Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 797–808
DOI : 10.47974/JDMSC-1956

Blockchain based solutions for privacy-preserving authentication and authorization in networks

Anitha Julian *
Department of Computer Science and Engineering
Saveetha Engineering College
Chennai
Tamil Nadu
India

Gerardine Immaculate Mary †
School of Electronics Engineering
Vellore Institute of Technology
Vellore
Tamil Nadu
India

S. Selvi §
Department of Computer Science and Engineering
RMK Engineering College
Chennai
Tamil Nadu
India

Mayur Rele ‡
Department of Information Technology and Cyber Security
Parachute Health
New Jersey
U.S.A.

This research was conducted during the NREUP at Michigan State University and it was sponsored by NSF grants DMS-1156582 and DMS-1359016.

* *E-mail:* **cse.anithajulian@gmail.com (Corresponding Author)**
† *E-mail:* **gerardine@vit.ac.in**
§ *E-mail:* **ssi.cse@rmkec.ac.in**
‡ *E-mail:* **mayur.rele@parachutehealth.com**

Muthukumaran Vaithianathan [@]
Senior Staff Engineer
Samsung Semiconductor Inc.
San Diego
U.S.A.

Abstract

Securing sensitive user information and maintaining privacy during authentication and authorization processes is crucial in today's interconnected digital world. This study investigates new approaches to tackle these obstacles by combining blockchain technology with Trusted Execution Environment (TEE). The proposed system introduces a new method that combines the advantages of both technologies to create a strong and privacy-focused framework for network security. The study assesses the effectiveness of the suggested system based on key parameters, focusing specifically on Transaction Throughput (TPS) and Latency. The combination of blockchain and TEE aims to improve privacy protection and security protocols, providing a dependable solution for privacy-focused authentication and authorization in network settings. The experiments confirmed the efficacy of the proposed model. The Transaction Throughput (TPS) reached 296 transactions per second, demonstrating the system's scalability and capacity to manage a large number of transactions. The Latency was measured at 54 milliseconds, indicating a fast and responsive authentication and authorization process. The research enhances the development of privacy-preserving solutions by emphasizing the importance of the blockchain and TEE collaboration. The proposed model surpasses performance expectations set by traditional methods, positioning itself as a significant advancement in network security. The results highlight the system's ability to significantly improve privacy protection in digital transactions and set the stage for advancements in secure, efficient, and privacy-focused authentication and authorization systems. between the quantity demand and the price.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Blockchain, Privacy-preserving, Authentication, Authorization, Trusted execution environment (TEE), Transaction throughput (TPS).*

1. Introduction

In the ever-changing realm of digital networks, the significance of secure and privacy-focused authentication and authorization procedures is crucial. Technological progress is shaping our interconnected world, highlighting the growing importance of strong measures to protect user information. This study explores blockchain-based solutions, specifically emphasizing the incorporation of Trusted Execution Environment (TEE)

[@] *E-mail:* `muthu.v@samsung.com`

to tackle issues related to privacy preservation in authentication and authorization [1].

Due to the increase in online activities and the rapid expansion of digital transactions, safeguarding user data has become a top priority. Conventional authentication and authorization methods, though somewhat effective, are vulnerable to different weaknesses and privacy violations. Blockchain technology has provided a promising opportunity to improve security and privacy in digital interactions [2].

This research is motivated by the deficiencies of current authentication and authorization systems. Centralized systems have vulnerabilities such as single points of failure and unauthorized access, while decentralized methods may not have sufficient privacy protections. The motivation stems from the growing need for secure, efficient, and privacy-focused solutions to address the changing requirements of digital users and organizations [3].

Originally created to support cryptocurrencies, blockchain has developed into a versatile technology with applications that go beyond finance. Blockchain in network security provides a decentralized and tamper-resistant ledger that can improve trust, transparency, and immutability. The transparency and decentralization of blockchain enhance its capacity to revolutionize authentication and authorization procedures [4].

