electronics

MDPI

Article

Blockchain-Based Authentication Protocol Design from a Cloud Computing Perspective

Zhiqiang Du [1], Wenlong Jiang [1], Chenguang Tian [1], Xiaofeng Rong [1,2,*] and Yuchao She [2]

[1] School of Computer Science and Engineering, Xi'an Technological University, Xi'an 710021, China; duzhiqiang@xatu.edu.cn (Z.D.); jiangwenlong@st.xatu.edu.cn (W.J.); tianchenguang@st.xatu.edu.cn (C.T.)
[2] Center of Information Technology, Xi'an Technological University, Xi'an 710021, China; sheyuchao@xatu.edu.cn
* Correspondence: rongxiaofeng@xatu.edu.cn

Abstract: Cloud computing is a disruptive technology that has transformed the way people access and utilize computing resources. Due to the diversity of services and complexity of environments, there is widespread interest in how to securely and efficiently authenticate users under the same domain. However, many traditional authentication methods involve untrusted third parties or overly centralized central authorities, which can compromise the security of the system. Therefore, it is crucial to establish secure authentication channels within trusted domains. In this context, we propose a secure and efficient authentication protocol, HIDA (Hyperledger Fabric Identity Authentication), for the cloud computing environment. Specifically, by introducing federated chain technology to securely isolate entities in the trust domain, and combining it with zero-knowledge proof technology, users' data are further secured. In addition, Subsequent Access Management allows users to prove their identity by revealing only brief credentials, greatly improving the efficiency of access. To ensure the security of the protocol, we performed a formal semantic analysis and proved that it can effectively protect against various attacks. At the same time, we conducted ten simulations to prove that the protocol is efficient and reliable in practical applications. The research results in this paper can provide new ideas and technical support for identity authentication in a cloud environment and provide a useful reference for realizing the authentication problem in cloud computing application scenarios.

Keywords: cloud computing; federated chains; zero-knowledge proofs; formal formalized semantic analysis

Citation: Du, Z.; Jiang, W.; Tian, C.; Rong, X.; She, Y. Blockchain-Based Authentication Protocol Design from a Cloud Computing Perspective. *Electronics* **2023**, *12*, 2140. https://doi.org/10.3390/electronics12092140

Academic Editor: Hamed Taherdoost

Received: 7 April 2023
Revised: 3 May 2023
Accepted: 4 May 2023
Published: 7 May 2023

1. Introduction

Cloud computing [1], as an Internet-based computing model, provides users with flexible, convenient, and economical computing and storage capabilities that greatly facilitate our lives. It quickly provides computing resources according to user needs to meet various business requirements and workload changes without requiring users to manage hardware and software. In daily use, cloud computing ensures a high availability of services through multiple data centers and corresponding backup mechanisms, reducing the risk of service interruption and providing users with more reliable services.

There is a growing trend of users preferring convenient and affordable cloud services as a platform for software development and server building. This trend has reduced labor and energy costs to some extent. However, traditional identity management models usually have a domain central node that manages the entire domain's business, which means that all data in the domain may be stored in the central node [2]. In this case, the security of the entire system depends entirely on the central node. Once a single point of failure occurs (such as a central node attack or central server downtime), the security of the system will be difficult to guarantee.

Although an increasing number of solutions are adopting distributed and decentralized approaches for deployment, designing a comprehensive identity management

system and a reasonable access control scheme in cloud computing environments remains a critical task, as many security and performance-related issues are yet to be resolved. Traditional identity management models are typically managed by central authorities or organizations [3], which can be easy targets for attackers and may suffer from poor management or abuse of power issues [4]. In addition, during identity authentication, users are required to provide a significant amount of personal identity information, which may result in the leakage of personal privacy. Simple data encryption alone is insufficient to ensure the security of communication between both parties, as eavesdropping by an attacker on sensitive data within the conversation can occur, ultimately leading to the desired attack effect. Examples of such attacks include the classic IP spoofing attack and SSL/TLS man-in-the-middle attacks. In fact, most existing identity management models suffer from single-point-of-failure and low efficiency issues, with the central server exposed to potential attacks that can result in the entire system being paralyzed [5].

Zero-knowledge proof (ZKVP) is used as a secure cryptographic technique. It is often used to prove the authenticity of a fact or information without revealing any specifics about the fact or piece of information, which means that the proving party does not need to reveal any additional information to the verifying party [6]. During the communication between two parties, a protocol based on zero-knowledge proof can encrypt the communication, thus effectively preventing man-in-the-middle attacks and other malicious behaviors.

A consortium blockchain network, also known as a private or permissioned blockchain network, is a type of blockchain network that is jointly managed and operated by multiple organizations or entities, and in which only authorized members are allowed to participate in transactions and verification [7]. These members typically have common interests or goals, and compared to public blockchain networks, consortium blockchain networks have stricter access permissions, making them more suitable for cooperation and transactions between enterprises and organizations [8]. Consortium blockchain has been used as an auxiliary support technology for identity management. By utilizing the consortium blockchain, sensitive nodes or organizations in the system can be securely isolated and protected, thus improving the security and reliability of the system. In addition, consortium blockchains can provide more efficient solutions for identity management. For example, VeChain is a supply chain management platform that utilizes a federated chain network to enhance the quality and security of products for companies. The platform also features a reliable identity management system that ensures traceability at every point in the supply chain, effectively protecting both businesses and consumers. Another example is Corda, an enterprise-grade blockchain platform focused on the financial services sector, which provides a secure and efficient transaction and identity management experience, ensuring that participants' identities are protected during transactions and identity verification. These federated chain applications are built on common interests and goals, leveraging blockchain technology to provide organizations and businesses with a more secure and efficient transaction and identity management solution.

Combining zero-knowledge proof technology with blockchain technology can bring the following benefits to identity management solutions:

- Better privacy protection: The audit access mechanism of consortium blockchain technology ensures that all nodes in the chain can only access and view the information they need, while zero-knowledge proof technology can achieve verification without disclosing any personal identity information, thereby better protecting personal privacy.
- More efficient identity verification: Consortium blockchain technology can provide a more efficient identity verification mechanism because it does not rely on traditional centralized identity verification institutions but instead implements decentralized identity verification based on blockchain technology. At the same time, zero-knowledge proof technology can help verifiers complete verification without the need to disclose identity information.

- More reliable identity management: Consortium blockchain technology can establish a more reliable identity management system because all identity information is stored on a distributed ledger to ensure that it is not tampered with. Using zero-knowledge proof technology for identity verification can enhance the reliability of identity verification, thereby reducing the risk of identity fraud and theft.

To better solve various problems arising from the traditional identity management model, an identity authentication scheme (HIDA) based on the combination of blockchain technology and zero-knowledge proof technology is proposed in this paper. It aims to achieve more secure, efficient, and reliable identity authentication. Our specific contributions are as follows:

- In this paper, we propose an efficient and secure authentication scheme (HIDA) based on the combination of blockchain technology and zero-knowledge proof technology, which can support efficient authentication of users to service providers in cloud computing scenarios.
- BAN logic was chosen to perform a formal security analysis of our solution to demonstrate the security and privacy protection that HIDA can provide.
- Finally, the performance of the HIDA scheme was evaluated by conducting simulation experiments and comparing it with the previous scheme. The experimental results show that HIDA not only has advantages in terms of security but also performs well in terms of efficiency. Specifically, our scheme can provide efficient authentication services in a cloud computing environment with a shorter response time and lower computational resource consumption compared to traditional schemes.

The following sections of this article are organized as follows: Section 2 reviews related work in the field of identity management; Section 3 provides a detailed problem statement and presents a threat model, upon which our design goals are based; Section 4 introduces relevant theoretical knowledge; Section 5 elaborates on the system model and specific solution; Section 6 provides a proof and analysis of the security of our solution; Section 7 conducts experiments in a simulated environment and compares our solution with previous works; and finally, Section 8 concludes the article.

