IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13378

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

Lalu Banothu[1], Ravi Kumar[2], Sandip Mandal[3], P. Shiva Teja[4]

Associate Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[1]

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad[2-4]

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 cutting-edge 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.

Keywords: Healthcare Data, Security, Blockchain Technology, Cloud Computing, Multi-Tenant, Cloud Environment, Secure Data Sharing, Healthcare Data Analytics, Secure Data Processing.

I. INTRODUCTION

Healthcare organizations increasingly depend on cloud-based analytics to extract meaningful insights from vast volumes of medical records, yet this shift introduces significant privacy and security challenges. In multi-tenant cloud environments where multiple entities share computational resources, the risk of data leakage, unauthorized access, and cross-tenant privacy breaches becomes a major concern. Traditional encryption methods fail to protect sensitive patient information during computation, as data must often be decrypted before analysis, exposing it to potential threats. Furthermore, the growing number of healthcare data breaches worldwide demonstrates the inadequacy of current security mechanisms in safeguarding sensitive medical records. Existing techniques also lack the capability to validate computations without revealing raw data, creating trust issues between data owners and processing entities. Another critical problem is the absence of a transparent and tamper-proof mechanism to log healthcare analytics, making it difficult to ensure integrity and accountability in shared environments. With telemedicine platforms rapidly expanding, secure data sharing between patients, doctors, and healthcare providers has become essential, yet conventional systems are unable to guarantee privacy-preserving analytics at scale. Additionally, multi-tenant cloud architectures struggle to isolate tenant data effectively, creating vulnerabilities that malicious actors can exploit. The absence of cryptographically verifiable computation mechanisms further complicates the reliability of analytics outputs. Blockchain-based solutions exist, but many lack integration with zero-knowledge proofs, limiting their ability to protect data during analytics. Therefore, a robust, scalable, and cryptographically secure framework is needed to enable privacy-preserving analytics on healthcare records without exposing sensitive data, while ensuring transparency, trust, and integrity in a multi-tenant cloud environment. This project aims to address these critical gaps by proposing a combined approach using zk-SNARKs, blockchain, and cloud security mechanisms to deliver a next-generation solution for secure healthcare analytics.

II. RELATED WORK

Several researchers have explored secure frameworks for managing and analyzing healthcare data in cloud computing environments. With the rapid digitization of healthcare systems, Electronic Health Records (EHRs) are increasingly stored and processed on cloud platforms due to their scalability, cost efficiency, and accessibility. However, traditional

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13378

cloud-based storage solutions face significant challenges related to data privacy, unauthorized access, and lack of transparency in data sharing. These concerns become more critical in multi-tenant cloud environments where multiple healthcare organizations share the same infrastructure.

Recent studies have proposed privacy-preserving mechanisms such as encryption techniques, secure access control models, and data anonymization methods to protect sensitive healthcare information stored in the cloud. While these approaches improve data confidentiality, they often introduce computational overhead and may limit the efficiency of large-scale healthcare analytics. Additionally, centralized cloud systems still face issues related to single points of failure, limited trust, and difficulty in maintaining data integrity across multiple stakeholders.

To overcome these challenges, researchers have increasingly focused on integrating blockchain technology with cloud-based healthcare systems. Blockchain provides a decentralized and tamper-resistant ledger that ensures transparency, immutability, and secure data sharing among authorized participants. By recording transactions related to healthcare data access and modifications on the blockchain, the system enhances accountability and prevents unauthorized alterations of patient records.

Several blockchain-based healthcare frameworks have been proposed to enable secure data sharing and access control among hospitals, patients, and healthcare providers. Smart contracts are often used to automate access permissions and enforce data usage policies. These mechanisms help ensure that only authorized users can access or analyze sensitive healthcare records while maintaining a transparent audit trail of all activities.

Despite these advancements, challenges remain in supporting efficient analytics on encrypted healthcare data in multi-tenant environments. Traditional blockchain systems may experience scalability issues when handling large volumes of healthcare data and real-time transactions. Therefore, hybrid architectures combining blockchain with secure cloud analytics have been proposed to improve performance while maintaining privacy and data integrity.

The main objective of this research is to design a secure and privacy-preserving framework for healthcare data analytics in multi-tenant cloud environments using blockchain technology. The proposed system aims to protect sensitive medical records while enabling efficient data analysis for healthcare providers and researchers. It integrates blockchain-based access control mechanisms with privacy-preserving data storage techniques to ensure secure management of patient information.

