Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 903–914
DOI : 10.47974/JDMSC-1965

Privacy-preserving authentication and authorization in networks using blockchain

Asha Sanap *
Department of Electronics and Communication Engineering
School of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

Sulakshana Sagar Malwade †
Department of Computer Engineering
Dr. Vishwanath Karad MIT World Peace University
Department of Polytechnic and Skill Development
Pune
Maharashtra
India

Rohini Bhosale §
Department of Computer Engineering
Pillai HoC College of Engineering and Technology
University of Mumbai
Maharashtra
India

Aarti Karandikar ‡
Department of Computer Science and Engineering (Data Science)
Shri Ramdeobaba College of Engineering and Management
Nagpur
Maharashtra
India

---

* *E-mail:* asha.sanap@mitwpu.edu.in (Corresponding Author)
† *E-mail:* sulakshana.malwade@mitwpu.edu.in
§ *E-mail:* rohinijadhavphd@gmail.com
‡ *E-mail:* karandikara@rknec.edu

Anuradha A. Bakare [@]
Department of Electronics and Communication Engineering
School of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

Vaishali Langote [#]
Department of Computer Science
School of Polytechnic
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

Abstract

Blockchain-based solutions offer a promising avenue for privacy-preserving authentication and authorization mechanisms. Through the immutable and decentralized nature of blockchain, individuals can maintain control over their personal data while still engaging in secure transactions and interactions. These solutions leverage cryptographic techniques to ensure privacy, such as zero-knowledge proofs, which allow one party to prove possession of certain information without revealing the information itself.By storing authentication and authorization data on the blockchain, users can access services without having to repeatedly provide sensitive information. Smart contracts can automate authorization processes, ensuring that only authorized parties can access certain resources or perform specific actions. Additionally, blockchain-based identity systems offer a self-sovereign approach, where individuals have full control over their digital identities, reducing the reliance on centralized authorities. Moreover, blockchain networks provide transparency and auditability, allowing users to track how their data is being used and ensuring compliance with privacy regulations. However, challenges such as scalability, interoperability, and user adoption remain to be addressed for widespread implementation. Overall, blockchain-based solutions hold great potential in providing privacy-preserving authentication and authorization while empowering individuals with greater control over their data.Blockchain-based solutions offer a promising avenue for privacy-preserving authentication and authorization mechanisms. Through the immutable and decentralized nature of blockchain, individuals can maintain control over their personal data while still engaging in secure transactions and interactions. These solutions leverage cryptographic

[@] *E-mail:* **anuradha.bakare@mitwpu.edu.in**
[#] *E-mail:* **vaishali.langote@mitwpu.edu.in**

techniques to ensure privacy, such as zero-knowledge proofs, which allow one party to prove possession of certain information without revealing the information itself.

Subject Classification: *68M25.*

Keywords: *Blockchain, Privacy-preserving, Authentication, Authorization, Self-sovereign identity.*

1. Introduction

In a time when using technology to do everything is so common, privacy and data protection is very important [1]. Users often have to give out private and sensitive information when using old-fashioned login and permission methods. This leaves them open to identity theft and improper access. New blockchain-based solutions, on the other hand, look like a good option. They offer privacy-protecting [2] identification and permission systems and give people more control over their digital IDs. Blockchain technology was first created as the foundation for cryptocurrency like Bitcoin. It has since grown into a flexible tool that can be used in many fields, such as identity management and protection.

At its core, blockchain is a decentralized, [3] unchangeable ledger that is kept up by a network of nodes. It safely records events in the order they happened. Because blockchain is spread, it is open, strong, and hard to change. This makes it a great choice for building trust in digital exchanges. Cryptographic methods are used to protect the privacy and security of private information during identification and authorization using blockchain. One important idea is zero-knowledge proofs, [4] which let one person (the prover) show that they know something to another person (the checker) without giving away the information. Blockchain-based identity systems also allow people to be self-sovereign, which means they

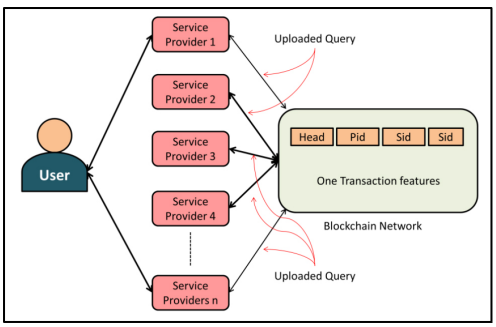

Figure 1

have full control over their digital identities. Users don't have to rely on third-party identity companies to handle and prove their names. This makes it easier for privacy and lowers the risk of identity theft. People can safely prove who they are on different sites without putting their privacy at risk by using cryptographic keys and digital signatures [5].

