanisms, which are critical for protecting sensitive industrial data. Furthermore, the lack of integration with advanced encryption frameworks often results in suboptimal privacy protection in these systems [23]. Despite these advantages, the use of ICN requires maintaining complex data structures and codebases. Additionally, since NDOs are often unencrypted, they may unintentionally expose sensitive information, posing a risk to the privacy of data owners [24].

To address these challenges, this work introduces a novel framework that integrates Zero-Knowledge Proof (ZKP), Ciphertext-Policy Attribute-Based Encryption (CP-ABE), ICN, and blockchain technology. Traditional ZKP systems require interaction between the prover and the verifier [25]. In contrast, non-interactive ZKPs allow proof verification without such interaction, making them highly suitable for decentralized environments like the IIoT [26, 27]. Compared to traditional asymmetric encryption techniques, such as RSA, data are required to be encrypted multiple times for each recipient, whilst ZKP systems encrypt data only once as opposed to N times for each recipient, significantly reducing resource consumption and streamlining the encryption process while preserving data security [28]. Additionally, non-interactive ZKP systems provide the IIoT with a more private and trustworthy verification method without needing a trusted third party.

1.1. Motivation

The motivation behind this research is to bridge the gap between theoretical advances in cryptography and its practical applications in IIoT environments. Considering the advantages and limitations of the ICN, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), and blockchain technology, this work aims to effectively address the security challenges and comply with the performance standards within the IIoT framework by strategically integrating CP-ABE with ICN in the IIoT context, thus enabling efficient and distributed data sharing while protecting user privacy through strict access control mechanisms. Furthermore, a non-interactive ZKP protocol called the Distributed Publish-Subscribe Industrial Internet of Things (DPS-IIoT) is innovatively integrated within the CP-ABE framework, assuring the authenticity of secret keys, significantly minimizing the bandwidth consumption typically associated with ineffective access control [29]. Specifically, the contributions of this research are as follows.

- This work presents a ZKP-based protocol, integrated with CP-ABE, which efficiently authenticates user attributes and reduces bandwidth consumption by filtering out unauthorized data requests in IIoT systems.
- work introduces the DPS-IIoT model, leveraging a Publish/Subscribe approach to ensure scalability and efficient data distribution, strategically employing ICN to minimize redundant data transmission and optimize bandwidth utilization.
- This work implements Hyperledger Fabric to store replicated copies of access policies and develop access control mechanisms using ZK-CP-ABE, executed through smart contracts (chain code). These mechanisms provide robust data security, verifiability, and scalability while enabling efficient and tamper-proof access management.

The remainder of this work is organized as follows. Section 2 presents the related work, the system model is presented in Section 3, and details of the proposed ZK-CP-ABE scheme are presented in Section 4. The experimental results are analyzed in Section 5 including insights into the practical implications, and finally, concluding remarks and future directions in Section 6.

2. Related Work

This section reviews the integration of CP-ABE and blockchain technologies in IIoT, focusing on three main aspects: CP-ABE application in IoT in section 2.1, the combination with blockchain in section 2.2, and the role of ICN under IIoT scenarios in section 2.3.

2.1. Attribute-Based Encryption with IoT

CP-ABE integration in IIoT mainly aims to enhance efficiency in key management, access structuring, and algorithmic complexities. For instance, Li *et al.* [30] introduced a Distributed Publisher-Driven secure data-sharing system for IC-IoT, reducing the communication overhead in CP-ABE systems. In another study, Li *et al.* [31] proposed a verifiable flexible data sharing (VFDS) mechanism, combining CP-ABE with identity-based signature (IBS) for distributed authentication in big-data sharing environments. Zhao *et al.* [32] focused on attribute revocation, proposing an outsourced CP-ABE scheme that maintains fixed ciphertext and key sizes. Zhang *et al.* [33] propose BCAE, a blockchain-based cross-domain authentication scheme for edge computing, enhancing secure identity verification and efficient key agreement for IoT devices through digital certificates, digital signatures, and blockchain technology. Khan *et al.* [34] addressed the limitations of traditional consensus mechanisms in private blockchains by proposing B-LPoET, a scalable and efficient multithreaded approach. This innovative consensus strategy informs our methodology for integrating blockchain with CP-ABE to optimize performance in IIoT contexts. Vanga *et al.* [35] suggested an RSA-based CP-ABE scheme with constant key and ciphertext size. Finally, Hao *et al.* [36] developed a CP-ABE system supporting entirely hidden attribute-based access policies using a garbled Bloom filter.

2.2. Access Control with Blockchain

Integrating blockchain technology with access control mechanisms has brought about innovative solutions. For instance, Wang *et al.* [37] combined Ethereum and ABE for secret critical supervision and fine-grained data access control. Fan *et al.* [38] utilized blockchain for recording access policies and implemented a user self-authentication system. Then, a novel integration of blockchain and CP-ABE was proposed in [39], addressing challenges related to blockchain regulation and privacy protection. Zhang *et al.* [40] combined ABE with blockchain in IoT and cloud computing environments, using byzantine fault-tolerant mechanisms for faster consensus. Zhang *et al.* [41] introduced a blockchain and zk-SNARK-based framework for privacy-preserving authentication and decentralized information sharing in VANETs. The use of pseudonym-based participation and IPFS ensures secure and scalable data management, while zk-SNARK verifies task integrity without exposing private information. However, its focus on vehicular networks limits broader applicability to IIoT scenarios, and the computational demands of zk-SNARK may challenge resource-constrained systems. Gebremariam *et al.* [42] developed a blockchain-enabled framework that enhances malicious node detection in IoT-WSNs, utilizing federated learning to classify and secure transactions against attacks. Han *et al.* [43] developed an innovative ABAC model, focusing on auditable access control to enhance privacy within IoT environments.

2.3. ICN with IoT

The application of ICN in IoT is an evolving research field. ICN enhances the availability of IoT data through distributed data caching while introducing new challenges in the authentication field. Xue *et al.* [44] explored the impacts of EDOS attacks in CP-ABE encrypted cloud systems. Meanwhile, Salvador *et al.* [45] introduced an innovative architecture merging CP-ABE's adaptability with symmetric key encryption's efficiency, aiming for secure data transfer and privacy. While current research demonstrates significant advancements in integrating CP-ABE, blockchain, and ICN within IoT environments to enhance security, efficiency, and scalability, a critical need remains for further exploration into optimized, cohesive solutions that address IIoT systems' rapidly evolving and specific challenges. Table 1 summarizes the key features of the existing studies discussed in this section, providing a clear comparison with the proposed framework.

3. System Model

This section describes the proposed asynchronous distributed network, DPS-IIoT, which combines the core principles of ICN with an advanced framework for content dissemination. The applicability of DPS-IIoT spans several critical IIoT domains, such as smart manufacturing, healthcare monitoring, and supply chain management. These applications benefit from secure data sharing, enhanced scalability, and real-time processing enabled by the integration of ICN, CP-ABE, and blockchain technologies.

