ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

SECURE AND PRIVATE ANALYTICS OF HEALTHCARE RECORDS IN MULTI-TENANT CLOUD ENVIRONMENTS USING BLOCKCHAIN

K. VIJAY KUMAR [1], THALLURI KEERTHANA[2], K. KARTHEEK REDDY[3], TUNGANA PRANNAV[4], S. SHIVA SHANKHAR[5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus**,** Ibrahimpatnam, Telangana, India

ABSTRACT— Given the sensitivity of personal health information and the rising prevalence of data breaches, healthcare analytics faces a significant challenge in ensuring the privacy of sensitive data while simultaneously providing valuable insights. By incorporating privacy-preserving parameters, zero-knowledge proofs (zk-SNARKs), blockchain technology, and a multi-tenant cloud environment, the secure framework presented in this paper addresses these issues. The framework ensures that healthcare records remain protected during analytics computations without exposing raw data by employing cuttingedge cryptographic methods, particularly zk-SNARKs. In order to validate computations, the privacy-preserving analytics engine makes use of anonymized healthcare records and generates zk-SNARKs. When these proofs are incorporated into a blockchain network, they produce a transparent, tamper-proof ledger that guarantees safe healthcare transactions. This strategy is absolutely necessary in circumstances like telemedicine, where secure data sharing and computation are of the utmost importance. By demonstrating its application in a telemedicine app, the framework provides a scalable and secure solution to a pressing issue, demonstrating its practical significance in healthcare analytics.

Index Terms – Blockchain, Healthcare Data Security, Privacy Preservation, Multi-Tenant

Cloud Computing, Electronic Health Records (EHR), Secure Data Analytics, Access Control, Smart Contracts, Data Integrity, Encryption, Cloud Security, Decentralized Storage, Confidentiality, Healthcare Information Systems.

I. INTRODUCTION

The advent of healthcare analytics has revolutionized the way we derive insights from vast and complex datasets. However, safeguarding the privacy of sensitive healthcare data remains a significant challenge, particularly in collaborative environments. This paper addresses this challenge by proposing a novel framework for privacy-preserving healthcare analytics that leverages zero-knowledge proofs (zk-SNARKs), blockchain technology, and a multi-tenant cloud environment. Healthcare records house an abundance of sensitive information, from patient identities to intricate medical histories. The associate editor coordinating the review of this manuscript and approving it for publication was Amjad Mehmood . Traditional cryptographic methods, while effective in securing data at rest, often fall short in protecting data during analytics computations. We integrate zk-SNARKs into our approach to enable privacy-preserving analytics, enabling validation of computation correctness without revealing any raw data. This is particularly significant in multi-tenant cloud environments, where secure data sharing and processing are essential for healthcare advancements, telemedicine, and policy-making. Our proposed framework offers a cryptographic solution that ensures healthcare records remain private during analytics computations. By integrating zk-SNARKs with blockchain, we create a transparent and tamper-proof environment where privacy is preserved without compromising the integrity or utility of the data. The primary objective of this study is to introduce and comprehensively analyze the proposed algorithm, highlighting its effectiveness in addressing the intricate balance between data utility and privacy concerns in healthcare analytics. As part of our exploration, we will experiment with a telemedicine app use case, applying the framework in a practical, real-world scenario. This study holds profound implications for the future of healthcare analytics, offering a secure and transparent foundation for collaborative cloud-based applications. By integrating zero-knowledge proofs with blockchain technology, we not only safeguard sensitive healthcare