Blockchain networks also offer openness and auditability, which lets users see how their data is being used and makes sure that privacy laws are followed. Every activity on the blockchain is permanent and recorded with a time stamp [6]. This makes it possible to see exactly who accessed and used data and when. This makes people more responsible and builds trust between people in digital exchanges.Even though there might be benefits, problems like scale, openness, and user adoption are still stopping blockchain-based identity and authorization solutions from being widely used [7].

2. Methodology

The above Figure 1 shows, the overview of the architecture, whereas Figure 2 show the process of Transaction and structure. Whereas Figure 3 Illustrating the Authentication and Authorization Phase for Blockchain-Based Solutions for Privacy-Preserving Authentication and Authorization.

2.1 *Advisory Control mechanism*

1. Adversary Capability: We assume the existence of a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ with the capability to impersonate service providers (SP) or mobile users and perform various attacks.

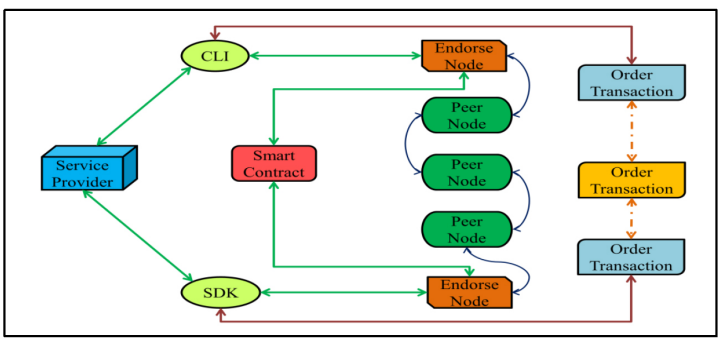

Figure 2

Processof Transaction and Structure

2. Control Over Public Channel: The adversary $\mathcal{A}$ can control the public channel between users (Ui) and service providers (Sj), allowing for message injection, blocking, eavesdropping, and tampering. Mathematically, this can be represented as:
3. Adversary Control:
   - $\mathcal{A}$ controls public channel between Ui and Sj

   Obtaining Authentication Factors: $\mathcal{A}$ can obtain either the mobile device or the password, representing the two authentication factors. Additionally, $\mathcal{A}$ can extract secret information from the mobile device and enumerate the password space $|DPW|$ using offline dictionary attacks. Mathematically:
4. Adversary Obtains Factors:
   - $\mathcal{A}$ obtains mobile device or password

   Offline Dictionary Attacks: The adversary $\mathcal{A}$ can perform offline dictionary attacks to enumerate the password space $|DPW|$. This involves attempting various combinations of passwords until a match is found. Mathematically:
5. Offline Dictionary Attacks:
   - $\mathcal{A}$ enumerates password space $|DPW|$

2.2 *Security*

In a Mobile Cloud Computing (MCC) structured service model, [8] the security needs for a blockchain-based identification and permission method cover a number of important areas. The first thing the plan needs to do is make sure that both the mobile user and the service provider can safely verify each other's names. Multi-factor security is an extra layer of safety that uses more than one way to prove who you are, like fingerprints, codes, or passwords. This lowers the chance of getting in without permission, even if one of the factors is broken [9].To stop bad people from getting in without permission or messing with security processes, it's important to protect against wrong password login/update attacks and reply attacks. There should be ways in the plan to find and stop these kinds of threats [11].