2. Related Work

Identity authentication is a security mechanism that confirms a user's identity through certain technical means to ensure that only legitimate users can access the corresponding services [9]. Currently, blockchain-based identity authentication can be divided into three methods: anonymous authentication, real-name authentication, and controllable anonymous authentication [3].

Anonymous authentication means that users do not need to reveal their true identity during the registration and authentication process. However, due to the openness and multi-party confirmation of the ledger, privacy protection of transaction identities cannot be guaranteed. Real-name authentication is similar to the traditional CA-based authentication scheme, where a third party issues an authentication certificate to prove the user's legitimacy. Currently, controllable anonymous authentication is more popular, and most schemes use ring signatures or blind signatures to anonymously operate user identities. However, the association between user identity information and account addresses is still stored in the third-party authentication institution. If the third party cannot guarantee its own security, the user's anonymous identity may still be obtained. Keltoum Bendiab and Nicholas Kolokotronis combined blockchain technology with a cloud environment to design a blockchain-based cloud identity management scheme. The proposed trust model allows CSPs to autonomously manage their trust relationships in a dynamic and distributed manner. Subsequently, domestic scholars designed an Ethereum-based Identity Management (EIDM) [10] scheme using the CIDM (Consolidated Identity Management) [11] protocol, smart contracts and reputation systems, and EIDM. The EIDM does away with the traditional Identity Management (IDM) proxy and uses blockchain technology to establish a trust relationship between the CSP and the cloud subscriber, thus

solving the problems of the single point of failure and over-reliance on third parties that exist in traditional authentication. However, this solution suffers from user privacy and man-in-the-middle attacks during initialization.

OAuth [12] is a well-known identity management protocol designed to help users manage their identities. In this protocol, users obtain a token from an authentication server and use it to access resources on a resource server. However, the protocol lacks trust in data and servers, and the authentication process depends entirely on the authentication server. The UPort [13], ShoCard [14], and Sovrin [15] solutions are all Distributed Ledger Technology (DLT) projects [15] currently implemented on blockchain platforms. These solutions utilize the idea of decentralization to varying degrees, but mainly aim to reshape the role of centralization and intermediaries. For the UPort solution, if an attacker can compromise the Uport application and replace the trusted party with a controller without being noticed, the Uport ID will be permanently compromised. For the ShoCard solution, the intermediary role does introduce uncertainty to the vertical existence of the ShoCard ID; if the company no longer exists, ShoCard users will not be able to use their authenticated results to access the system [16]. As for the Sovrin solution, users must rely on the institutions that represent them and maintain the distributed ledger in the Sovrin network. Depending on the selection and implementation of the intermediary agency, a lot of information may be in its hands [16].

In addition, there are also some blockchain-based IoT device identity authentication schemes. For example, the scheme proposed by Liangqin Gong et al. [17] considers recording device identity information in a distributed ledger to ensure identity verification transactions are recorded in the blockchain network. However, the threshold and feature weight settings in this scheme are static and require regular training updates. The scheme proposed by Gan et al. [18] uses a private chain to store node public key information, but this scheme is based on a completely trusted central CA node, which has a single point of failure. The scheme proposed by Li Wenjie [19] uses an improved model based on the claim identity authentication model and declares user attribute ownership using digital signatures and hash values. However, the authentication authority in this scheme is centrally managed, and if the manager of the authentication center behaves improperly or is attacked, attackers may steal or tamper with user identity information, leading to further fraud or infringement of user privacy.

Therefore, these schemes all need further improvement to enhance security and stability. According to the existing solutions for identity authentication on the blockchain, most of them heavily rely on authentication nodes or third-party platforms. Exposing the core nodes of the system on the public network itself poses a risk of attack. Once these nodes are compromised, there is a possibility of all user identity information being leaked. Our scheme attempts to isolate the authentication nodes from user access, logically avoiding the possibility of the authentication nodes being attacked, thereby improving the robustness and security of the system model.

3. Problem Statement

In this section, we describe two application scenarios with authentication requirements in a cloud-based environment. Different organizations complete the corresponding tasks. We discuss the possible security threats during the authentication process and summarize the objectives of our design.

3.1. Scenario Description

With the rapid development of cloud computing, more and more services are being deployed on lightweight and convenient cloud platforms. Figures 1 and 2 depict scenarios for identity authentication based on CA certificates and user credentials. Figure 1 includes three parts: a center authentication (CA), a cloud user, and a cloud service provider (CSP). The user requests centralized authentication from the CA, which verifies and stores the user's information and finally issues a certificate for future access. Figure 2 includes

three parts: a cloud service provider, a cloud data center (CDC), and a cloud user. Users within the same security domain no longer need to be authenticated by the CA before requesting services from the cloud service provider. The specific authentication process is completed by the cloud service provider. Users submit registration requests to the cloud service provider, which then transfers the authentication business to the data processing center for review and registration of user identities. Multiple service providers may form a single alliance organization and share the same group of data centers, but more schemes choose to combine CSP and CDC designs.

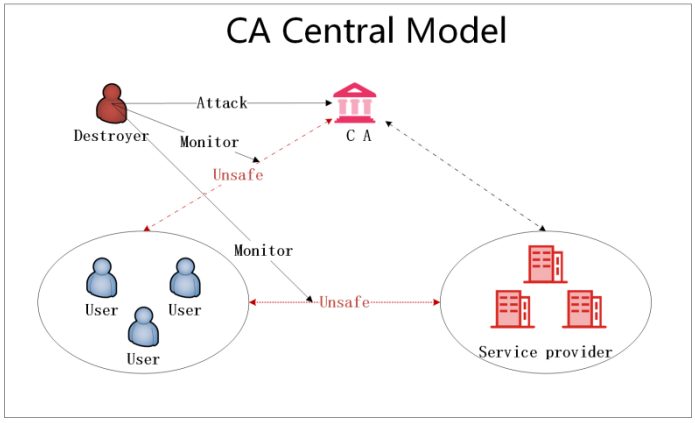


Figure 1. CA Centre based authentication model.

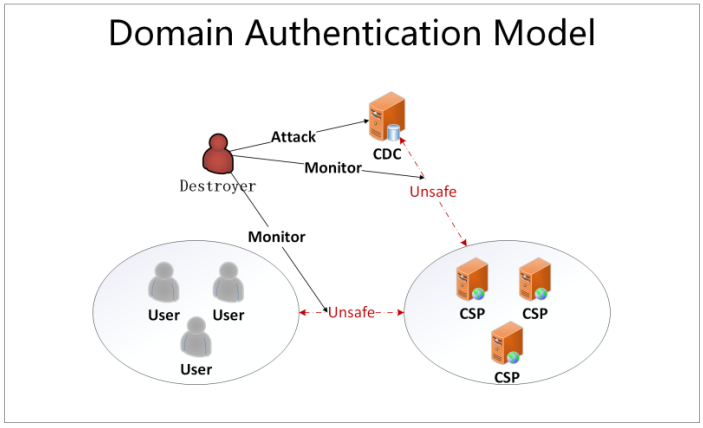


Figure 2. Intra-domain-based business separated authentication model.

3.2. Security Threats

Different models are suitable for different business needs. Centralized authentication based on authoritative organization authentication is more suitable for government and educational organizations, while credential-based identity authentication based on service provider registration seems to be more suitable for flexible small enterprises or companies. When deploying user data into public clouds, these resources naturally become the target of cybercriminals. Therefore, we should consider their security and privacy issues more carefully.