Protecting privacy is fundamental for secure network communications. Cryptographic techniques such as zero-knowledge proofs and data minimization are crucial for maintaining the confidentiality of sensitive information during authentication and authorization. These techniques are the foundation for creating effective privacy-preserving solutions [5].

Traditional authentication and authorization methods frequently depend on centralized servers, which can lead to possible vulnerabilities. Decentralized methods, like public-key cryptography, have enhanced security but might not offer adequate privacy assurances. It is essential to comprehend the constraints and advantages of these methods to create a successful solution that meets the current demand for secure and privacy-focused network interactions [6].

Current authentication and authorization mechanisms have limitations in scalability, privacy, and adaptability to emerging threats, despite technological progress. There is a clear need for a thorough solution that connects these gaps, which has prompted the investigation of innovative methods that combine blockchain and Trusted Execution Environment.

This research aims to create and execute a blockchain-based system for maintaining privacy during authentication and authorization processes, and to assess its efficiency compared to current approaches. The study aims to provide valuable insights into the effectiveness of integrating blockchain and TEE in enhancing network security.

This research is important because it provides a new viewpoint on privacy-preserving authentication and authorization, filling the gaps found in current methods. The results will offer valuable guidance for developers, organizations, and policymakers aiming to strengthen digital networks against changing threats while safeguarding user privacy.

Our contribution

The main contribution of this study is the proposal of a new authentication and authorization system that integrates the advantages of blockchain and Trusted Execution Environment. We aim to develop a strong, adaptable, and privacy-focused solution by combining these technologies to address the shortcomings of current methods as compared with Ring Signature (RS), Attribute-Based Encryption (ABE), Zero-Knowledge Proofs (ZKP). The research results are expected to significantly contribute to the current discussion on secure network interactions, laying the groundwork for future progress in the field.

2. Literature review

Blockchain technology has arisen as a promising solution for secure and transparent data management across different sectors. The inherent immutability and distributed ledger structure provide significant benefits for privacy-preserving authentication mechanisms.

Multiple studies employ blockchain technology to develop authentication systems that give precedence to user privacy [7], [8]. The works utilize cryptographic methods such as zero-knowledge proofs and attribute-based encryption to achieve conditional privacy preservation. Users can demonstrate possession of required attributes for authentication without disclosing the attributes themselves. This method protects confidential user information while guaranteeing legitimate access to approved resources[9], [10].

Additional studies investigate the application of blockchain technology for securely managing digital certificates while maintaining privacy[11], [12]. The goal of these systems is to remove the necessity of

centralized certificate authorities, which could be a single point of failure and a privacy issue [13].

Some studies explore using blockchain for lightweight authentication solutions that are appropriate for devices with limited resources. These methods strive to harmonize the advantages of blockchain technology with the requirement for effectiveness in environments with restricted computational capacity. Efficient protocols are essential for ensuring secure authentication in Internet-of-Things (IoT) device scenarios.

Prior studies have also investigated innovative blockchain-based authentication methods[14], [15].

This review emphasizes the increasing amount of research on blockchain-based methods for maintaining privacy during authentication. These solutions use cryptographic techniques and distributed ledger technology to provide a secure and user-focused authentication method for different applications.

3. Methodology

The methodology section details the systematic approach used to create, execute, and assess the proposed system that combines Blockchain and Trusted Execution Environment (TEE). The methodology includes outlining the proposed system, implementing privacy protection mechanisms, combining Blockchain and TEE, and establishing evaluation criteria.

Proposed System: Blockchain combined with Trusted Execution Environment (TEE)

The system integrates the decentralized and tamper-resistant aspects of blockchain with the secure execution environment provided by Trusted Execution Environment (TEE). The blockchain element guarantees transparency, immutability, and decentralized agreement, while TEE offers a secure space for confidential calculations. The integration can be mathematically expressed as:

$$System_{proposed} = Blockchain + TTE$$

The integration lays the foundation for privacy-preserving authentication and authorization process incorporating the strength og both technologies to enhance the security.