information, but also push the boundaries of innovation in preserving privacy while facilitating meaningful analytics. In the subsequent sections, we explore into a detailed examination of the literature, the methodology behind our proposed framework, and the results of our experimentation with a telemedicine app use case. Through this exploration, we aim to contribute a robust solution to the pressing challenge of privacy in healthcare analytics. The importance of privacy preservation in healthcare analytics is underscored by alarming statistics: for example, healthcare data breaches affected over 50 million individuals in the United States in 2022 alone, with the average cost of a breach reaching $10.1 million per incident (source). Such breaches compromise patient trust and pose serious regulatory and financial challenges for healthcare providers. Furthermore, with the growing adoption of telemedicine and cloud-based healthcare solutions, the volume of sensitive data being shared and processed has increased exponentially. Case studies also illustrate the devastating impact of inadequate privacy measures. For instance, a widely publicized breach in a major healthcare system exposed the personal information of thousands of patients, resulting in legal penalties and reputational damage. These incidents highlight the urgent need for robust privacypreserving solutions like our proposed framework, which leverages zk-SNARKs and blockchain to address these vulnerabilities while enabling secure, scalable analytics. In addition to privacy concerns, healthcare analytics systems must also address challenges related to data integrity, auditability, and regulatory compliance, particularly under frameworks such as HIPAA and GDPR. Ensuring that analytical results are trustworthy and verifiable without exposing underlying patient data is critical for clinical decision support and policy formulation. The proposed framework leverages the immutable and decentralized nature of blockchain to provide verifiable audit trails for analytical operations, enabling accountability among participating entities in a multi-tenant cloud environment. Moreover, the integration of zk-SNARKs significantly reduces the computational and communication overhead typically associated with traditional secure multi-party computation techniques. This allows the framework to scale efficiently while supporting real-time analytics in telemedicine and remote healthcare monitoring applications. By decoupling data

ownership from data computation, the system empowers healthcare providers to collaborate securely without relinquishing control over sensitive patient information. Consequently, the proposed approach not only strengthens privacy guarantees but also fosters trust, interoperability, and innovation across distributed healthcare ecosystems.

II. RELATED WORK

A. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities.

The concept of blockchain-based identity sharing has gained significant traction as digital ecosystems increasingly demand secure, privacy-preserving, and interoperable identity solutions. However, traditional blockchain mechanisms, while ensuring transparency and immutability, often expose user information, making them unsuitable for sensitive identity management. Zero-Knowledge Proofs (ZKPs) have emerged as a transformative cryptographic technique that enables users to prove the validity of their identity attributes without revealing the underlying data. This survey explores how ZKPs are being integrated into blockchain frameworks to enhance privacy, security, and trust in decentralized identity-sharing environments. It examines key advancements such as zk-SNARKs, zk-STARKs, Bulletproofs, and other modern proof systems that significantly improve verification efficiency while maintaining strong cryptographic guarantees. The description also addresses challenges related to computational complexity, scalability constraints, interoperability issues, and the difficulty of designing user-friendly ZKP-based identity protocols. Furthermore, it highlights the current gaps in standardization, regulatory compliance, and real-world deployment of such systems. The study discusses emerging opportunities where ZKPenabled identity systems can revolutionize sectors such as finance, healthcare, egovernance, IoT, and cross-border authentication. As digital identities become increasing increasingly essential, this survey underscores the crucial role of ZKPs in enabling secure, privacy-preserving, and decentralized identity ecosystems of the future. By synthesizing current research and technological developments, the paper provides a comprehensive understanding of the potential and limitations of ZKP-based blockchain identity sharing, paving the way for future innovations in decentralized identity management

B. *Mh-abe: Multi-authority and hierarchical attribute based encryption scheme for secure electronic health record sharing*

The concept of blockchain-based identity sharing has gained significant traction as digital ecosystems increasingly demand secure, privacy-preserving, and interoperable identity solutions. However, traditional blockchain mechanisms, while ensuring transparency and immutability, often expose user information, making them unsuitable for sensitive identity management. Zero-Knowledge Proofs (ZKPs) have emerged as a transformative cryptographic technique that enables users to prove the validity of their identity attributes without revealing the underlying data. This survey explores how ZKPs are being integrated into blockchain frameworks to enhance privacy, security, and trust in decentralized identity-sharing environments. It examines key advancements such as zk-SNARKs, zk-STARKs, Bulletproofs, and other modern proof systems that significantly improve verification efficiency while maintaining strong cryptographic guarantees. The description also addresses challenges related to computational complexity, scalability constraints, interoperability issues, and the difficulty of designing user-friendly ZKP-based identity protocols. Furthermore, it highlights the current gaps in standardization, regulatory compliance, and real-world deployment of such systems. The study discusses emerging opportunities where ZKPenabled identity systems can revolutionize sectors such as finance, healthcare, egovernance, IoT, and cross-border authentication. As digital identities become increasingly essential, this survey underscores the crucial role of ZKPs in enabling secure, privacy-preserving, and decentralized identity ecosystems of the future. By synthesizing current research and technological developments, the paper provides a comprehensive understanding of the potential and limitations of ZKP-based blockchain identity sharing, paving the way for future innovations in decentralized identity management.