For the model in Figure 1, all system business will flow to the authentication center for data filtering and storage. First, we should consider the performance issue with CA. With the continuous growth in the number of users, the lightweight central service may not be able to support simultaneous multi-user access. In addition, when attackers attempt to block and destroy CA using worm attacks and other methods, it may cause the entire system to be paralyzed. Secondly, CA has the highest authority in the system, and all user data will flow into the central organization for review and storage. If CA is tempted

by other larger interests and causes corruption, all information will be directly disclosed, leading to privacy leaks.

For the model in Figure 2, users can undergo identity authentication in different security domains based on different service providers. Although private CDCs in each security domain can to some extent avoid the single point of failure problem brought on by over-centralization of CA, from another perspective, not all domain users are completely trustworthy. This model only separates service businesses from authentication businesses, improving the overall operating efficiency of the system model, but does not further perform security maintenance on the CDC. When there are channel listeners in the system, attackers can intercept and listen to the communication between the two parties to obtain credential information. In addition, after the CDC is separated, attackers are more likely to launch attacks on specific business servers to block the normal operation of the system.

3.3. Design Goals

Identity security: All user requests should be transmitted through reliable channels, the information used for authentication should only belong to the user, and no adversary can impersonate a legitimate user to access services.

Business separation: When users request services in different domains, they should register with a specific service provider. The specific identity authentication is then forwarded to the corresponding data center for processing. To ensure high performance of the system as a whole, the service provider should split the data center into another independent server, focusing only on user access to business.

Entity isolation: To prevent independent data centers from being easily destroyed by attackers, corresponding measures should be taken to ensure their security isolation. When the data center is hidden in a specific security domain and does not accept any unfamiliar requests, the overall security and robustness of the system can be greatly improved.

Secure transmission: To protect user data from eavesdroppers, more security measures are needed to prevent information leakage. Therefore, we can implement permitted access within the domain and encryption using the zero-knowledge proof method to improve the security of the system.

Mutual authentication: During the authentication process, users and service providers can authenticate each other. Service providers only provide services to authenticated users, while users only trust services provided by authenticated service providers.

Scalability: The system has no single point of failure and, therefore, can support large-scale identity authentication business processing.

4. Preliminaries

This section focuses on the technical knowledge covered in the article. We first review some basic concepts and definitions of cryptography [20] and then normalize the Fait–Shamir protocol in zero-knowledge proofs. Finally, we refer to blockchain technology and describe the possible benefits of choosing this technology.

4.1. Elliptic Curve [21]

Definition 1. (the elliptic curve discrete logarithm problem**).** *Let P be a base point arbitrarily chosen from the elliptic curve EP(a,b). For any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the probability of finding $k \in \mathbb{Z}_n^*$ satisfying equation $\mathcal{Q} = k\mathcal{P}$ is negligible when the parameters are given.*

4.2. RSA [22] Secure Public Key Encryption

RSA is a public-key encryption algorithm based on the large prime number decomposition puzzle, proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. The

RSA algorithm uses a pair of keys, a public key and a private key, to encrypt and decrypt data [23].

Definition 2 (RSA**).** *Let ℓ be a function such that for all n, $\ell(n) \leq 2^{(n-2)}$. The public key encryption scheme is defined as follows, where Algorithm 1 specifies the GenRSA function's specific process:*

1. *Gen: Given input 1^n, run GenRSA (1^n) to obtain (N,e,d). Output the public key pk = <N,e> and private key sk = <N,d>.*
2. *Enc: Given a public key pk = <N,e> and a message m∈ {0, 1}^ℓ(n), choose a random string $r \leftarrow \{0,1\}^{\{||N||-\ell(n)-1\}}$, and interpret r||m as an element of $\mathbb{Z}_n$. The output ciphertext is c := [(r||m)e mod N].*
3. *Dec: Given the private key sk = <N,d> and the ciphertext c∈$\mathbb{Z}_n^*$, compute the message m := [cd mod N], and output the low l(n) bits of m.*

Algorithm 1. GenRSA

Input: security parameter 1^n
Output: N,e,d
1. (N,e,d) ← GenModulus (1^n);
2. ϕ(N) = (p − 1) (q − 1);
3. Choose e satisfied with gcd (e,ϕ(N)) = 1;
4. Computer d:= [e^{-1} mod ϕ(N)];
5. Return N,e,d;

4.3. Zero-Knowledge Proof (Fait–Shamir Protocol [24])

Zero-knowledge proofs were proposed by S. Goldwasser, S. Micali, and C. Rackoff in the early 1980s. This proof method allows the prover to prove to the verifier that it possesses a particular piece of information without revealing its secret information. In communication between a communicating entity B (the prover) and A (the verifier), if B is able to successfully prove to A that it possesses the secret but A is unable to infer the secret information, the proof is shown to have zero knowledge. In addition, a zero-knowledge proof needs to satisfy correctness, i.e., the inability of A to master a proof method that makes it highly probable that B possesses the secret. Finally, a zero-knowledge proof also needs to satisfy completeness, i.e., B possesses a theorem-proving method that makes A believe that B can complete the proof. Next, we give specific definitions in Algorithms 2 and 3, and describe the proof process in detail. The flow of the scheme is shown in Figure 3.

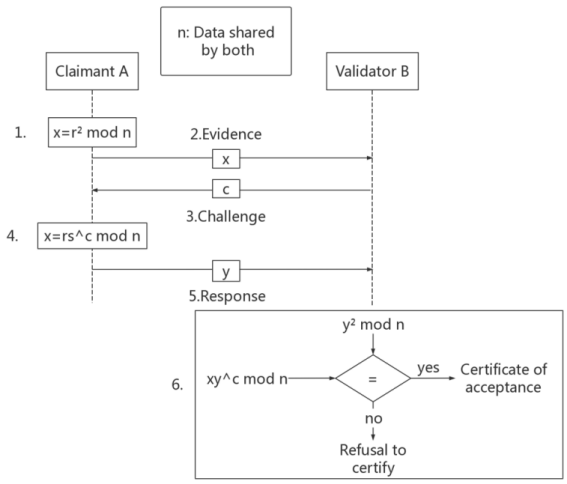


Figure 3. The Fait–Shamir protocol.

Definition 3. *The zero-knowledge proof based on the Fait–Shamir protocol consists of four algorithms (Gen,Prf,Chg,Vrfy) for the prover A and the verifier B. The details of the algorithms are as follows:*

- *(pk,sk)* $\leftarrow$ *FS.Gen(*1^{λ}*): The key generation algorithm takes a security parameter* $\lambda \in \mathbb{N}$ *as input and outputs the public prover key pk and the signing key sk.*
- *(x)* $\leftarrow$ *FS.Prf(r): The evidence generation algorithm selects a random number r, where* $(0 \leq r < n) \cap r \leftarrow \mathbb{Z}_n$*, and computes the evidence x to be used in the subsequent proof based on r.*
- *(y)* $\leftarrow$ *FS.Chg(c): The challenge–response algorithm computes the corresponding response y by A after receiving the random number c* $\in$ *{0, 1}* generated by B for the challenge.*
- *{0, 1}** $\leftarrow$ *FS.Vrfy(): The key generation algorithm outputs the public prover key pk and the secret key sk for signing when given a security parameter* $\lambda \in \mathbb{N}$ *as input.*

Algorithm 2. Proof/Challenge information generation

Input: Prover public key Pk and secret private key Sk, r (commitment random number)/c (challenge random number).
Output: Output corresponding evidence x and response y
1. Compute n = (pk,sk) $\in \mathbb{Z}_n^*$;
2. Compute x = r^2 mod n;
3. Or Compute y = rs c mod n;
Return x or y;

Algorithm 3. Verify secret

Input: corresponding evidence x and response y
Output: Verification result: succeed or fail.
1. Compute x == y;
2. if true return 1;
3. else return 0;

4.4. Blockchain Technology

Blockchain technology is a decentralized, public, and distributed ledger technology used to record and verify transactions and data transfers. It consists of a series of blocks, each containing information about specific transactions such as transaction amount, timestamp, and participant addresses. Each block is linked to the previous block, forming an immutable chain that makes it impossible for anyone to alter previous transaction records. This means that blockchain technology has a high level of security and transparency, as all participants can view and verify transactions, and no centralized institution or single entity can manipulate it. Additionally, due to its decentralized nature, blockchain technology can address some of the problems that exist in traditional centralized systems, such as single points of failure, data leaks, and security concerns.