3. Smart Contact of proposed Method

3.1 *Initialization Phase*

In the initialization phase [10] of the consortium blockchain network, authorized Service Providers (SPs) become nodes in the network. The Manager of the consortium blockchain (MSP) selects cryptographic parameters including an additive group of points G with order q, where P serves as a generator of G. Additionally, six hash functions $h0$, $h1$, $h2$, $h3$, $h4$, $h5$ are chosen to ensure security. Each SP generates a private key SK_Sj and computes its public key $PK\_Sj = SK\_Sj * P$, registering it with MSP. SPs also publish their privilege unit price lists on their websites. On the blockchain, smart contracts (Algorithms 1–4) are initialized and deployed. MSP publishes the selected parameters $\{G, q, P, PK\_Sj, h0, h1, h2, h3, h4, h5\}$ for network consistency and security. This initialization phase establishes the foundation for secure and transparent interactions within the consortium blockchain network.

3.2 *User registration Phase*

Step 1: User Ui selects an SP Srj closest to the mobile device MD, chooses a random number $SKUi \in Zq^*$, and generates a service subscription list L recording desired privileges, service periods, and payment amounts. MD calculates the public key $PKUi = SKUi \cdot P$ and $PIDi = h5(PKUi)$. Then, MD generates a signature $Sui = Sig(SKUi, PIDi \,||\, T1 \,||\, L)$ and a NIZK proof. Finally, Ui transmits $\{PIDi, PKUi, SUi, L, reg, T1, \pi\}$ to Srj and pays service fees securely.

Step 2: Upon receiving the message at time 2T2, Srj checks $|T2 - T1| < \Delta T$ and validates π to confirm PKUi validity. If valid, Srj confirms $(PKUi, SUi, PIDi \,||\, T1 \,||\, L) = 1$, checks fee equivalence, computes SRSj, and submits the registration transaction to the blockchain.

Step 3: Transaction processing is explained in Section 4.3. Smart contract Algorithm 2 verifies the transaction, recalculates costs, and checks fee correctness for each SP. Satisfied conditions lead to blockchain storage; otherwise, Srj interrupts and refunds fees.

Step 4: Upon receipt, Ui inputs $PWUi$ into MD, generates $Zi = h0(PIDi \,||\, PWUi \,||\, bi)$, $Fi = (SKUi \,||\, T1) \oplus Zi$, and $V = h3(h2(SKUi \,||\, T1 \,||\, Zi))$. Finally, Ui stores Fi, V, bi, PKUi, π, and L securely.

Step 5: All SPs request subscription fees from Srj off-chain based on acceptance SP identity IDSj and transaction list L.

Algorithm:

1: Initialize variable U as a User instance with attributes PIDi,UPKi,IDSj,PKSj,L,1T1,SUI,and SRSj.
2: Retrieve the latest transaction U* associated with the Personal ID PIDi from the key-value database to verify the uniqueness of the user identity.
3: If *≠NullU*=Null,then return an error message stating "User is already registered".
4: Extract the service subscription list L from U.
5: Iterate through each Service Provider (SP) j inL.
6: Calculate the unit price UPSj of the access privilege LP[j] on SP Sj.
7: Compute the total cost cost=UPSj×LDSj for each service subscribed.
8: If the calculated cost costcost does not match the recorded cost LC[j] in L, return an error message indicating that either the subscription list is incorrect or the user did not pay enough.
9: Store the transaction U in the blockchain.
10: Finish user registration and subscription.
11: Return a success message indicating "Mobile user is successfully registered!".

4. Authentication and Authorization Phase

The authentication and authorization phase for blockchain-based solutions for privacy-preserving authentication and authorization into a mathematical model step by step:

Step 1: User Initialization

Each user Ui initializes their identity by generating a pair of cryptographic keys: a public key PKUi and a private key SKUi.

$$(PKUi, SKUi) = KeyGen()$$

Step 2: Service Provider (SP) Registration

Each SP Sj registers on the blockchain network by generating a public-private key pair (PKSj, SKSj) and publishing its public key.

$$(PKSj, SKSj) = KeyGen()$$

Step 3: User Authentication Request

User Ui sends an authentication request to an SP Sj by transmitting their identity PIDi, public key PKUi, and authentication data.