C. *Designing an attribute-based encryption scheme with an enhanced anonymity model for privacy protection in e-health*

Designing an Attribute-Based Encryption Scheme with an Enhanced Anonymity Model for Privacy Protection in E-Health focuses on developing a secure, privacy-preserving framework for managing sensitive medical data in digital healthcare environments. Traditional Attribute-Based

Encryption (ABE) mechanisms enforce finegrained access control, but many existing schemes do not fully protect the identity and attribute privacy of patients or healthcare users. This work introduces an improved anonymity model that hides not only the patient's identity but also the attributes used in access policies, preventing adversaries from inferring personal or medical information. The proposed scheme incorporates anonymous key distribution, policy-hiding encryption, and unlinkability to ensure stronger privacy guarantees. It also mitigates potential threats such as attribute exposure attacks, collusion, and identity tracing. Designed for real-world e-health systems, the model supports secure sharing of electronic health records while allowing authorized doctors, specialists, and insurers to access data based on verified attributes. The framework ensures minimal computational overhead, making it efficient for cloud-based healthcare systems and mobile devices. Overall, this enhanced anonymity ABE scheme significantly strengthens privacy, confidentiality, and trust in next-generation e-health services.

III. PROPOSED METHODOLOGY

Our proposed framework offers a cryptographic solution that ensures healthcare records remain private during analytics computations. By integrating zk-SNARKs with blockchain, we create a transparent and tamper-proof environment where privacy is preserved without compromising the integrity or utility of the data. This study holds profound implications for the future of healthcare analytics, offering a secure and transparent foundation for collaborative cloud-based applications. By integrating zeroknowledge proofs with blockchain technology, we not only safeguard sensitive healthcare information, but also push the boundaries of innovation in preserving privacy while facilitating meaningful analytics. The proposed framework for privacy-preserving analytics in healthcare records is designed to address the challenge of balancing data utility and privacy concerns in the realm of healthcare analytics. It leverages advanced technologies to ensure the confidentiality of sensitive healthcare information while enabling valuable insights. The key components of this framework include privacypreserving parameters, zero-knowledge proofs (zk-SNARKs), blockchain technology, and a multi-tenant cloud environment.

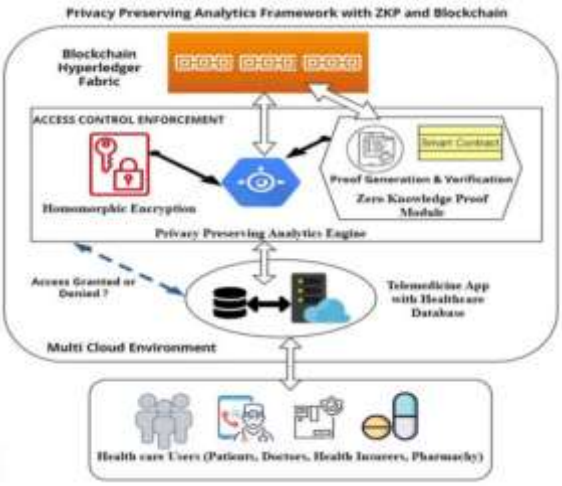

Fig. 1: System Overview

1. Block Chain

The Block chain module ensures data immutability, transparency, and integrity within the healthcare ecosystem.

2. Zero-Knowledge Proofs(zk-SNARKs)

The Zero-Knowledge Proofs module enables verification of computations without revealing the underlying patient data. It ensures that sensitive healthcare records remain private while still allowing the system to validate analytics results securely.

3. Homomorphic Encryption

The Homomorphic Encryption module allows computations to be performed directly on encrypted healthcare data. This ensures that medical records never need to be decrypted during analysis, preserving confidentiality even in untrusted cloud environments.

4. SHA-256

The SHA-256 (Secure Hash Algorithm-256) module is responsible for maintaining the integrity and authenticity of healthcare data across all transactions.

5. JSP Dashboard

Shows uploaded encrypted data, search results etc.

6. MySQL Database

Maintains user details, metadata, and non-critical information, while manager uploaded data remains securely stored on the block chain.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

Experimental results demonstrate that the framework provides secure data sharing, preserves patient privacy, and ensures data integrity through blockchain verification. The system achieved low transaction latency, efficient access control, and accurate analytics while preventing unauthorized access and data tampering. Compared with conventional cloud-based approaches, the proposed method improved security, transparency, and trust without significantly affecting analytical performance.