A federated chain is a private chain based on blockchain technology that consists of a group of pre-authorized participants, which are usually businesses, government agencies, or organizations. Unlike public blockchains, federated chains allow participants to selectively disclose or protect their data, thus allowing for trustworthiness and security while maintaining data privacy. In a federated chain, participants need to be authenticated and authorized to join the network and participate in transactions. Each participant has a local copy of all transactions and associated data that are verified and authorized by a consensus algorithm. Unlike public blockchains, federated chains typically use more efficient consensus algorithms because of the relatively small number of participants and the higher speed and throughput required for transactions. In addition, federated chains are also more flexible and customizable, as participants can configure and deploy them to meet specific needs.

Hyperledger Fabric is a permissioned blockchain platform that serves as the foundation for many federated chains. It was selected as the basis for this experiment because of its features that support the creation and operation of permissioned networks. Hyperledger Fabric allows for fine-grained control of permissions, providing greater flexibility in the management of the network. Additionally, it supports a modular architecture that allows for easy customization and integration with existing systems. A federated chain based on Hyperledger Fabric consists of a group of pre-authorized participants who are authenticated and authorized to join the network and participate in transactions. Each participant has a local copy of all transactions and associated data that are verified and authorized by a consensus algorithm. Hyperledger Fabric's pluggable consensus algorithm allows for a more efficient consensus mechanism that can be customized based on the requirements of the network. In summary, Hyperledger Fabric was selected as the foundation for this experiment because of its features that support permissioned networks, fine-grained control of permissions, modular architecture, and pluggable consensus algorithm.

5. Design of HIDA

Starting from this section, we provide in Table 1 the symbols used in the protocol and their related meanings to facilitate a better understanding in the subsequent description.

Table 1. The symbol description in the identity authentication protocol.

Symbol	Meaning
PK_n	Public key for entity n
SK_n	Private key of entity n
K_n	Key for entity n
E (K_n, M)	Encryption of M using the key of entity n
D (K_n, M)	Decryption of M using the key of entity n
A→B:m	Entity A sends a message to Entity B m
ID_n	Unique ID of entity n
T_n	Entity n generated timestamp and signature
Hash (M)	Hash for M using MD5

In this section, we first introduce the system model and then provide a detailed description of a secure authentication scheme based on blockchain technology and zero-knowledge proofs in a cloud computing environment.

5.1. System Model

To achieve a secure and efficient identity authentication scheme, we have designed a system model combining blockchain technology and zero-knowledge proof, as shown in Figure 4. The model consists of several parts: cloud users, cloud service organizations, cloud data centers, and blockchain networks.

In the CDC organization, a node can communicate with a designated node in the CSP, and they share a blockchain in the same channel. Separating business and identity management has the benefit of improving CSP service efficiency because identity authentication consumes computing resources, while CSP provides cloud resource usage to users. Therefore, separating identity authentication functionality allows CSP to focus on business processing. Another advantage is scalability. If additional CSP organizations want to join the blockchain network, the organization need only apply for a node in the CDC group to achieve subsequent user access management. In the identity management and authentication model based on the Fabric network, CSP provides interfaces for users to register and log in with their identity information. In Hyperledger Fabric, there is more than one node that provides services to users on the same channel, and they share a ledger. As the administrator of the blockchain network, they monitor the state of the entire network and can view the information in the corresponding blocks. In a network environment, the most trusted party is oneself, so the user's identity

credentials must be stored in ciphertext in the block and transmitted in ciphertext form during transmission to prevent man-in-the-middle attacks.

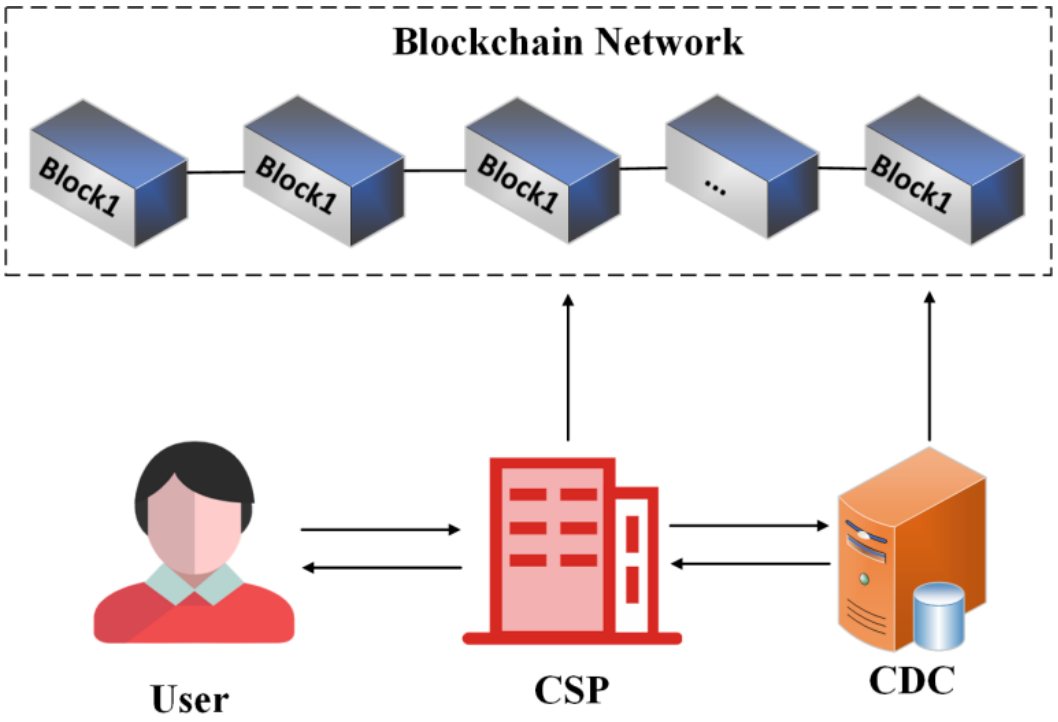


Figure 4. Secure and efficient identity authentication system model.

5.2. Specific Steps

As shown in Figure 5, the proposed scheme consists of seven steps. In these steps, we can observe that users only need to interact with CSP, and all related authentication tasks will be performed by CDC, thereby reducing the computational burden on CSP. The specific authentication process of the scheme is as follows:

(1) Initializing the user environment means that all system parameters have been instantiated, including <N,e,d> for encryption, which is computed by the user running GenRSA(1^n) and inputting the security parameter 1^n. The public key is represented by <N,e>, and the private key is represented by <N,d>. In addition, system parameters for a specific elliptic curve are pre-defined, and mathematical operations and calculations necessary for encryption and decryption are performed. These system parameters include the elliptic curve identifier cid, parameters for the base field Fq of the elliptic curve, parameters a and b for the elliptic curve equation, the order N and cofactor cf of the curve, as well as the embedding degree k and f of the curve E(Fq). Using these system parameters, a bilinear mapping from G1 to G2 can be defined, where P1 and P2 are generators of the cyclic subgroups G1 and G2 that generate the curve E(Fq). In addition, a bilinear pairing identifier eid and a homomorphic mapping Ψ from G2 to G1 are required. The user sets the password as the user s secret s and hash s to get x. It then finds the two points G and H on the elliptic curve, and multiply points G and H by x to get xG and xH.