$$AuthRequest = (PIDi, PKUi, AuthData)$$

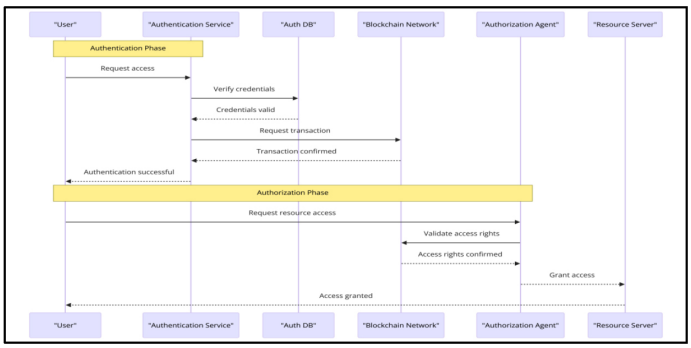

Figure 3

Illustrating the Authentication and Authorization Phase for Blockchain-Based Solutions for Privacy-Preserving Authentication and Authorization

Step 4: SP Verification and Authentication

Upon receiving the authentication request, SP Sj verifies the user's identity and authenticity by validating the user's public key and authentication data.

Step 5: Blockchain Verification

After successful verification by SP Sj, the authentication request details are recorded on the blockchain for transparency and accountability.

$$Transaction = (PIDi, PKUi, AuthData, Timestamp)$$

Step 6: Authorization Decision

Upon successful authentication, SP Sj makes an authorization decision based on the user's identity and requested actions.

Step 7: Access Granted

If the authorization decision is positive, SP Sj grants access to the requested resources or services to user Ui.

Step 8: Blockchain Logging

The access granted event is logged on the blockchain for audit and accountability purposes.

$$Transaction = (PIDi, Action, Timestamp)$$

5. Performance Analysis

Table 1 shows the operational running time (in milliseconds) for different types of users and Service Providers (SPs). Users' time is made up of things like temporary storage (Tmp), session management (Tsm),

hashing (Th), file encryption (Tfe), mobile computation (Tmc), blockchain processing (Tbp), payment authentication (Tpa), and the expiration of private keys (Texp).

Table 1

Operational Running time for user and SP

Parameter	User	SP
Tmp	34.25	5.23
Tsm	14.23	2.35
Th	33.45	6.45
Tfe	56.23	3.25
Tmc	12.45	4.56
Tbp	56.23	1.75
Tpa	44.12	1.14
Texp	18.05	2.15

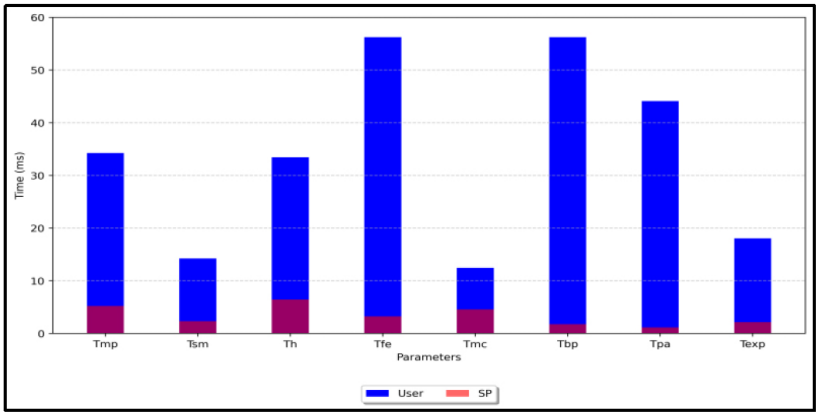

Figure 4

Operational running time for users and Service Providers (SPs) across different parameters

It is shown in Figure 4 and 5 how long each method takes to run for both people and SPs, as well as how much it costs in milliseconds. There is a comparison of the different authentication methods in Table 2 based on how quickly they can be used. AES (Advanced Encryption Standard), Asymmetric encryption, a Hybrid system that combines symmetric and asymmetric encryption and the proposed method are some of the methods.

Table 2

Authenticator Phase and Computational Comparison

Method	User (ms)	SP (ms)	Final Cost (ms)
AES	79.25	12.56	90.23
Asymmetric	65.25	11.25	75.33
Hybrid	26.35	2.65	30.26
Propsoed	40.56	10.45	52.34

It is shown in figure 4 how long each method takes to run for both people and SPs, as well as how much it costs in milliseconds. It has been seen that the proposed method strikes a middle ground between security and processing efficiency, scoring somewhere in the middle of the other methods. Even though AES works well for SPs, it costs more to run for users, which could mean problems with scaling.