3.1. Entity definition

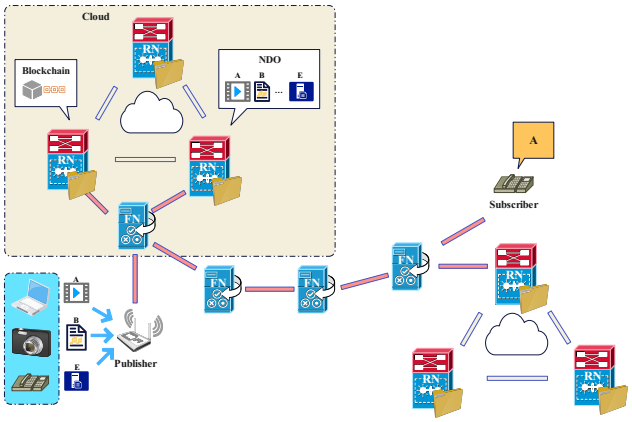


Figure 2: Entity definition of DPS-IIoT architecture

The architecture of the DPS-IIoT consists of five critical elements: the Publisher, responsible for data issuance and key generation; the Rendezvous Node, serving as the system's directory and managing key distribution; the Forwarding Node, facilitating data transit; the Subscriber, as the end consumer of information, validating and using keys for secure access; and the Blockchain, which ensures tamper-proof storage and validation of access policies to fortify the network's security and integrity, as shown in Fig 2.

Device (D): In the IIoT ecosystem, the device, represented as D, is the source of data generation, producing Named Data Objects (NDO_i). Each NDO_is is distinctively tagged within a specified namespace $\mathcal{N}$, playing a critical role in the network's data dynamics. These NDO_is can be strategically duplicated across various nodes within the system, a measure that significantly boosts the network's redundancy and resilience.

Publisher (P): The Publisher, denoted as P, is central in structuring the IIoT landscape. It exerts control over the namespace $\mathcal{N}$ and meticulously formulates access control policies, represented as Π. When these policies are coupled with the NDO_i, they facilitate controlled dissemination of information towards Rendezvous Nodes, thereby effectively regulating access to the data. For instance, in a smart factory setting, the P could represent an IoT-enabled machine sharing real-time operational data, ensuring secure access by authorized personnel or systems only.

Rendezvous Node (RN_k): The Rendezvous Node, labeled as RN_k, serves as an essential intermediary within the architecture. It plays a dual role: acting as a resolver for NDO_i and a temporary guardian of these data objects. Tasked with implementing encryption by predefined policies Π, the Rendezvous Node ensures secure and effective policy enforcement. As an integral component of the blockchain network, the Rendezvous Node oversees secure policy execution and ensures efficient content navigation.

Table 1
Comparative Analysis of Related Work

Study	Key Features	Limitations
Li *et al.* [30]	Introduced a Distributed Publisher-Driven secure data-sharing system to reduce communication overhead in CP-ABE systems.	Lacks dynamic attribute revocation and scalability for rapidly changing IIoT environments.
Zhao *et al.* [32]	Proposed an outsourced CP-ABE scheme with fixed ciphertext sizes, enhancing performance in resource-constrained environments.	Limited scalability and higher dependency on trusted third parties, unsuitable for large-scale IIoT deployments.
Wang *et al.* [37]	Combined Ethereum and ABE for fine-grained data access control with secret critical supervision.	Introduces high computational overhead and latency due to the inherent complexity of blockchain and ABE integration.
Zhang *et al.* [40]	Integrated ABE with blockchain using Byzantine fault-tolerant mechanisms for faster consensus and improved reliability in cloud environments.	Primarily focuses on cloud computing and lacks adaptation to IIoT-specific requirements, such as low-latency processing.
Xue *et al.* [44]	Explored EDOS attack impacts and proposed enhancements in CP-ABE encrypted cloud systems.	Does not incorporate robust mechanisms for ICN integration or address real-time data sharing challenges in IIoT.
Proposed Framework	Integrates CP-ABE, ICN, and blockchain to achieve scalability, efficient data sharing, and enhanced security through non-interactive ZKP.	Implementation complexity requires comprehensive deployment strategies in highly dynamic IIoT networks.

Forwarding Node (FN_l): The Forwarding Node, identified as FN_l, manages and optimizes the network's transmission architecture. It ensures the smooth conveyance of NDO_i towards the designated Rendezvous Nodes, facilitating effective data dissemination. FN_l can be utilized in healthcare IoT systems to deliver critical patient data to specialized analysis nodes without delays, ensuring both reliability and security.

Blockchain: The blockchain, integral to the system's security matrix, operates as a distributed ledger $\mathcal{L}$. This ledger $\mathcal{L}$ undergirds the network's structural integrity and security framework. It firmly secures the network's access control processes via smart contracts $\mathcal{SC}$, ensuring that policy management Π is governed by immutable rules ρ_Π and transparent verification protocols $\mathcal{V}_\Pi$. Mathematically, the blockchain's role can be expressed as $\mathcal{L}(\mathcal{SC}, \Pi) \rightarrow \{\rho_\Pi, \mathcal{V}_\Pi\}$, signifying its foundational function in instilling a robust layer of trust and reliability across the network's operations.

Subscriber (Σ): Subscribers, denoted as Σ, are dynamically engaged with the network, actively soliciting particular Named Data Objects (NDO_i) from Rendezvous Nodes via requests tagged as msg_{sub}. These Σ entities are tuned into receiving relevant updates and content that align with their specific interests in the namespace $\mathcal{N}$, highlighting their proactive involvement in the network's data exchange ecosystem.

3.2. Workflow

The architecture of DPS-IIoT is intricately designed to orchestrate secure and efficient data management. The proposed architecture finds broad applicability across IIoT scenarios. In smart factories, it secures data exchange between machinery under strict access controls. In healthcare, it enables the safe sharing of patient information among authorized parties. With blockchain and ZKP integration, it strengthens security in supply chain management by ensuring stakeholder authentication and traceability. Additionally, the DPS-IIoT model supports intelligent transportation systems, facilitating secure vehicle data sharing to enhance traffic safety and efficiency while preserving user privacy. As shown in Fig 3, the system's workflow is carried out in four phases.

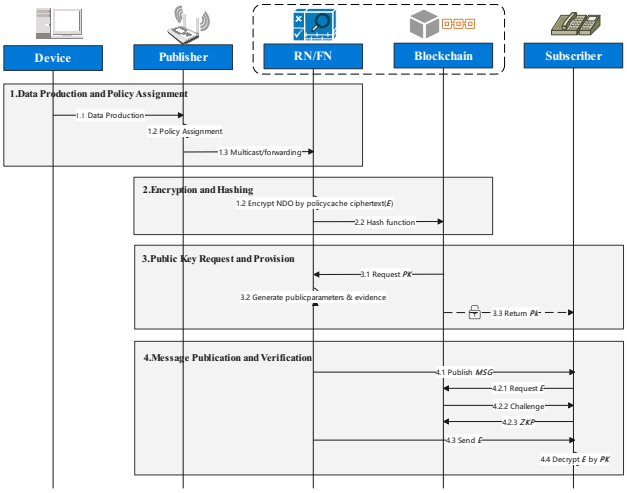


Figure 3: Workflow of DPS-IIoT

Step 1: Data Production and Policy Assignment.