(2) After the user has initialized the environment, they send the following registration request information to the CSP (where ID_u is the user's ID, Username is the user's registered name, and T_u is the user's timestamp to prevent replay attacks):

$$\text{User} \rightarrow \text{CSP: Request\_Enroll}(ID_u, \text{Username}, xG, xH, T_u)$$

(3) After receiving the registration request from the user, CSP checks its local ledger to see if there is any corresponding block information with ID_u. If the information exists, CSP responds to the user with a message m_1 indicating that the user already exists with Tcsp. Otherwise, CSP sends the user's registration identity information, including IDu and EGH, to CDC.

$$CSP \rightarrow CDC: Message(ID_u, xG, xH, T_s)$$

(4) After receiving the message from CSP, CDC generates a random value of c. CDC encrypts c using the secret key K_{cdc}, resulting in $E_c = E(K_{cdc}, c)$, and stores it along with xG and xH in the local ledger corresponding to ID_u.

(5) The registration result m_2 returned to CSP includes E_c, the ciphertext $EK_{cdc} = E(PK_u, K_{cdc})$ obtained by encrypting Kcdc with the user's public key, and the user ID.

(6) After receiving the message from CDC, CSP stores more detailed user information, including IDu, username, and user registration time-related information in a block for later user information querying operations. CSP then returns the registration result message to the user as follows (where m_3 represents the message containing E_c, EK_{cdc}, and the registration success information):

$$CSP \rightarrow User: Respond(m_3, T_s)$$

(7) After receiving the registration result message from CSP, the user decrypts $E(PK_u, K_{cdc})$ using the private key SK_n to obtain K_{cdc}. Then, the user decrypts Ec using Kcdc to obtain the plaintext c and stores it locally for the next identity verification. When the user needs to verify their identity to access cloud resources, The user only needs to provide a random value v which is calculated by $(v - cx)$ to obtain an r (r is called a promise) to complete the operation of verifying the user's identity. The user sends a login request to CSP, and the request message includes the following content (where vG and vH are obtained by doubling G and H points by v, and Tu is the user-generated timestamp):

$$User \rightarrow CSP: Request\_Verify(ID_u, Username, r, vG, vH, T_u)$$

(8) After receiving the login request from the user, the CSP checks if the user with IDu is registered. If the user is not registered, the CSP returns a message m1 indicating that the user does not exist. Otherwise, the CSP sends IDu, r, vG, and vH to the CDC.

$$CSP \rightarrow CDC: Message\ (ID_u, r, vG, vH)$$

(9) After receiving the message from CSP, CDC uses the doubling method to multiply the G and H points by r to obtain rG and rH. Then, CDC queries the corresponding information of the user in the local ledger using IDu to obtain (xG, xH) and $E(K_{cdc}, c)$, and decrypts E(Kcdc, c) using Kcdc to obtain c. Next, CDC multiplies the xG and xH points by c using the doubling method to obtain cxG and cxH, and sets a = rG + c(xG) and b = rH + c(xH). Finally, CDC verifies if a equals vG and b equals vH as sent by the user and returns the verification result m2 to CSP. The reason why the equality of the two sides can prove that the user owns s is as follows:

$$vG = rG + c(xG) = (v - cx)G + cxG = vG$$

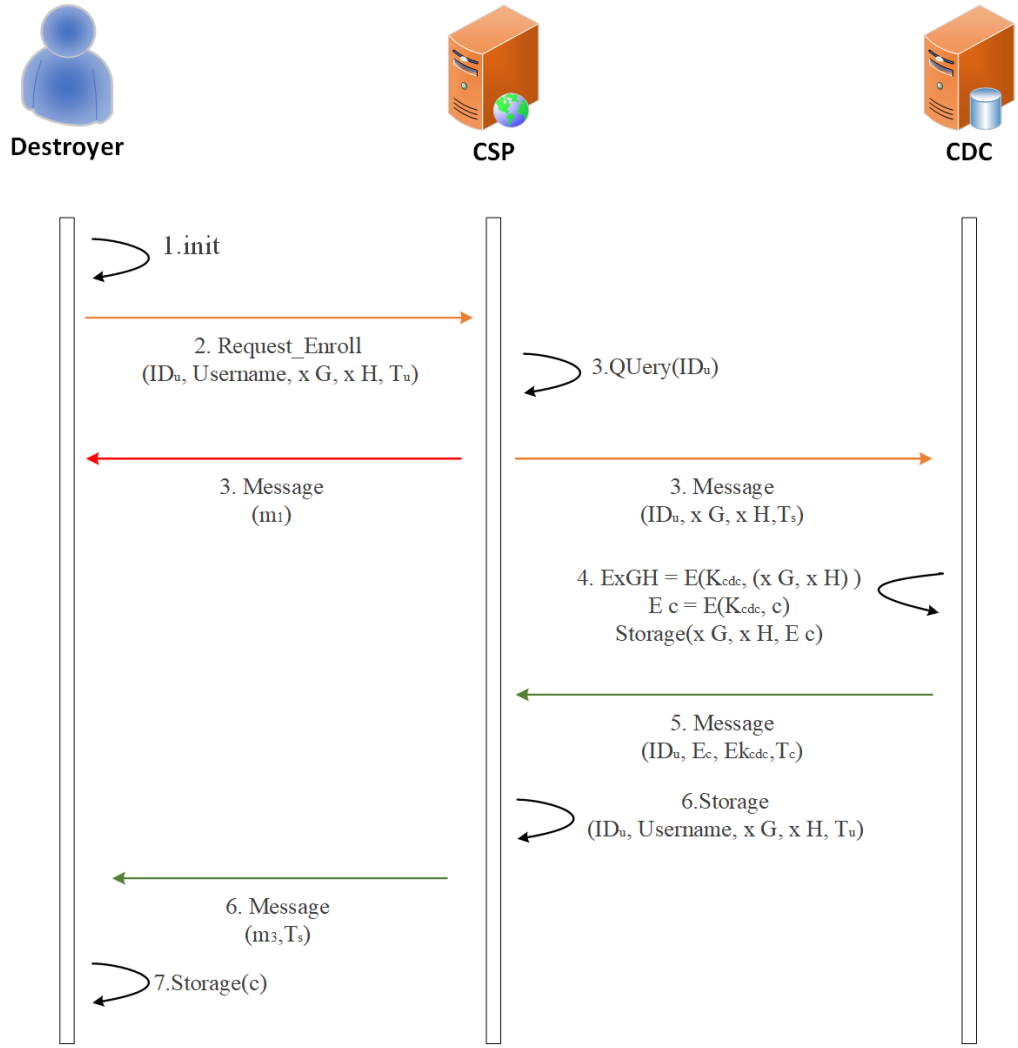


Figure 5. Specific protocol of identity authentication.

6. Security Analysis

The proposed HIDA authentication model in this paper involves three entities $U \in \mathbb{P} = (\mathbb{U} \cup \mathbb{S} \cup \mathbb{C})$, which are cloud users (to be authenticated), cloud service providers, and cloud data centers. We assume that $U \in \mathbb{P}$ has long-term asymmetric keys (sku, pku). During the operation of an entire system, let us assume the existence of adversary $\mathcal{A}$ who tries to disrupt the system in polynomial time. The possible ways of disruption mainly include attacks on the three-party entities and eavesdropping on the communication between the two parties to obtain sensitive data transmitted over the channel, thereby causing user identity leakage. We will analyze and prove the infeasibility of various types of attacks below.