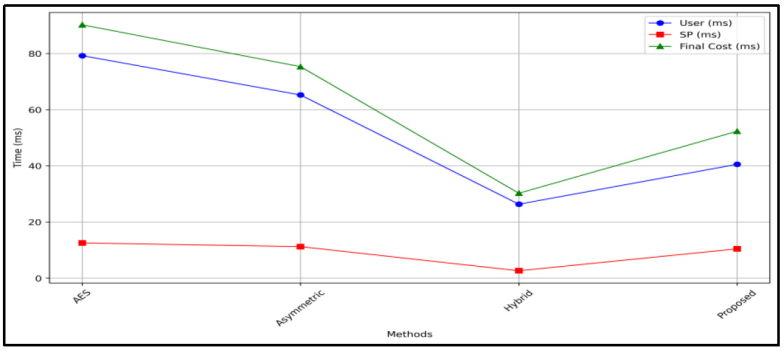

Figure 5

Authentication Methods and Computational Comparison

6. Conclusion

Blockchain-based solutions look like they could help make identification and authorization systems in network settings more private. By using autonomous and unchangeable ledgers, these solutions deal with important issues like keeping data safe, being open, and having faith in identification processes. Blockchain networks use cryptography to make sure that users are who they say they are. They also protect users' privacy by keeping private data from getting out.Adding smart contracts also makes it possible to automate the permission process, which makes

sure that rules for access control are followed in a clear and effective way. It's important to remember, though, that blockchain-based solutions don't come without costs. Scalability, interoperability, and legal compliance are still issues that need to be fixed before it can be used by more people.

References

[1] AlAhmad, A.S.; Kahtan, H.; Alzoubi, Y.I.; Ali, O.; Jaradat, A. Mobile cloud computing models security issues: A systematic review. *J. Netw. Comput. Appl.*, 190, 103152 (2021).

[2] Li, Z.; Wang, D.; Morais, E. Quantum-Safe Round-Optimal Password Authentication for Mobile Devices. *IEEE Trans. Dependable Secur. Comput.*, 19, 1885–1899 (2022).

[3] He, D.; Zeadally, S.; Kumar, N.; Wu, W. Efficient and Anonymous Mobile User Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server Architectures. *IEEE Trans. Inf. Forensics Secur.*, 11, 2052–2064 (2016).

[4] He, D.; Kumar, N.; Khan, M.K.; Wang, L.; Shen, J. Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. *IEEE Syst. J.*, 12, 1621–1631 (2018).

[5] Roy, S.; Das, A.K.; Chatterjee, S.; Kumar, N.; Chattopadhyay, S.; Rodrigues, J.J.P.C. Provably Secure Fine-Grained Data Access Control Over Multiple Cloud Servers in Mobile Cloud Computing Based Healthcare Applications. *IEEE Trans. Ind. Inform.*, 15, 457–468 (2019).

[6] M. Kuperberg, "Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective," in *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008-1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[7] B. Yousra, S. Yassine, M. Yassine, S. Said, T. Lo'ai and K. Salah, "A Novel Secure and Privacy-Preserving Model for OpenID Connect Based on Blockchain," in *IEEE Access*, vol. 11, pp. 67660-67678 (2023), doi: 10.1109/ACCESS.2023.3292143.

[8] A. Lahbib, K. Toumi, A. Laouiti and S. Martin, "Blockchain based Privacy Aware Distributed Access Management Framework for Industry 4.0," 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, pp. 51-56 (2021), doi: 10.1109/WETICE53228.2021.00021.

[9] Limkar, Suresh, Ashok, Wankhede Vishal, Singh, Sanjeev, Singh, Amrik, Wagh, Sharmila K. & Ajani, Samir N. A mechanism to ensure identity-based anonymity and authentication for IoT infrastructure using cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1597–1611 (2023).

[10] S. Paavolainen and C. Carr, "Security properties of light clients on the Ethereum blockchain", *IEEE Access*, vol. 8, pp. 124339-124358 (2020).