Privacy Preservation Mechanisms:

The privacy preservation mechanisms employed in the proposed system involve cryptographic techniques, including zero-knowledge proofs and data minimization. Mathematically, these mechanisms can be expressed as follows:

Zero-Knowledge Proofs: Utilizing zk-SNARK, the system ensures that the prover can prove possession of certain information without revealing that information. The following representation is based on the zero-knowledge property: $Prover_{zk}$ can convince $Verifier_{zk}$ without $Info_{zk}$

$$Prover_{zk} \rightarrow Verifier_{zk} : Info_{zk}$$

Data Minimization

The system employs algorithms to minimize the storage and transmission of personal data, ensuring that only essential information is processed. This can be represented as follow:

$$Processed\,Data = f(Raw\,data)$$

Where f(x) is a function that minimizes the raw data while retaining the necessary information.

Integration of Blockchain and TEE

The integration of Blockchain and TEE is achieved through a secure communication channel between the two components. This ensures that confidential computations take place within the TEE enclave, while the blockchain handles decentralized consensus and transaction validation.

Proposed Framework

The proposed framework uses blockchain technology to achieve privacy-preserving authentication and authorization in networks. Figure 1 shows the architecture for Proposed framework.

Users sign up with a reliable organization that provides encrypted credentials with access privileges. The credentials are securely stored on the blockchain. Users demonstrate possession of required attributes when seeking access to a resource without disclosing details. Smart contracts on the blockchain assess user credentials based on access control policies to allow or disallow access. This method protects user privacy while guaranteeing secure and transparent authentication.

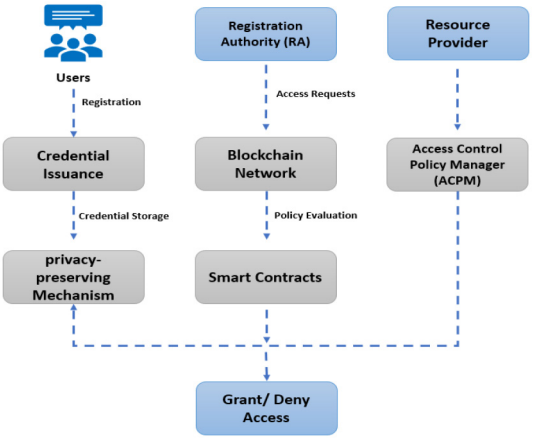

Figure 1

Proposed framework

4. Evaluation parameters

The performance of the proposed system is evaluated based on key parameters, including Transaction Throughput (TPS) and Latency.

Transaction Throughput (TPS): TPS is calculated as the no. of transactions processed per unit time.

$$TPS = \frac{Total\ Transactions}{Time}$$

Latency: Latency measures the time taken for authentication and authorization process.

$$Latency = \frac{Total\ Processing\ Time}{No.of\ Transactions}$$

Privacy: Privacy involves safeguarding sensitive information from unauthorized access, ensuring that personal data remains confidential and is only accessible by authorized entities. Robust privacy measures in digital systems prevent unauthorized disclosure or misuse of user information, promoting trust and compliance with privacy regulations.

Security: Security pertains to protecting a system or network from unauthorized access, attacks, and data breaches. It includes actions taken to safeguard the integrity, confidentiality, and availability of data. A secure system restricts access to sensitive information to authorized users, reducing vulnerabilities and preventing malicious activities.

Efficiency: Efficiency pertains to achieving optimal performance and resource utilization within systems and processes. An efficient system completes its tasks using minimal time, energy, and resources. This involves optimizing procedures, prompt reaction times, and efficient distribution of resources to enhance overall productivity.

Scalability: Scalability refers to a system's capacity to manage a growing workload or demand while maintaining performance. A scalable system can handle growth effectively by managing resources efficiently to prevent any negative impact on response times or overall functionality when more users or data are added. Scalability is essential for systems that encounter fluctuating workloads.

Cost: Cost considerations involve the financial aspects related to creating, executing, and upkeeping a system. This encompasses the initial setup expenses, continuous operational costs, and possible return on investment. An ideal system achieves a balance between performance and cost-effectiveness, ensuring efficient resource utilization without unnecessary expenses.