6.1. Security Analysis

Claim 1: The CDC in this model has a high level of security protection and can effectively prevent system crashes caused by single-point attacks.

Analysis: The system model constructed in this article is based on a secure consortium chain using Fabric as a permission-granted blockchain. This means that only authorized entities can participate in the chain and access and process sensitive data and business logic. At the same time, permission-granted consortium chains have higher transaction processing speeds and scalability because only a small number of authorized nodes participate in verifying and adding new blocks, rather than all nodes needing to participate in the process. As shown in Figure 6, when an attacker is in a complex environment and wants to

perform access attacks on the CDC, the likelihood of a successful attack is negligible due to being unauthorized.

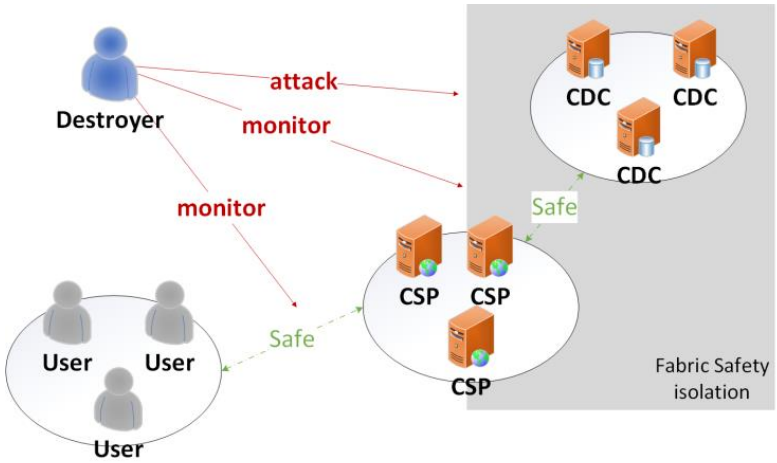


Figure 6. Safety model under HIDA.

6.2. Privacy Analysis

Claim 2: User data can be securely transmitted in the proposed model.

Analysis: This paper cleverly combines asymmetric encryption and symmetric encryption techniques to protect sensitive user data and uses zero-knowledge proof technology and blockchain technology to achieve secure authentication and storage of user identities. Therefore, unauthorized attackers find it difficult to eavesdrop on the channel. Secondly, assuming the difficulty of the RSA problem and the relatedness of GenRSA, selecting H as a random oracle [25] and using Π to represent the construction method in Algorithm 1, it can be proved that Π has indistinguishable encryption in the presence of eavesdropping by an adversary $\mathcal{A}$. Define $\varepsilon(n) = \Pr[\mathrm{PubK}^{\mathrm{eav}}_{A,\Pi}(n) = 1]$ and use the random oracle model to prove its security.

6.3. Formal Analysis

BAN logic is a logical system for analyzing the security of communication protocols, proposed by computer scientists Michael Burrows, Martín Abadi, and Roger Needham in 1989 [26]. Its main purpose is to analyze and prove the security of communication protocols, which are sets of rules used to exchange information between two parties. BAN logic defines a set of logical formulas and rules to analyze the security of these protocols. These formulas and rules describe the processes of sending, receiving, and processing information, and allow for the derivation of properties such as non-attackability and confidentiality of the protocol.

- BAN logical reasoning rule:

  (1) Rules of message meaning:

  (1.1) $\dfrac{\mathrm{P}|\equiv \mathrm{Q} \overset{\mathrm{K}}{\leftrightarrow} P, P \lhd \{X\}_K}{P|\equiv Q \sim X}$

  (1.2) $\dfrac{\mathrm{P}|\equiv \overset{K}{\rightarrow} \mathrm{Q}, P \lhd \{X\}_{K^{-1}}}{P|\equiv Q \sim X}$

  (1.3) $\dfrac{\mathrm{P}|\equiv Q \underset{\mathrm{Y}}{\leftrightarrow} \mathrm{P}, P \lhd \{X\}_Y}{P|\equiv Q \sim X}$

  (2) Temporary value verification rules:

$$\frac{\mathrm{P}|\equiv \#(X), \mathrm{P}|\equiv \mathrm{Q} \mid \sim \mathrm{X}}{P|\equiv Q|\equiv X}$$

(3) Arbitration rules:

$$\frac{\mathrm{P}|\equiv Q|\Rightarrow X, \mathrm{P}|\equiv \mathrm{Q}|\equiv \mathrm{X}}{P\ |\equiv X}$$

(4) Faith rules:

$$\frac{\mathrm{P}|\equiv X, \mathrm{P}|\equiv Y}{P\ |\equiv (X,Y)} \quad \frac{\mathrm{P}\ |\equiv (X,Y)}{P\ |\equiv X} \quad \frac{\mathrm{P}|\equiv Q|\equiv (X,Y)}{P|\equiv Q|\equiv X}$$

(5) Send rules:

$$\mathrm{s}\frac{\mathrm{P}|\equiv Q|\ \sim (X,Y)}{P|\equiv Q|\ \sim X}$$

(6) Receive rules:

$$\frac{\mathrm{P}\lhd(\mathrm{X},\mathrm{Y})}{P\lhd X} \quad \frac{\mathrm{P}\lhd\langle X\rangle_Y}{P\lhd X} \quad \frac{\mathrm{P}|\equiv Q\overset{K}{\leftrightarrow}P, P\lhd\{X\}_K}{P\lhd X}$$

$$\frac{\mathrm{P}|\equiv\overset{K}{\rightarrow}P, P\lhd\{X\}_K}{P\lhd X} \quad \frac{\mathrm{P}|\equiv Q|\sim(X,Y)}{P|\equiv Q|\sim X}$$

(7) Fresh rules:

$$\frac{\mathrm{P}\ |\equiv \#(X)}{P\ |\equiv \#(X,Y)}$$

(8) Share key rules:

$$\frac{\mathrm{P}\ |\equiv R\overset{X}{\leftrightarrow}R'}{P\ |\equiv R'\overset{X}{\leftrightarrow}R} \quad \frac{\mathrm{P}\Big|\equiv Q\Big|\equiv R\overset{X}{\leftrightarrow}R'}{P\Big|\equiv Q\Big|\equiv R'\overset{X}{\leftrightarrow}R}$$

(9) Sharing of secret rules:

$$\frac{\mathrm{P}\ |\equiv R\underset{x}{\leftrightarrow}R'}{P\ |\equiv R'\underset{x}{\leftrightarrow}R} \quad \frac{\mathrm{P}\Big|\equiv Q\Big|\equiv R\underset{X}{\leftrightarrow}R'}{P\Big|\equiv Q\Big|\equiv R'\underset{x}{\leftrightarrow}R}$$

- The agreement is idealized:

  Message 1: U→S:{IDu, Username, xG, xH, Tu}Ks
  Message 2: S→C:{IDu,xG, xH, Ts}Kc
  Message 3: C→S:{IDu, {Ec, EKcdc}Kuc, Tc}Ks
  Message 4: S→U:{ {Ec, EKcdc}Kuc, Ts}Ku

- Initialize the hypothesis:

(1) $\mathrm{U}\ |\equiv\overset{K_s}{\rightarrow}\mathrm{S}$
(2) $\mathrm{U}\ |\equiv\overset{K_c}{\rightarrow}C$
(3) $\mathrm{S}\ |\equiv\overset{K_u}{\rightarrow}\mathrm{U}$
(4) $\mathrm{S}\ |\equiv\overset{K_c}{\rightarrow}\mathrm{C}$
(5) $\mathrm{C}\ |\equiv\overset{K_u}{\rightarrow}\mathrm{U}$
(6) $\mathrm{C}\ |\equiv\overset{K_s}{\rightarrow}\mathrm{S}$
(7) $\mathrm{S}\ |\equiv \mathrm{U}(|\Rightarrow xG, xH)$
(8) $\mathrm{C}\ |\equiv \mathrm{S}(|\Rightarrow xG, xH)$
(9) $\mathrm{S}\ |\equiv \mathrm{C}\left(|\Rightarrow \{E_c, EK_{cdc}\}_{K_{uc}}\right)$
(10) $\mathrm{U}\ |\equiv \mathrm{S}\left(|\Rightarrow \{E_c, EK_{cdc}\}_{K_{uc}}\right)$
(11) $\mathrm{U}\ |\equiv \sharp(\mathrm{T}_s)$
(12) $\mathrm{U}\ |\equiv \sharp(\mathrm{T}_c)$
(13) $\mathrm{S}\ |\equiv \sharp(\mathrm{T}_u)$

(14) $S \mid\equiv \sharp(T_c)$
(15) $C \mid\equiv \sharp(T_u)$
(16) $C \mid\equiv \sharp(T_s)$

- The purpose of certification:

(1) $S \mid\equiv \{xG, xH\}$
(2) $C \mid\equiv \{xG, xH\}$
(3) $S\left\{\{E_c, EK_{cdc}\}_{K_{uc}}\right\}$
(4) $U\left\{\{E_c, EK_{cdc}\}_{K_{uc}}\right\}$

- Logical inference:

(i)

message 1 $\Rightarrow S \lhd \{ID_u, Username, xG, xH, T_u\}_{K_s}$	(1a)
(1a) $\wedge$ assumption (3) $\Rightarrow S \mid\equiv U \sim \{ID_u, Username, xG, xH, T_u\}$	(1b)
rule (7) $\wedge$ assumption (12) $\Rightarrow S\sharp\{ID_u, Username, xG, xH, T_u\}$	(1c)
(1b), (1c) $\wedge$ rule (2) $\Rightarrow S \mid\equiv U \mid\equiv \{ID_u, Username, xG, xH, T_u\}$	(1d)
(1d) $\wedge$ rule (4) $\Rightarrow S \mid\equiv U \mid\equiv \{xG, xH\}$	(1e)
(1e) $\wedge$ assumption (7) $\Rightarrow S \mid\equiv \{xG, xH\}$	(a)

(ii) Similarly, the above message and assumptions under the reasoning of the BAN logic rules lead to proof (b): $C \mid\equiv \{xG, xH\}$ (b)

(iii)

message 3 $\Rightarrow S \lhd \left\{ID_u, \{Ec, EK_{cdc}\}_{K_{uc}}, T_c\right\}_{K_s}$	(2a)
(2a) $\wedge$ assumption (4) $\Rightarrow S \mid\equiv C \sim \left\{ID_u, \{E_c, EK_{cdc}\}_{K_{uc}}, T_c\right\}$	(2b)
rule (7) $\wedge$ assumption (14) $\Rightarrow S\sharp\left\{ID_u, \{E_c, EK_{cdc}\}_{K_{uc}}, T_c\right\}$	(2c)
(2b), (2c) $\wedge$ rule (2) $\Rightarrow S \mid\equiv C \mid\equiv \left\{ID_u, \{E_c, EK_{cdc}\}_{K_{uc}}, T_c\right\}$	(2d)
(2d) $\wedge$ rule (4) $\Rightarrow S \mid\equiv C \mid\equiv \{E_c, EK_{cdc}\}_{K_{uc}}$	(2e)
(2e) $\wedge$ assumption (7) $\Rightarrow S \mid\equiv \{E_c, EK_{cdc}\}_{K_{uc}}$	(c)

(iv) Similarly, the above message and assumptions under the reasoning of the BAN logic rules lead to proof (d): $U \mid\equiv \{E_c, EK_{cdc}\}_{K_{uc}}$ (d)

In summary, the steps of the HIDA protocol have been proven to be secure by means of a formal language, and to satisfy the security properties of confidentiality, integrity, and authentication.

7. Efficiency Analysis

We conducted simulation testing on the overall model of the system in the Fabric network and implemented the chaincode related to HIDA user identity information registration. At the same time, we compared and displayed the performance indicators and key elements of each link. The relevant configuration of the experimental environment is detailed in Table 2.

Table 2. The experimental environment.

Name	Configure
Processor	Intel(R) Core(TM) i5-2430M
Run memory	4 GB
Operating System	Ubuntu 20.04
Docker	20.10.1
Docker-compose	1.25.0-rc1
Go	go1.14.6 linux/amd64
Fabric	2.3.0

7.1. Functional Testing

The HIDA functional test implemented a simple client. Firstly, xG, xH, G, and H were generated for user registration. The user's password was used as a parameter to call the user proof generation interface to produce the corresponding user proof string. Secondly, r, vG, and vH were generated for verifying the user's identity. After registration, the user would receive user challenge data, which, along with the password and user proof string, were used as parameters to call the user verification generation interface, generating the user verification string. The user proof string and the user verification string were used in the user identity access request and verify user identity access request, respectively.

During the registration process, the user provided their ID, username, and user-proof string to the CSP and called the user registration interface with the appropriate parameters to complete registration. The registration result contained the user's basic information (ID, username, and registration status), as well as the encrypted challenge encoded in Base64. The functionality was successfully executed and met expectations based on testing.

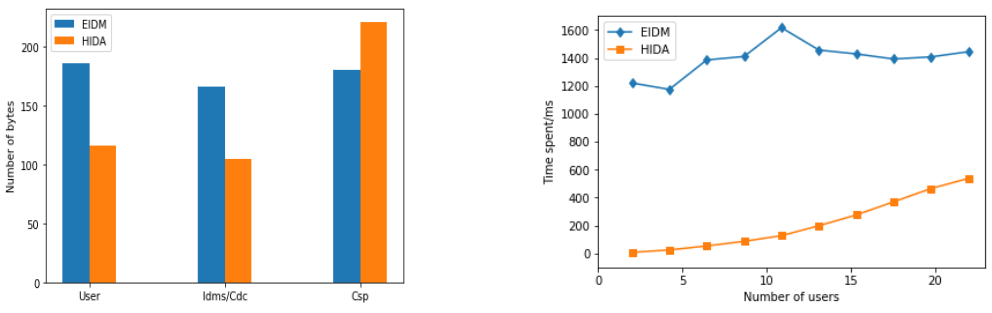
7.2. Performance Testing

The SIDM (Secure Identity Management) protocol is a privacy-preserving protocol designed with a zero-knowledge proof on the basis of the CIDM protocol, which solves the problems of the man-in-the-middle attack and user privacy leakage in traditional identity authentication. We have conducted corresponding comparative statistics on the data transmission of the three-party entities, and the results show that our scheme is significantly better than the above scheme in terms of data volume on both the user and authentication sides. Table 3 shows the relevant comparison data.

Table 3. The relevant comparison data.

	SIDM			**HIDA**		
	User	**Idms**	**Csp**	**User**	**Cdc**	**Csp**
Send (bytes)	106	50	110	100	8	113
Receive (bytes)	80	116	70	16	97	108
Total (bytes)	186	166	180	116	105	221

The authentication time of the designed HIDA scheme for different numbers of users was calculated using a Shell script. The authentication for each user count was statistically measured ten times, and the longest and shortest times were excluded before calculating the average. The results are shown in Figure 7. It can be observed from the results that the HIDA scheme performs significantly faster than the EIDM scheme for different numbers of users.



(**a**) (**b**)

Figure 7. (**a**,**b**) performance comparison.