The scope of the research includes developing a scalable architecture that allows multiple healthcare organizations to securely store, share, and analyze medical records in a shared cloud infrastructure. Encryption techniques and secure key management mechanisms are employed to protect patient data from unauthorized access. Blockchain technology is used to maintain an immutable record of all data transactions, ensuring transparency and accountability across the system.

Additionally, the system incorporates secure analytics mechanisms that enable healthcare institutions to derive meaningful insights from medical data without compromising patient privacy. Access control policies and smart contracts regulate data usage and ensure compliance with healthcare privacy standards. The framework also includes mechanisms to detect suspicious activities and unauthorized data access attempts within the cloud environment.

Performance evaluation is conducted by analyzing the system's efficiency, scalability, and security under different healthcare data workloads and multi-tenant scenarios. The research ultimately aims to provide a reliable, secure, and privacy-preserving solution for healthcare data analytics, improving data protection, trust, and collaboration among healthcare stakeholders in cloud-based environments.

III. LITERATURE SURVEY

Title: Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities.
Author: A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep
Year: 2024
Description:
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

DOI: 10.17148/IARJSET.2026.13378

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 ZKP-enabled identity systems can revolutionize sectors such as finance, healthcare, e-governance, 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.

Title: Mh-abe: Multi-authority and hierarchical attribute based encryption scheme for secure electronic health record sharing.
Author: S. Roy, J. Agrawal, A. Kumar, and U. P. Rao
Year: 2024.
Description:
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 ZKP-enabled identity systems can revolutionize sectors such as finance, healthcare, e-governance, 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.

Title: Designing an attribute-based encryption scheme with an enhanced anonymity model for privacy protection in e-health
Author: K. Zala, H. K. Thakkar, N. Dholakia, M. Shukla, and D. Thumar
Year: 2024
Description:
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 fine-grained 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.

Title: Dual blockchain-based data sharing mechanism with privacy protection for medical Internet of Things.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13378

Author: L. Liu, R. Liu, Z. Lv, D. Huang, and X. Liu
Year: 2024
Description:
Dual blockchain-based data sharing mechanism with privacy protection for medical Internet of Things" proposes a secure and efficient framework to manage the large volumes of sensitive health data generated by IoT-enabled medical devices. Traditional centralized MIoT systems face vulnerabilities such as data tampering, unauthorized access, and single points of failure, which put patient privacy and system reliability at risk. This project introduces a dual-blockchain architecture that combines a public blockchain for transparency and auditability with a private blockchain for secure storage and management of sensitive health data. The private blockchain stores encrypted medical records, access permissions, and device authentication details to ensure confidentiality and controlled data sharing among authorized parties. The public blockchain maintains metadata, transaction hashes, and audit trails to verify data integrity without exposing sensitive information. Smart contracts are employed to automate access control, patient consent management, and secure communication between healthcare providers, devices, and IoT networks. Privacy-preserving techniques, such as pseudonymization, attribute-based encryption, and lightweight cryptographic protocols, are integrated to further protect patient data. The system is designed to be scalable and efficient, supporting real-time data transmission and processing from multiple IoT devices. By separating sensitive data management from transparency mechanisms, the dual blockchain approach ensures both security and accountability. This framework enhances trust among patients, healthcare providers, and medical device manufacturers while reducing the risk of breaches. It provides a reliable and tamper-proof mechanism for secure medical data sharing in next-generation MIoT ecosystems, addressing the critical challenges of privacy, security, and interoperability. The architecture also allows easy integration with existing healthcare networks and cloud infrastructure, making it practical for real-world deployment.