- Produce data: Let D be the data produced by a device, such that $D \in \mathcal{D}$, where $\mathcal{D}$ is the set of all possible data.
- Assign naming scope, make policy: A policy π is defined as a function $\pi : \mathcal{D} \rightarrow \mathcal{P}$, where $\mathcal{P}$ is the

set of all possible policies. The publisher assigns the data a naming scope N and policy $\pi(D)$.

- Multicast/Forwarding: The data D is multicast or forwarded to nodes in the network $\mathcal{N}$, where $\mathcal{N}$ is the set of all nodes.

Step 2: Encryption and Hashing.

- Encrypt NDOs by policy, cache ciphertext(E): The encrypted data E is given by $E = \text{Enc}_{\pi}(D)$, where Enc is the encryption function parameterized by policy $\pi(D)$.
- Put HASH: A hash function $h : \mathcal{D} \rightarrow \mathcal{H}$ maps data D to a hash value $h(D)$, where $\mathcal{H}$ is the set of all possible hashes. The hash of the encrypted data is $h(E)$.

Step 3: Public Key Request and Provision.

- Request PK: A subscriber requests the public key PK, where $PK \in \mathcal{K}$ and $\mathcal{K}$ is the set of all possible public keys.
- Generate public key parameters + evidence: Parameters θ and evidence ϵ are generated, where $\theta, \epsilon \in \mathcal{K}$.
- Return PK: The public key PK is returned, $PK = f(\theta, \epsilon)$, where f is a function generating PK from parameters θ and evidence ϵ.

Step 4: Message Publication and Verification.

- Publish MSG: Let M be a message published, $M \in \mathcal{M}$, where $\mathcal{M}$ is the set of all possible messages.
- Request E: The encrypted data E is requested by the subscriber.
- Challenge: A challenge C is issued, $C \in \mathcal{C}$, where $\mathcal{C}$ is the set of all possible challenges.
- ZKP: A zero-knowledge proof function $\mathcal{Z}$ confirms that the subscriber can access E without revealing any D or the PK.
- Send E: The encrypted data E is sent to the subscriber after successful verification.
- Decrypt E by PK: The subscriber decrypts the encrypted data E using the public key PK, to retrieve the original data D. This is represented as $D = \text{Dec}_{PK}(E)$, where Dec is the decryption function.

3.3. Search and Retrieval Stage

The search stage in the DPS-IIoT system ensures that data requests are securely resolved and matched with access policies. When a subscriber submits a request for a specific NDO_i) the request, tagged as msg_{sub}, is forwarded to the Rendezvous Node (RN_k). The RN_k checks the request against the predefined access control policies stored on the blockchain. Using ZKP, the subscriber proves the authenticity of their attributes without revealing sensitive details. The process ensures that unauthorized requests are filtered out, thereby enhancing security. If the request matches the access policy, the Rendezvous Node retrieves the corresponding encrypted NDO_i and returns it to the subscriber. The subscriber uses their private key SK to decrypt the content. This mechanism leverages the blockchain for immutable policy verification and ZKP for secure attribute validation, ensuring privacy and efficiency throughout the search and retrieval process.

4. Proposed ZK-CP-ABE Scheme

In this section, we introduce the detailed algorithm design. The protocol for initial identity authentication using non-interactive ZKPs, $Auth(ID_{entity}) \xrightarrow{ZKP} Verified$, is at the basis of the suggested approach. This process obviates the need for traditional public key exchange mechanisms and mitigates the risks associated with private key exposure.

4.1. Optimizing Decryption in CP-ABE Systems for IIoT Environments

Optimizing the decryption process in the ZK-CP-ABE scheme enhances efficiency and scalability in IIoT systems. By reducing computational overhead and introducing pre-decryption authentication, the scheme minimizes resource wastage and ensures real-time processing, critical for resource-constrained IIoT environments. In standard CP-ABE frameworks, the decryption model, denoted as $\mathcal{D}(C, PK, SK)$, where C represents ciphertext and PK and SK are the public and private keys, respectively, mandates the complete download of ciphertext C aligned with the access policy $\mathcal{P}$. This protocol, while ensuring policy adherence, leads to high computational and bandwidth utilization, particularly when $\mathcal{D}(C, PK, SK)$ fails due to critical errors, resulting in wasted data transmission (Δ_{trans}) and decryption efforts ($\Delta_{decrypt}$). The algorithm designed for the IIoT ecosystems introduces mathematical refinements to mitigate these resource expenditures. It achieves this through two pivotal adaptations.

4.1.1. Hash-Based Data Encryption

Instead of encrypting the entire data D, the algorithm computes a hash $H(D)$ and encrypts it, i.e., $\mathcal{E}(H(D), \mathcal{A})$, where $\mathcal{A}$ represents the set of attributes. This modification significantly lowers the volume of encrypted data (Δ_{vol}), optimizing bandwidth usage.

4.1.2. Pre-Decryption Authentication

Before decryption, the algorithm embeds an essential authentication phase, $\mathcal{A}(C, PK, SK)$. Employing a ZKP mechanism validates the legitimacy of the decryption request. This pre-validation step is crucial in circumventing the transmission of encrypted data $\mathcal{E}$ when validation fails, thereby conserving resources.

4.2. System Setup and Key Generation

The setup of DPS-IIoT starts by generating a large prime p, selecting a bilinear group G_0 of prime order p, and

defining a bilinear pairing operation $e : G_0 \times G_0 \rightarrow G_1$. From this group, a generator g is chosen by ensuring it is a primitive root that can generate all elements of the group G_0 through its powers, foundational for cryptographic operations. The hash function $H : 0,1^* \rightarrow G_0$ can map any given attribute (expressed in binary) to an element in the group. Subsequently, two random numbers $\alpha, \beta \in \mathbb{Z}_p$ are selected—where $\mathbb{Z}_p$ denotes the multiplicative group of integers modulo p—and the system parameters $h = g^\beta$ and $u = e(g,g)^\alpha$ are computed as shown in Eq 1.

$$PK = \{G_0, g, h, u\}, MK = \{\alpha, \beta\} \tag{1}$$

4.3. Generation of User-Specific Keys and Evidence

The design of this setup fulfills two key objectives: firstly, it computes the private key SK by utilizing initial parameters and user-specific attributes; secondly, it generates public proof for the SK to enable ZKP validation. Let $Y = \{y_1, y_2, \ldots, y_m\}$ symbolize a set of weighted attributes critical for decryption. The algorithm selects a random value r from the finite field $\mathbb{Z}_p$. Each attribute y_j in Y independently assigns a unique random value r_j from $\mathbb{Z}_p$. The value of D is specifically computed as $D = g^{(\alpha+r)/\beta}$, where α and β are the master key parameters, and r is the randomly selected value. This computation ensures that D is unique to the user and incorporates both the randomness of r and the cryptographic strength of the master key parameters. The algorithm's pivotal step involves calculating the SK and integrating these elements per a specific formula. The SK calculation is defined in Eq 2.