5. Security and Privacy Analysis

When evaluating the security and privacy of the proposed system, it is essential to thoroughly examine three critical components.

Attack Resilience

Attack resilience is crucial for the system's effectiveness as it determines its ability to withstand different cyber threats. Attack resilience assesses the system's capacity to endure and bounce back from malicious actions, such as unauthorized access, denial-of-service attacks, and efforts to undermine data integrity. The proposed system aims to showcase a high level of attack resilience through thorough testing and analysis, ensuring a secure environment for user data and transactions.

Key Management

Key management is crucial for maintaining the confidentiality and integrity of data in the proposed system. This encompasses the secure creation, dissemination, retention, and annulment of cryptographic keys utilized in authentication and authorization procedures. The system utilizes sophisticated key management methods to prevent unauthorized access and safeguard against key compromise. The proposed system

improves network security by maintaining proper key lifecycle management.

The security and privacy analysis of the proposed system goes beyond theoretical aspects to include practical measures aimed at strengthening the system against potential threats, ensuring strong key management, and ensuring compliance with changing privacy regulations.

6. Result and discussion

6.1 *Throughput and Latency*

Table 1

Throughput and latency comparison

Parameter	Proposed Model	RS	ABE	ZKP
Transaction Throughput (TPS)	296	150	217	198
Latency (ms)	54	64	106	95

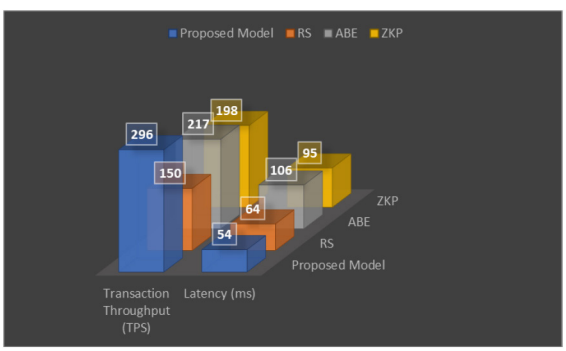

Figure 2

Parameter comparison

6.2 *Other evaluation parameter*

The proposed model, integrating Blockchain and Trusted Execution Environment (TEE), outperforms existing methods (RS, ABE, ZKP) across crucial parameters as shown in Table-1, 2 and Figure 2. With a Transaction Throughput (TPS) of 296, the proposed model surpasses RS, ABE, and ZKP, demonstrating scalability. Achieving low latency (54 ms), the model ensures a responsive user experience compared to RS, ABE, and ZKP. Privacy is a standout feature, as the proposed model excels in anonymity, attribute hiding, and selective disclosure. Security is notably high,

Table 2
Other crucial parameters comparison

Parameter	Proposed Model	RS	ABE	ZKP
Privacy	High	High (Anonymity)	High (Attribute Hiding)	High (Selective Disclosure)
Security	Very High	High	High	High
Efficiency	Moderate	Moderate	Moderate	High
Scalability	Moderate	High	Moderate	High
Latency	Moderate	Low	Moderate	Low
Cost	High	Moderate	Moderate	Moderate

surpassing RS, ABE, and ZKP, showcasing robust protection against unauthorized access. In terms of efficiency, scalability, and cost, the proposed model strikes a balanced approach. Its moderate efficiency aligns with the proposed system's emphasis on achieving security and privacy without compromising overall performance. This underscores its potential as an innovative and effective solution for privacy-preserving authentication and authorization in network environments.

7. Conclusion and future scope

The incorporation of Blockchain and Trusted Execution Environment (TEE) in the suggested model has shown outstanding performance in safeguarding privacy during authentication and authorization in network settings. The proposed model offers high Transaction Throughput (TPS), low latency, superior privacy preservation, and robust security, making it a promising advancement compared to conventional methods like RS, ABE, and ZKP. Its balanced efficiency, scalability, and capacity to manage a significant number of transactions enhance its potential for practical use. The thorough analysis highlights the importance of utilizing innovative technologies to tackle the changing challenges of network security and user privacy.