7.3. Experimental Summary

The experimental results show that the HIDA protocol has the smallest byte-wise overhead in each step of the verification process. In addition, we compared the HIDA protocol with CIDM and EIDM protocols, and found that the HIDA protocol has a higher value in terms of privacy protection for users. Furthermore, we studied the time overhead of user verification between HIDA and EIDM. The experimental results demonstrate that the time overhead of the HIDA protocol for user verification is much lower than that of EIDM. This finding further confirms the innovation and value of the HIDA protocol in the field of privacy protection. Therefore, we believe that the HIDA protocol has broad application prospects, and future research can further explore its application in other fields.

8. Conclusions

The popularization of cloud computing has made our lives more convenient, but it has also brought many challenges to traditional identity authentication. To solve the problems of single point of failure, privacy security, efficiency, and transparency in traditional identity authentication in a cloud environment, this paper designs and implements the HIDA identity authentication scheme based on the Hyperledger Fabric platform, with the main work as follows:

This paper mainly introduces the HIDA identity authentication scheme designed based on the Hyperledger Fabric platform. First, we introduce the challenges faced by traditional identity authentication in cloud computing environments, including single points of failure, privacy security, efficiency, and transparency issues. Then, we elaborate on the design ideas and implementation of the HIDA scheme, including key technologies such as user identity information registration, user identity verification, and user access control. Finally, we conduct experimental simulations and performance tests to verify the security and efficiency advantages of the scheme.

Through the research in this paper, we have drawn the following conclusions: First, the HIDA scheme can effectively solve the privacy and security problems of traditional identity authentication in a cloud environment, ensuring the security and controllability of user data. Second, the HIDA scheme adopts modern cryptography technologies such as zero-knowledge proof, which can effectively avoid security threats such as man-in-the-middle attacks, ensuring the security of the system. Third, through experimental simulations and performance tests, we have verified the efficiency and superiority of the HIDA scheme under different numbers of users, demonstrating its practicality and feasibility. Overall, the HIDA identity authentication scheme designed and implemented in this paper is a feasible, secure, and efficient solution that can provide strong support and guarantees for identity authentication in the field of cloud computing. In the future, we will continue to optimize the scheme to improve its security and efficiency, better meeting user and market needs.

Since the birth of blockchain technology, its special underlying architecture and security model have been widely sought after. It has been widely used not only in the field of cryptocurrency but also in various work scenarios. In recent years, research combining blockchain technology with cloud computing has also increased. This combination is expected to bring better data security, higher efficiency, and lower costs. In the future, we hope to see more excellent solutions being borrowed and cited to better promote the development of this field.

Author Contributions: Methodology, W.J.; Formal analysis, W.J.; Investigation, Z.D. and Y.S.; Resources, X.R.; Data organization, C.T. and Y.S.; Writing-original draft, W.J.; Writing-review and editing, W.J., X.R. and Z.D.; Visualization, X.R.; Supervision, Z.D.; Funding acquisition, X.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research work was partially supported by the Shaanxi Natural Science Basic Research Project (Grant No. 2020JM-565), the Shaanxi International Science and Technology Cooperation Program Project (Grant No. 2021KW-07), and Xi'an Weiyang District Science and Technology Plan Project, No. 202025.

Informed Consent Statement: Not applicable.

Data Availability Statement: All the data are included in the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Leavitt, N. Is cloud computing really ready for prime time. *Growth* **2009**, *27*, 15–20. [CrossRef]
2. Li, W.; Wu, J.; Cao, J.; Chen, N.; Zhang, Q.; Buyya, R. Blockchain-based trust management in cloud computing systems: A taxonomy, review and future directions. *J. Cloud Comput.* **2021**, *10*, 35. [CrossRef]
3. Yao, Q.; Zhang, D. Survey on identity management in blockchain. *J. Softw.* **2021**, *32*, 2260–2286.
4. Carlin, S.; Curran, K. Cloud computing security. In *Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments*; IGI Global: Hershey, PA, USA, 2013; pp. 12–17.
5. Shukla, S.; Patel, S.J. A novel ECC-based provably secure and privacy-preserving multi-factor authentication protocol for cloud computing. *Computing* **2022**, *104*, 1173–1202. [CrossRef]
6. Goldwasser, S.; Micali, S.; Rackoff, C. The knowledge complexity of interactive proof-systems. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*; Association for Computing Machinery and Morgan & Claypool Publishers: Manhattan, NY, USA, 2019; pp. 203–225.
7. Kamboj, P.; Khare, S.; Pal, S. User authentication using Blockchain based smart contract in role-based access control. *Peer-to-Peer Netw. Appl.* **2021**, *14*, 2961–2976. [CrossRef]
8. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: A distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
9. Hammi, M.T.; Bellot, P.; Serhrouchni, A. BCTrust: A Decentralized Authentication Blockchain-Based Mechanism. In Proceedings of the 2018 IEEE Wireless Communications and Networking Conference (WCNC), Barcelona, Spain, 15–18 April 2018; pp. 1–6.
10. Suguna, M.; Anusia, R.; Shalinie, S.M.; Deepti, S. Secure Identity Management in Mobile Cloud Computing. In Proceedings of the 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Chennai, India, 23–25 March 2017; pp. 42–45.
11. Khalil, I.; Khreishah, A.; Azeem, M. Consolidated Identity Management System for secure mobile cloud computing. *Comput. Netw.* **2014**, *65*, 99–110. [CrossRef]
12. Jones, M.; Hardt, D. *No. RFC6750*; The Oauth 2.0 Authorization Framework: Bearer Token Usage; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2012.
13. Lundkvist, C.; Heck, R.; Torstensson, J.; Mitton, Z.; Sena, M. Uport: A Platform for Self-Sovereign Identity. 2017. Available online: https://whitepaper.uport.me/uPort_whitepaper_DRAFT20170221.pdf (accessed on 3 May 2023).
14. Shrier, D.; Wu, W.; Pentland, A. Blockchain & infrastructure (identity, data security). *Mass. Inst. Technol.-Connect. Sci.* **2016**, *1*, 1–19.
15. Tobin, A.; Reed, D. The inevitable rise of self-sovereign identity. *Sovrin Found.* **2016**, *29*, 18.
16. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
17. Gong, L.; Alghazzawi, D.M.; Cheng, L. BCoT sentry: A blockchain-based identity authentication framework for IoT devices. *Information* **2021**, *12*, 203. [CrossRef]
18. Gan, S. An IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices Using Blockchain. Master's Thesis, Indian Institute of Technology Kanpur, Kanpur, India, 2017.
19. Alsayed Kassem, J.; Sayeed, S.; Marco-Gisbert, H.; Pervez, Z.; Dahal, K. DNS-IdM: A blockchain identity management system to secure personal data sharing in a network. *Appl. Sci.* **2019**, *9*, 2953. [CrossRef]
20. Cheng, Y.; Jia, Z.; Gong, B.; Wang, L.P.; Lei, Y. F. Threshold Signature Scheme with Strong Forward Security Based on Chinese Remainder Theorem. In *Security and Privacy in New Computing Environments, Proceedings of the Second EAI International Conference, SPNCE 2019, Tianjin, China, 13–14 April 2019*; Springer International Publishing: Manhattan, NY, USA, 2019; pp. 15–28.
21. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
22. Rivest, R.L.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
23. Kaltz, J.; Lindell, Y. *Introduction to Modern Cryptography: Principles and Protocols*; CRC Press: Boca Raton, FL, USA, 2008.
24. Fiege, U.; Fiat, A.; Shamir, A. Zero knowledge proofs of identity. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, New York, NY, USA, 1 January 1987; pp. 210–217.
25. Canetti, R.; Goldreich, O.; Halevi, S. The random oracle methodology, revisited. *J. ACM* **2004**, *51*, 557–594. [CrossRef]
26. Wessels, J. Application of BAN-logic. *CMG Finance BV* **2001**, *19*, 23.