$$SK = \Big\{ D = g^{(\alpha+r)/\beta}, \quad \forall y_j \in Y : \quad D_j = g^r \cdot H(y_j)^{r_j}, D'_j = g^{r_j} \Big\} \tag{2}$$

Algorithm 1 Generate Key and Evidence

Require: $Y = \{y_1, y_2, \ldots, y_m\}$ (weighted attributes), $MK = \{\alpha, \beta\}$ (master key)
Ensure: SK (private key), EV (evidence for SK)

```
Select a random value r from the finite field Z_p
Initialize SK = { }
for each attribute y_j in Y do
    Select a unique random value r_j from Z_p
    Compute D_j = g^r · H(y_j)^{r_j}
    Compute D'_j = g^{r_j}
    Add D_j and D'_j to SK
end for
Compute D = g^{(α+r)/β} and add to SK
Choose large primes p and q, set n = p · q
Select length t for evidence EV
Compute X = |Hash256(SK)[0, ..., t]|^2
Formulate EV = {X, n = p * q}
return SK, EV
```

As Algorithm 1 shows, the subsequent algorithm generates evidence supporting the possession of the private key SK. Let n be a large composite number, specifically the product of two distinct large primes, denoted by p and q, such that $n = p \cdot q$. The length of the evidence EV in bytes is represented by t, where the system's desired security level chooses both n and t. The relationship is formalized in Eq 3.

$$\begin{aligned} X &= \left(\sum_{i=0}^{t} \text{Hash256}(SK)_i \right)^2 \\ &= \left(\sum_{i=1}^{t} y_i \right)^2 = \sum_{i=1}^{t} y_i^2 \\ &= \sum_{i=1}^{t} x_i \\ EV &= \{X, n = pq\} \end{aligned} \tag{3}$$

4.4. Encryption of Data under Access Control Policies

Initially, a hash function $\mathcal{H}$ is applied to the dataset M to generate a data summary $M_{meta} = \mathcal{H}(M)$. This technique is noted for its effectiveness in enhancing storage and reducing bandwidth during data transmission. The encryption algorithm's primary function is to encrypt the plaintext M with an access structure $\mathcal{T}$, represented by a tree.

Algorithm 2 Encrypt Data

Require: M (plaintext), A (access structure), $PK = \{G_0, g, h, u\}$ (public key)
Ensure: CT (ciphertext)

```
Compute M_meta = H(M) using hash function H
Initialize access tree T based on A
Select a random secret s from Z_p
Define polynomial q_R at root R with q_R(0) = s
for each node x within the tree T do
    if x equals the root node R then
        Proceed to next node
    else
        Set q_x(0) equal to the value of q_{parent of x} evaluated at the index of x
        Randomly select d_x points to fully establish the polynomial q_x
    end if
end for
Compute C̄ = M · e(g,g)^{α·s} and C = h^s
for each leaf node l in T do
    Compute C_l = g^{q_l(0)}
    Compute C'_l = H(att(l))^{q_l(0)}
end for
Assemble ciphertext CT = {T, C̄, C, {C_l, C'_l}_{∀l∈Leaves(T)}}
return CT
```

As Algorithm 2 shows, the encryption process initiates at the root node R of $\mathcal{T}$ and proceeds recursively

to each node x, where it constructs a unique polynomial q_x. Utilizing Lagrange interpolation, defined as $f(x) = \sum_{i=1}^{d} f(x_i)\left(\prod_{j=1,j\neq i}^{d} \frac{x-x_j}{x_i-x_j}\right)$, the polynomial q_x at each node x is defined with a maximum degree d_x equal to the threshold of the node, k_x-1. The encryption process initiates at the root node R, where a random secret s is chosen from the set $\mathbb{Z}_p$. This secret establishes the initial condition of the polynomial q_R at R by setting $q_R(0)$ equal to s. For each subsequent node x within the tree $\mathcal{T}$, the zero value of their respective polynomial $q_x(0)$ is determined based on the value of the polynomial at their parent node, specifically as $q_{\text{parent of } x}(\text{index of } x)$. To completely define the polynomial q_x at each node x, d_x distinct points are randomly selected, where d_x denotes the degree of the polynomial at node x. During decryption, the user's private key attributes, denoted as inputs to these polynomials, allow for the reconstruction of plaintext M through calculated interpolation. With L representing the set of leaf nodes in $\mathcal{T}$, the ciphertext CT is computed as outlined in Eq 4.

$$\begin{aligned} CT =& \mathcal{T}, \bar{C} = M \times e(g,g)^{\alpha \times s}, C = h^s \\ & \forall l \in L : C_l = g^{q_l(0)}, C_l' = H(\text{att}(l))^{q_l(0)} \end{aligned} \tag{4}$$

4.5. Verification of Secret Key Authenticity

The $Proof$ algorithm, incorporating the Feige-Fiat-Shamir (FFS) protocol, adopts a mathematical strategy to confirm the existence of a secret key SK without disclosing the corresponding details. Specifically, it allows the prover P (the data requester) to authenticate their identity via SK before requesting encrypted data from the storage server, optimizing bandwidth usage as shown in Algorithm 3.

Algorithm 3 Zero-Knowledge Proof Verification

Require: SK (secret key), EV (evidence)
Ensure: Boolean value indicating proof validity
1: Prover P generates a random variable $r \in (0, n)$
2: Prover P computes $a = f(r, SK)$
3: Initialize verification sequence e by the Verifier V
4: V issues a challenge based on EV
5: **for** $i = 1$ to t **do**
6: Generate $e_i \in \{0, 1\}$ randomly
7: **end for**
8: Prover P responds with $ANS = r \cdot \prod_{i=1}^{t} y_i^{e_i} \mod n$
9: Verifier V checks the response ANS
10: Compute $\lambda = \prod_{i=1}^{t} EV.x_i^{e_i} \mod n$
11: **if** $ANS^2 \equiv a \cdot \lambda \mod n$ **then**
12: **return** True
13: **else**
14: **return** False
15: **end if**

In the verification process, the prover P initiates by selecting a random number r within the range $(0, n)$, where n is a publicly known parameter about the evidence variable EV. Next, using a function f based on the secret key SK and the random integer r, P computes a specified value a. This computation ensures that data access requests can only be processed after verification. The formalization of this procedure aims to minimize unnecessary data transmission by granting access exclusively to requests that successfully pass this authentication phase, as shown in Eq 5.

$$Initialize(EV) = \{r, a | r \in (0, n), a \equiv r^2 \mod n\} \tag{5}$$

Further, labeled as V (who may represent either the data owner or the entity overseeing storage services), the verifier constructs a sequence of variables e derived from the maintained evidence EV associated with the secret key SK. Subsequently, V initiates a series of challenges, as shown in Eq 6.

$$\begin{aligned} Challenge(EV) &= GenerateRandomSequence(seed, t) \\ &= \{e_1, e_2, ..., e_t\}, \text{ where } e_t \in \{0, 1\} \end{aligned} \tag{6}$$

Upon receipt of the challenge, the prover P computes a response, denoted by ANS, utilizing the private key. This response is then returned within a single round of communication, as formulated in Eq 7.