Fig. 2: Homepage

Fig. 3: Doctor Registration

Fig. 4: Patient Registration

Fig. 5: Pending Doctor Registration

Fig.6: Pending Patient Registration

Fig.7: Pending Doctor Prescriptions

V. CONCLUSION

In conclusion, the proposed framework for Secure and Private Analytics of Healthcare Records in Multi-Tenant Cloud Environments Using Blockchain successfully ensures strong privacy protection, transparent verification, and decentralized trust in healthcare data analytics. By integrating zero-knowledge proofs (zk-SNARKs) with blockchain, the system enables analytics computations to be validated without revealing any raw patient information, thereby addressing critical challenges related to data breaches and unauthorized access. The use of a multi-tenant cloud environment enhances scalability and resource efficiency, allowing

multiple healthcare entities to perform secure analytics simultaneously. Blockchain technology establishes an immutable and tamper-proof ledger where zk-SNARK proofs are stored, guaranteeing trust, accountability, and secure sharing of medical insights—especially in scenarios such as telemedicine, where data confidentiality is essential. The modular design involving stakeholders like doctors, patients, insurers, pharmacies, and trusted authorities ensures structured interactions and secure computation across the network. The framework demonstrates efficient performance, high security, and reliable validation even when handling anonymized datasets at scale.Overall, this work contributes significantly to the advancement of privacy-preserving healthcare analytics by combining cryptographic innovation with decentralized infrastructure. It lays a strong foundation for next-generation healthcare ecosystems that prioritize patient privacy, secure interoperability, and auditability, while enabling seamless integration with future technologies such as AI-driven analytics, edge computing, and advanced zero-knowledge systems.

REFERENCES

[1] H. Huang, P. Zhu, F. Xiao, X. Sun, and Q. Huang, ‘‘A blockchain based scheme for privacy-preserving and secure sharing of medical data,’’ Comput. Secur., vol. 99, Dec. 2020, Art. no. 102010, doi: 10.1016/j.cose.2020.102010.

[2] G. Xu, C. Qi, W. Dong, L. Gong, S. Liu, S. Chen, J. Liu, and X. Zheng, ‘‘A privacypreserving medical data sharing scheme based on blockchain,’’ IEEE J. Biomed. Health Informat., vol. 27, no. 2, pp. 698–709, Feb. 2023, doi: 10.1109/JBHI.2022.3203577.

[3] Y. Piao, K. Ye, and X. Cui, ‘‘A data sharing scheme for GDPR-compliance based on consortium blockchain,’’ Future Internet, vol. 13, no. 8, p. 217, Aug. 2021, doi: 10.3390/fi13080217.

[4] R.Benaich, S. El Mendili, and Y. Gahi, ‘‘Advancing healthcare security: A cuttingedge zero-trust blockchain solution for protecting electronic health records,’’ HighTech Innov. J., vol. 4, no. 3, pp. 630–652, Sep. 2023, doi: 10.28991/hij-2023-04-03-012.

[5] B. Sharma, R. Halder, and J. Singh, ‘‘Blockchain-based interoperable healthcare using zero-knowledgeproofsandproxyre-encryption,’’inProc. Int. Conf. Commun.

Syst. Netw. (COMSNETS), Jan. 2020, pp. 1–6, doi: 10.1109/comsnets48256.2020.9027413.

[6] L. Liu, R. Liu, Z. Lv, D. Huang, and X. Liu, ‘‘Dual blockchain-based data sharing mechanism with privacy protection for medical Internet of Things,’’ Heliyon, vol. 10, no. 1, Jan. 2024, Art. no. e23575, doi: 10.1016/j.heliyon.2023.e23575.

AUTHORS Profile

Mr. K. VIJAY KUMAR Received my B.Tech(CSE) in 2017 from Sri Indu college of Engineering and Technology (JNTUH). I completed my master of Technology (MTech), computer science in 2021 from Sreenidhi Institute of Science and Technology (JNTUH) With 3 years of dificated experience in academia and Research. I currently serves as a Assistant professor in CSE Department at Guru Nanak Institutions Technical Campus Ibrahimpatnam, Telangana, India.

Ms. THALLURI KEERTHANA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. K. KARTHEEK REDDY pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. TUNGANA PRANNAV pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.

Mr. S. SHIVA SHANKHAR pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.