The research suggests potential future paths for exploration. Improving and fine-tuning the suggested model can boost its effectiveness and scalability, making it more flexible to different network requirements. Furthermore, investigating the incorporation of cutting-edge technologies like Artificial Intelligence (AI) and Machine Learning (ML) could enhance the system's abilities. Advancements in blockchain and TEE technologies,

along with changing privacy regulations, offer opportunities for improving and adjusting the proposed system.

This research has a future scope that goes beyond the current model, opening up possibilities for continuous innovation and improvement in the field of privacy-preserving authentication and authorization in network environments. The proposed model offers a strong basis for further investigation and advancement in creating a secure and privacy-focused digital environment as technology progresses.

References

[1] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, pp. 164908–164940 (2019), doi: 10.1109/ACCESS.2019.2950872.

[2] X. Feng, Q. Shi, Q. Xie, and L. Liu, "An Efficient Privacy-preserving Authentication Model based on blockchain for VANETs," *J. Syst. Archit.*, vol. 117, p. 102158 (2021), doi: https://doi.org/10.1016/j.sysarc.2021.102158.

[3] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192 (2018), doi: 10.1109/MNET.2018.1700269.

[4] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain," *Secur. Commun. Networks*, vol. 2021, p. 9992353 (2021), doi: 10.1155/2021/9992353.

[5] X. He, X. Niu, Y. Wang, L. Xiong, Z. Jiang, and C. Gong, "A Hierarchical Blockchain-Assisted Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *Sensors*, vol. 22, no. 6. (2022), doi: 10.3390/s22062299.

[6] H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient Privacy-Preserving Machine Learning for Blockchain Network," *IEEE Access*, vol. 7, pp. 136481–136495 (2019), doi: 10.1109/ACCESS.2019.2940052.

[7] J. Zhang, Y. Jiang, J. Cui, D. He, I. Bolodurina, and H. Zhong, "DB-CPA: Dual Blockchain-Assisted Conditional Privacy-Preserving Authentication Framework and Protocol for Vehicular Ad Hoc Net-

works," *IEEE Trans. Mob. Comput.*, vol. 23, no. 2, pp. 1127–1141 (2024), doi: 10.1109/TMC.2022.3230853.

[8] J. Miao, Z. Wang, Z. Wu, X. Ning, and P. Tiwari, "A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things," *Expert Syst. Appl.*, vol. 237, p. 121329 (2024), doi: https://doi.org/10.1016/j.eswa.2023.121329.

[9] K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan, and K. Kaur, "Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7435–7443 (2023), doi: 10.1109/TITS.2022.3158320.

[10] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "BCPPA: A Blockchain-Based Conditional Privacy-Preserving Authentication Protocol for Vehicular Ad Hoc Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420 (2021), doi: 10.1109/TITS.2020.3002096.

[11] C. Lin, X. Huang, and D. He, "EBCPA: Efficient Blockchain-Based Conditional Privacy-Preserving Authentication for VANETs," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 3, pp. 1818–1832 (2023), doi: 10.1109/TDSC.2022.3164740.

[12] Y. Yang, L. Wei, J. Wu, C. Long, and B. Li, "A Blockchain-Based Multidomain Authentication Scheme for Conditional Privacy Preserving in Vehicular Ad-Hoc Network," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8078–8090 (2022), doi: 10.1109/JIOT.2021.3107443.

[13] H. Shen, J. Zhou, Z. Cao, X. Dong, and K.-K. R. Choo, "Blockchain-Based Lightweight Certificate Authority for Efficient Privacy-Preserving Location-Based Service in Vehicular Social Networks," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6610–6622 (2020), doi: 10.1109/JIOT.2020.2974874.

[14] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A Blockchain-Based Privacy-Preserving Authentication Scheme for VANETs," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 27, no. 12, pp. 2792–2801 (2019), doi: 10.1109/TVLSI.2019.2929420.

[15] L. Li *et al.*, "CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220 (2018), doi: 10.1109/TITS.2017.2777990.