$$ANS = r \prod_{i=1}^{t} y_i^{e_i} \mod n \tag{7}$$

The verifier, V, assesses the response ANS. This scrutiny is performed by the evaluation criteria EV and the established public parameters, as shown in Eq 8. The verification process effectively verifies decryption requests by combining ZKP, thereby reducing unnecessary bandwidth consumption and computational load, and improving model performance. The verifier V can replicate the $Challenge$ k times to align with the system's prescribed security threshold, ensuring the robustness of the verification process. If any challenge is not met within a round, the proof procedure is terminated, preventing unauthorized decryption attempts and optimizing system performance.

$$\begin{aligned} Check(ANS, EV) &= \begin{cases} 1, ANS^2 \equiv a\lambda \mod n \\ 0, ANS^2 \neq a\lambda \mod n \end{cases} \\ \lambda &= \prod_{i=1}^{t} EV.x_i^{e_i} \mod n \end{aligned} \tag{8}$$

4.6. Decryption of Ciphertext to Obtain Metadata

The decryption algorithm, denoted as Dec, is formulated as a recursive procedure. In the context of the encryption phase, the access policy is articulated through a tree structure. Correspondingly, we instantiate a recursive algorithm, $DecNode(CT, SK, x)$ commences its decryption process from the root and proceeds through successive layers of the tree, as shown in Algorithm 4.

Algorithm 4 Decryption Process

Require: CT (Ciphertext), SK (Secret Key), PK (Public Key)
Ensure: M_{meta} (Decrypted Metadata)

function DecNode(CT, SK, x)
  if x matches a leaf node **then**
    $i \leftarrow attribute(x)$
    return $\frac{e(D_i, C_x)}{e(D'_i, C'_x)}$ ▷ $D_i = g^r \cdot H(i)^{r_i}, C_x = h^{q_x(0)}, D'_i = g^{r_i}, C'_x = H(i)^{q_x(0)}$
  else
    Initialize $F_x \leftarrow 1$
    for each child node z of x **do**
      $F_z \leftarrow$ DecNode(CT, SK, z)
      Update F_x using F_z and Lagrange interpolation
    end for
    return F_x
  end if
end function
$\mathcal{T} \leftarrow$ Extract tree structure from CT
$\bar{C}, C \leftarrow$ Extract ciphertext components from CT
$R \leftarrow$ Root of tree $\mathcal{T}$
$M_{meta} \leftarrow$ DecNode(CT, SK, R)
return M_{meta}

The inputs to this algorithm are the ciphertext $CT = (\mathcal{T}, \bar{C}, C)$, the private key SK, which is associated with a specific set of attributes, and a node x from the tree $\mathcal{T}$. If x corresponds to a leaf node, where $i = \text{att}(x)$, the decryption is defined by the subsequent calculation as illustrated in Eq 9.

$$\begin{aligned} DecNode(CT, SK, x) &= \frac{e(D_i, C_x)}{e(D'_i, C'_x)} \\ &= \frac{e(g^r \times H(i)^{r_i}, h^{q_x(0)})}{e(g^{r_i}, H(i)^{q_x(0)})} \\ &= e(g, g)^{r \times q_x(0)} \end{aligned} \tag{9}$$

Consider a non-leaf node x. For each child node z of x, the function $DecNode$ is executed independently to determine F_z. Define S_x as the set containing all such child nodes z, where the cardinality of S_x is denoted by k_x. The condition $k_x > 0$ necessitates that $F_z \neq 1$. Conversely, if $k_x = 0$, it follows that $F_z = 1$. The formulation of F_x is represented as Eq 10.

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z^{\Lambda(\text{ind}(x), S'_x)}(0) = \tilde{e}(g, g)^{r\gamma q_x(0)}, \\ k &= index(x), S'_x = \{ index(z) \mid z \in S_x \} \end{aligned} \tag{10}$$

Finally, the plaintext, denoted as M, is deciphered utilizing the ciphertext key CK by Eq 11.

$$\begin{aligned} \tilde{C} / (e(C, D)/A) &= \tilde{C} / \left(e\left(h^s, g^{(\alpha+r)/\beta}\right) / e(g, g)^{rs} \right) \\ &= e(g, g)^{rqR(0)} = e(g, g)^{rs} = M \end{aligned} \tag{11}$$

5. Experimental Results and Analysis

This section presents a comprehensive comparative analysis of the methods introduced above, beginning with the details of the experimental settings in Section 5.1. The analysis evaluates the proposed algorithm and system across three key dimensions: the algorithm's performance is as assessed in Section 5.3, the scalability performance is evaluated in Section 5.4, and the system throughput is examined in Section 5.5.

5.1. Experimental Settings

In this work, a comprehensive set of experimental configurations is carefully planned to demonstrate the system's ability to accommodate large volumes of traffic while minimizing bandwidth utilization. The blockchain is implemented using Hyperledger Fabric to store access control policies and validate user requests via smart contracts. For experimental evaluation, the hardware configuration comprises two computer servers: the first equipped with a 3.60GHz i7-7700 CPU and 8GB of RAM, and the second furnished with an i7-7500U CPU at 2.90GHz coupled with 16GB RAM. Additional apparatus includes a 1.5GHz Raspberry Pi with 4GB RAM, powered by an ARM A72 CPU. The dataset used in the experiments is simulated to model typical IIoT traffic scenarios, including data from smart manufacturing, healthcare, and industrial sensors.

5.2. Robustness Against Attacks

The proposed ZK-CP-ABE scheme significantly enhances security by leveraging non-interactive ZKP for prevalidation to prevent unauthorized access and blockchain for tamper-proof policy enforcement, ensuring robust protection against key forgery, replay attacks, and policy manipulation. The DPS-IIoT system shows resilience against external threats, including DDoS attacks and unauthorized data interception, which are critical for ensuring system availability and data integrity in IIoT environments.

Proof: Let $\mathcal{N}$ represent the DPS-IIoT network. The resilience R against external attacks is modeled as Eq 12.

$$R(\mathcal{N}) = 1 - \exp(-\gamma \cdot \Phi(\mathcal{N})) \tag{12}$$

where γ represents the network defense parameter, which quantifies the strength of the system's defenses against external attacks, and $\Phi(\mathcal{N})$ denotes the probability distribution of attack vectors, which defines the likelihood of different types of attacks occurring in the system. Here, $\mathcal{N}$ represents the DPS-IIoT network, the subject of our security analysis.

5.3. Algorithm Performance Evaluation

This section presents a comparative evaluation of the ZK-CP-ABE scheme against advanced CP-ABE models tailored for industrial applications. Key research efforts in this domain focus on improvements like minimizing secret key sizes, symbolized as $\delta(SK)$ [46], enhancing policy and access control frameworks $\mathcal{F}_{AC}$ [47], and reducing the computational complexities Θ_{enc} and Θ_{dec} of encryption and

decryption processes [48]. Moreover, the strategy incorporates a distributed key distribution mechanism $\mathcal{D}_{CA}$ using multiple Certificate Authorities (CAs) to enhance system robustness ρ.

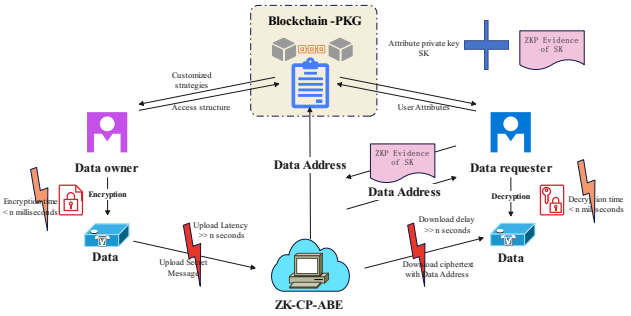


Figure 4: Design Principle of ZK-CP-ABE

As the IIoT continues to advance with greater cloud integration and the expansion of online services, the demand for bandwidth on cloud infrastructures, denoted as β_{cloud}, has significantly increased. This rise in β_{cloud} is disproportionate to the increases in computational γ_{comp} and storage σ_{store} capacities. Addressing this imbalance requires a strategy beyond mere algorithmic refinement $\mathcal{R}_{alg}$. As Fig 4 shows, the proposed method extends traditional CP-ABE enhancements by integrating a ZKP mechanism, denoted as $\mathcal{ZKP}_{enc-dec}$, within the encryption-decryption process. This approach discreetly verifies the existence of a user's private key SK, mitigating bandwidth consumption $\Delta\beta_{unprod}$ from ineffective access control queries. Furthermore, $\mathcal{ZKP}_{enc-dec}$ enables a shift towards a bandwidth-efficient symmetric encryption model in the CP-ABE framework, signifying a significant leap in data security for IIoT systems. To quantify the bandwidth efficiency $\eta_{bandwidth}$ of the proposed algorithm, a comparative analysis is performed against the benchmarks in [46], [47], and [48], focusing on bandwidth utilization improvements $\Delta\eta_{bandwidth}$ and performance enhancement $\Delta\rho_{performance}$. The experimental framework is outlined as follows.

5.3.1. Computational Analysis Relative to Attribute Policies

For a set of attributes $\mathcal{A}$, with the cardinality $|\mathcal{A}| \in [10, 20, ..., 90, 100]$, we assess the computational overhead $C_{\text{overhead}}(f, \mathcal{A})$ for functions $f \in \{GenKey, Enc, Dec\}$. The study reveals a direct correlation $C_{\text{overhead}}(f, \mathcal{A}) \propto |\mathcal{A}|$, emphasizing the computational demand's dependency on the number of attributes within the policy. By optimizing the number and relevance of attributes, the system can maintain computational efficiency while meeting security requirements.

5.3.2. Bandwidth Consumption Analysis for Varying Data Sizes

Let M represent the size of plaintext data, varying within a specified range. The bandwidth requirement $B_{\text{alg}}(M)$ for each data magnitude M is evaluated to assess how the ABE algorithm adapts to changes in data size. The function $B_{\text{alg}}(M)$ provides a quantitative understanding of the algorithm's scalability and efficiency.

5.3.3. Ratio Analysis of Operational Duration to Transmission Latency

Fixing the attribute count at 50, the operational duration $T_{\text{op}}(M)$ and transmission latency $T_{\text{trans}}(M)$ are analyzed for varying data sizes $M \in [2, 4, ..., 512, 1024]$ MB. The ratio $R_{\text{efficiency}}(M) = T_{\text{op}}(M)/T_{\text{trans}}(M)$ quantifies the balance between processing and transmission efficiency, offering a critical metric for assessing algorithm performance across different data sizes. The analysis reveals that while the operational duration increases linearly with data size, the transmission latency exhibits a more gradual rise.

5.4. Scalability performance evaluation

The conclusive statistics are shown in Fig 5 and Fig 6. The advantages of our approach are evident from the following illustrations.

5.4.1. Algorithmic Complexity Analysis

Evaluating the functions $GenKey()$, $Enc()$, and $Dec()$ within our framework reveals a minimal operational time variance Δt_{op} compared to alternative algorithms. This variance is quantified as $\Delta t_{\text{op}}(f) \approx$ a few milliseconds (ms), for each function f in the set $\{GenKey, Enc, Dec\}$. For benchmarking, equivalent tests based on Ref [49, 29, 22] were deployed on a similarly configured PC, and parallel tests were performed using identical clients and logic. This marginal discrepancy underscores the comparable efficiency of our framework's cryptographic operations.

5.4.2. Bandwidth Utilization Efficiency

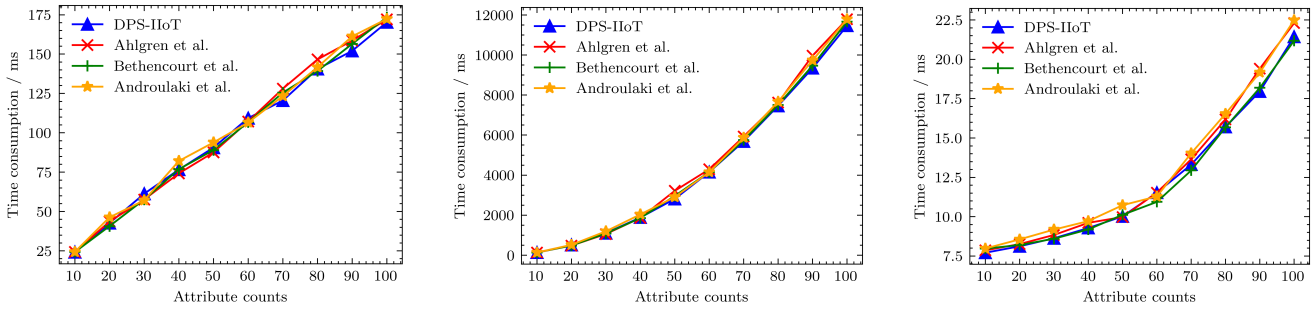
We define $B_{\text{alg}}(M)$ as the bandwidth utilization for processing plaintext of size M. The proposed algorithm markedly optimizes bandwidth consumption, formulated as $B_{\text{alg}}(M) = B_{\text{ZKP}} + \mathcal{O}(1)$ for larger M values. In this context, B_{ZKP} signifies the consistent bandwidth expenditure associated with ZKP challenges, irrespective of the plaintext size.

5.4.3. Proportional Analysis of Time Consumption

As the size of the plaintext data M expands, there is a notable rise in the proportion of CP-ABE operational time relative to the transmission time, symbolized as $R_{CP-ABE}(M)$. Particularly for more extensive data sizes, $R_{CP-ABE}(M)$ tends to reach close to 100%. Despite this increase, the time efficiency of our algorithm consistently maintains a stable and moderate pace.

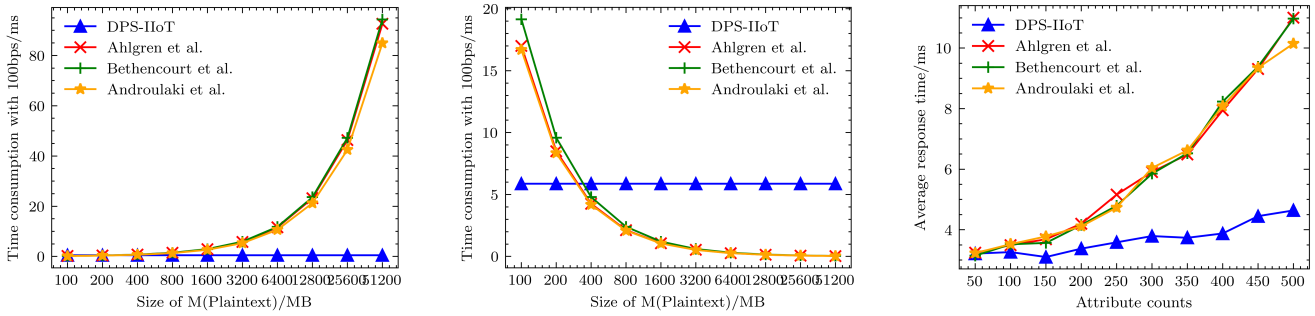
5.5. System Performance Evaluation

The blockchain system is deployed on $PC1$ using multiple virtual machines, each equipped with a customized chain code (smart contract). To emulate a realistic IC-IoT environment, MQTT is adopted as the communication protocol, and the broker, EMQ, is deployed on $PC1$ within a Docker container. On $PC2$, subscriber and publisher clients



(a) The performance of $GenKey()$ (b) The performance of $Enc()$ (c) The performance of $Dec()$

Figure 5: Comparative analysis of time consumption between the DPS-IIoT and selected baseline references



(a) Bandwidth consumption of algorithm execution (b) Proportional comparison of CP-ABE time cost to data transmission time (c) The average response time for varying numbers of concurrent clients

Figure 6: Comparative analysis of bandwidth consumption between the DPS-IIoT and selected baseline references

are implemented to interact via the MQTT protocol, with each client possessing the ability to invoke the chain code within the blockchain. Additionally, a client is deployed on a Raspberry Pi to emulate a device, programmed to periodically upload data and maintain transmission in adherence to the MQTT protocol. The results shown in Fig 6 capture the average response time as the number of concurrent clients increases. The simulation utilizes MQTT based architecture, EMQ agent deployed on Docker, and smart contract interaction.

To assess the system's throughput capabilities in a distributed context, experiments were conducted simulating various counts (denoted as N) of concurrent subscriber/publisher clients accessing the blockchain system over a predefined duration to evaluate the average response time. Specifically, N is varied within the set $\{50, 100, \ldots, 500\}$. In the context of CP-ABE, the attribute count for testing is consistently set at $K = 50$, and the data block size is fixed at $S = 512KB$. The results are shown in Fig 6c.

6. Conclusions and Future Work

The ICN model aims to enhance the network architecture to perform more effective content access and distribution, while effectively solving the interruption and high traffic scenarios in network communication. This work introduces the ZK-CP-ABE algorithm for the IIoT and the DPS-IIoT system, forming a scalable and reliable access control framework. The proposed ZK-CP-ABE algorithm uniquely integrates ZKP protocols to assign secret keys tied to specific user attributes, ensuring precise access control and significantly reducing bandwidth usage. By combining non-interactive ZKP, CP-ABE, and blockchain technology, this approach addresses critical challenges in IIoT, including privacy preservation, security, and scalability, which are inadequately addressed in existing solutions. Experiments and comparative analysis confirm that the proposed methods can significantly reduce the use of network bandwidth while maintaining a solid level of throughput.

Future research includes the following aspects:

1. Enhancing the scalability and efficiency of blockchain technology within the IIoT is a crucial area of research, involving crafting innovative consensus algorithms designed to speed up transaction processing and minimize latency.
2. Integrating the proposed system with cutting-edge technologies like 5G, edge computing, and AI promises to create a more cohesive and high-performing IIoT network, enhancing overall system efficiency and connectivity.
3. Implementing and rigorously testing the system in actual industrial environments will provide valuable insights into its real-world performance, adaptability, scalability, and security.

4. Exploring the application of the ZK-CP-ABE algorithm and the DPS-IIoT framework across a range of industrial domains will help evaluate the versatility and effectiveness in various operational settings.

References

[1] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, Y. Wang, A survey of internet of things communication using icn: A use case perspective, Computer Communications 142-143 (2019) 95–123.

[2] S. Zhou, K. Li, Y. Chen, C. Yang, W. Liang, A. Y. Zomaya, Trustbcfl: Mitigating data bias in iot through blockchain-enabled federated learning, IEEE Internet of Things Journal (2024).

[3] W. Liang, Y. Yang, C. Yang, Y. Hu, S. Xie, K.-C. Li, J. Cao, Pdpchain: A consortium blockchain-based privacy protection scheme for personal data, IEEE Transactions on Reliability (2022).

[4] D. Li, D. Han, N. Crespi, R. Minerva, K.-C. Li, A blockchain-based secure storage and access control scheme for supply chain finance, The Journal of Supercomputing 79 (1) (2023) 109–138.

[5] J. Li, D. Han, D. Li, H. Li, Blockchain and or based data sharing solution for internet of things, in: International Conference on Blockchain and Trustworthy Systems, Springer Nature Singapore Singapore, 2023, pp. 116–127.

[6] W. Shao, Y. Wei, P. Rajapaksha, D. Li, Z. Luo, N. Crespi, Low-latency dimensional expansion and anomaly detection empowered secure iot network, IEEE Transactions on Network and Service Management (99) (2023) 1–1.

[7] J. Long, W. Liang, K.-C. Li, Y. Wei, M. D. Marino, A regularized cross-layer ladder network for intrusion detection in industrial internet of things, IEEE Transactions on Industrial Informatics 19 (2) (2022) 1747–1755.

[8] C. Diao, D. Zhang, W. Liang, K.-C. Li, Y. Hong, J.-L. Gaudiot, A novel spatial-temporal multi-scale alignment graph neural network security model for vehicles prediction, IEEE Transactions on Intelligent Transportation Systems 24 (1) (2022) 904–914.

[9] D. Li, D. Han, B. Xia, T.-H. Weng, A. Castiglione, K.-C. Li, Fabric-gc: A blockchain-based gantt chart system for cross-organizational project management, Computer Science and Information Systems 19 (3) 1213–1240.

[10] H. Li, D. Han, M. Tang, A privacy-preserving storage scheme for logistics data with assistance of blockchain, IEEE Internet of Things Journal (2021).

[11] D. Li, D. Han, T.-H. Weng, Z. Zheng, H. Li, H. Liu, A. Castiglione, K.-C. Li, Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey, Soft Computing 26 (9) (2022) 4423–4440.

[12] H. Liu, D. Han, D. Li, Behavior analysis and blockchain based trust management in vanets, J. Parallel Distributed Comput. 151 (2021) 61–69.

[13] D. Li, D. Han, Z. Zheng, T.-H. Weng, H. Li, H. Liu, A. Castiglione, K.-C. Li, Moocschain: A blockchain-based secure storage and sharing scheme for moocs learning, Computer Standards & Interfaces 81 (2022) 103597.

[14] H. Li, D. Han, C.-C. Chang, Dac4sh: A novel data access control scheme for smart home using smart contracts, IEEE Sensors Journal 23 (6) (2023) 6178–6191.

[15] W. Liang, S. Xie, K.-C. Li, X. Li, X. Kui, A. Y. Zomaya, Mc-dsc: A dynamic secure resource configuration scheme based on medical consortium blockchain, IEEE Transactions on Information Forensics and Security (2024).

[16] H. Li, D. Li, W. Liang, A smart contract-driven access control scheme with integrity checking for electronic health records, Cluster Computing (2024) 1–21.

[17] N. Hu, D. Zhang, K. Xie, W. Liang, K. Li, A. Zomaya, Multi-graph fusion based graph convolutional networks for traffic prediction, Computer Communications 210 (2023) 194–204.

[18] J. Cai, W. Liang, X. Li, K. Li, Z. Gui, M. K. Khan, Gtxchain: A secure iot smart blockchain architecture based on graph neural network, IEEE Internet of Things Journal (2023).

[19] W. Liang, Y. Li, J. Xu, Z. Qin, D. Zhang, K.-C. Li, Qos prediction and adversarial attack protection for distributed services under dlaas, IEEE Transactions on Computers (2023).

[20] S. Zhang, B. Hu, W. Liang, K.-C. Li, A.-S. K. Pathan, A trajectory privacy-preserving scheme based on transition matrix and caching for iiot, IEEE Internet of Things Journal (2023).

[21] Y. Liu, W. Liang, K. Xie, S. Xie, K. Li, W. Meng, Lightpay: A lightweight and secure off-chain multi-path payment scheme based on adapter signatures, IEEE Transactions on Services Computing (2023).

[22] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, 2007 IEEE Symposium on Security and Privacy (SP '07) (2007) 321–334.

[23] Z. Zhang, C.-H. Lung, X. Wei, M. Chen, S. Chatterjee, Z. Zhang, In-network caching for icn-based iot (icn-iot): A comprehensive survey, IEEE Internet of Things Journal 10 (16) (2023) 14595–14620.

[24] A. Sahai, B. Waters, Fuzzy identity-based encryption, IACR Cryptol. ePrint Arch. 2004 (2005) 86.

[25] S. Khezr, A. Yassine, R. Benlamri, M. S. Hossain, An edge intelligent blockchain-based reputation system for iiot data ecosystem, IEEE transactions on industrial informatics 18 (11) (2022) 8346–8355.

[26] S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof-systems, in: STOC '85, 1985.

[27] M. Blum, P. Feldman, S. Micali, Non-interactive zero-knowledge and its applications, in: STOC '88, 1988.

[28] C. P. Sah, Robustness of zero-knowledge proofs using rsa problem, in: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2022, pp. 40–44.

[29] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. Cocco, J. Yellick, Hyperledger fabric: a distributed operating system for permissioned blockchains, Proceedings of the Thirteenth EuroSys Conference (2018).

[30] R. Li, H. Asaeda, J. Li, A distributed publisher-driven secure data sharing scheme for information-centric iot, IEEE Internet of Things Journal 4 (2017) 791–803.

[31] R. Li, H. Asaeda, J. Li, X. Fu, A verifiable and flexible data sharing mechanism for information-centric iot, 2017 IEEE International Conference on Communications (ICC) (2017) 1–7.

[32] Y. Zhao, M. Ren, S. Jiang, G. Zhu, H. Xiong, An efficient and revocable storage cp-abe scheme in the cloud computing, Computing 101 (2018) 1041–1065.

[33] S. Zhang, Z. Yan, W. Liang, K.-C. Li, B. Di Martino, Bcae: A blockchain-based cross domain authentication scheme for edge computing, IEEE Internet of Things Journal (2024).

[34] A. A. Khan, S. Dhabi, J. Yang, W. Alhakami, S. Bourouis, L. Yee, B-lpoet: A middleware lightweight proof-of-elapsed time (poet) for efficient distributed transaction execution and security on blockchain using multithreading technology, Computers and Electrical Engineering 118 (2024) 109343.

[35] V. Odelu, A. Das, M. K. Khan, K.-K. R. Choo, M. Jo, Expressive cp-abe scheme for mobile devices in iot satisfying constant-size keys and ciphertexts, IEEE Access 5 (2017) 3273–3283.

[36] J. Hao, C. Huang, J. Ni, H. Rong, M. Xian, X. Shen, Fine-grained data access control with attribute-hiding policy for cloud-based iot, Comput. Networks 153 (2019) 1–10.

[37] S.-R. Wang, Y. Zhang, Y. Zhang, A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, IEEE Access 6 (2018) 38437–38450.

[38] K. Fan, J. Wang, X. Wang, H. Li, Y. Yang, A secure and verifiable outsourced access control scheme in fog-cloud computing, Sensors (Basel, Switzerland) 17 (2017).

[39] C. Yuan, M. xue Xu, X. Si, B. Li, Blockchain with accountable cp-abe: How to effectively protect the electronic documents, 2017 IEEE

23rd International Conference on Parallel and Distributed Systems (ICPADS) (2017) 800–803.

[40] Y. Zhang, D. He, K.-K. R. Choo, Bads: Blockchain-based architecture for data sharing with abs and cp-abe in iot, Wirel. Commun. Mob. Comput. 2018 (2018) 2783658:1–2783658:9.

[41] X. Zhang, X. Chen, S. Liu, S. Zhong, Anonymous authentication and information sharing scheme based on blockchain and zero knowledge proof for vanets, IEEE Transactions on Vehicular Technology (2024).

[42] G. G. Gebremariam, J. Panda, S. Indu, Blockchain-based secure localization against malicious nodes in iot-based wireless sensor networks using federated learning, Wireless communications and mobile computing 2023 (1) (2023) 8068038.

[43] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, K.-C. Li, A blockchain-based auditable access control system for private data in service-centric iot environments, IEEE Transactions on Industrial Informatics 18 (5) (2021) 3530–3540.

[44] K. Xue, W. Chen, W. Li, J. Hong, P. Hong, Combining data owner-side and cloud-side access control for encrypted cloud storage, IEEE Transactions on Information Forensics and Security 13 (2018) 2062–2074.

[45] S. Pérez, D. Rotondi, D. Pedone, L. Straniero, M. Nuñez, F. Gigante, Towards the cp-abe application for privacy-preserving secure data sharing in iot contexts, in: IMIS, 2017.

[46] F. Guo, Y. Mu, W. Susilo, D. Wong, V. Varadharajan, Cp-abe with constant-size keys for lightweight devices, IEEE Transactions on Information Forensics and Security 9 (2014) 763–771.

[47] S. Wang, H. Wang, J. Li, H. Wang, J. Chaudhry, M. Alazab, H. Song, A fast cp-abe system for cyber-physical security and privacy in mobile healthcare network, IEEE Transactions on Industry Applications 56 (2020) 4467–4477.

[48] S. Ding, C. Li, H. Li, A novel efficient pairing-free cp-abe based on elliptic curve cryptography for iot, IEEE Access 6 (2018) 27336–27345.

[49] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, B. Ohlman, A survey of information-centric networking, IEEE Communications Magazine 50 (2012).