Title: Advancing healthcare security: A cutting-edge zero-trust blockchain solution for protecting electronic health records
Author: . Benaich, S. El Mendili, and Y. Gahi
Year: 2023.
Description:
Advancing Healthcare Security: A Cutting-Edge Zero-Trust Blockchain Solution for Protecting Electronic Health Records introduces a next-generation security framework that combines the principles of Zero-Trust Architecture (ZTA) with blockchain technology to safeguard sensitive electronic health records (EHRs). Unlike traditional perimeter-based healthcare systems that assume internal entities are trustworthy, the zero-trust model enforces continuous verification, least-privilege access, and strong authentication for every user, device, and application. By integrating blockchain, the system ensures tamper-resistant audit logs**,** decentralized access control**,** and immutable record integrity, eliminating single points of failure and reducing vulnerability to cyberattacks. The solution employs cryptographic mechanisms such as identity-based encryption**,** multi-factor authentication**,** and smart contracts to automate secure data sharing and enforce dynamic access policies. Each access request is validated through context-aware checks, minimizing the risk of insider threats and unauthorized data exposure. Sensitive health data is encrypted and stored off-chain, while blockchain maintains secure metadata and verifiable access transactions. This hybrid model enhances transparency, accountability, and interoperability across hospitals, clinics, insurers, and telemedicine providers. Designed for large-scale healthcare ecosystems, the architecture delivers resilience against ransomware, data breaches, and policy violations. Overall, this cutting-edge zero-trust blockchain solution significantly elevates the security, privacy, and reliability of electronic health record management in modern digital healthcare environments.

Title: A privacy-preserving medical data sharing scheme based on blockchain
Author: G. Xu, C. Qi, W. Dong, L. Gong, S. Liu, S. Chen, J. Liu, and X. Zheng
Year: 2023.
Description:
A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain presents a secure and decentralized framework for managing and sharing electronic medical data across hospitals, clinics, patients, and healthcare service providers. Traditional medical data systems rely on centralized servers, which are vulnerable to data tampering, unauthorized access, and single points of failure. This scheme leverages blockchain's immutability**,** transparency, and distributed trust model to ensure secure and verifiable medical record storage. The framework integrates cryptographic techniques such as Attribute-Based Encryption (ABE)**,** pseudonymization**,** and hash-based indexing to guarantee data confidentiality and patient anonymity. Sensitive medical data is stored off-chain in encrypted form, while blockchain stores metadata, access permissions, and audit trails. This ensures that no unauthorized user can view or alter patient records, while every access request is fully traceable. Smart contracts automate permission management and consent mechanisms, allowing patients to dynamically control who can access their medical information. The proposed scheme also mitigates threats like insider attacks, record tampering, and data leakage through strong authentication and decentralized verification. Designed to

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13378

operate efficiently in real-world medical networks, the system supports interoperability across multiple healthcare institutions. Overall, this blockchain-based privacy-preserving model enhances trust, security, and data availability in next-generation digital healthcare ecosystems.

IV. PROPOSED SYSTEM

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 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. 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 privacy-preserving parameters, zero-knowledge proofs (zk-SNARKs), blockchain technology, and a multi-tenant cloud environment.

PROPOSED SYSTEM ADVANTAGES

- Healthcare data securely encrypted using homomorphic encryption techniques.
- Balancing data utility and privacy in healthcare analytics.
- We aim to contribute a robust solution to the pressing challenge of privacy in healthcare analyze
- Reduces the risk of data breaches and cyber-attacks by applying advanced encryption mechanisms
- Enables scalable and efficient data processing for large healthcare datasets in multi-tenant cloud environments.
- Enhances compliance with healthcare data privacy regulations and standards.
- Provides a secure framework for storing, accessing, and analyzing medical records in distributed systems.
- The system can efficiently handle large healthcare datasets, making it suitable for hospitals, laboratories, and research institutions.
- Authorized doctors, hospitals, and researchers can securely access records through a distributed framework, improving collaboration while maintaining privacy.
- Blockchain ensures traceability of all data transactions, increasing trust among patients, healthcare providers, and researchers.

Zero-Knowledge Proof using zk-SNARKs (Primary Algorithm)

The main algorithm used in this project is the Zero-Knowledge Proof technique, particularly zk-SNARKs, along with the integration of Blockchain technology. Zero-Knowledge Proof is a cryptographic method that enables one party to prove the correctness of a statement or computation to another party without revealing the actual underlying data. In this project, this concept is applied to healthcare records, which contain highly sensitive patient information. The system generates cryptographic proofs using zk-SNARKs to verify that data processing and analytics have been performed correctly while ensuring that the original medical records remain private. These proofs are then recorded on a blockchain network, which provides a decentralized, transparent, and tamper-proof ledger for storing verification results. By using blockchain, the system ensures data integrity, immutability, and secure sharing of information across multiple tenants in a cloud environment. Additionally, privacy-preserving data handling and encryption techniques are used to protect patient records from unauthorized access. Overall, the combination of zero-knowledge proofs and blockchain allows the system to perform secure and private analytics on healthcare data while maintaining confidentiality, reliability, and trust among different users in the cloud infrastructure.

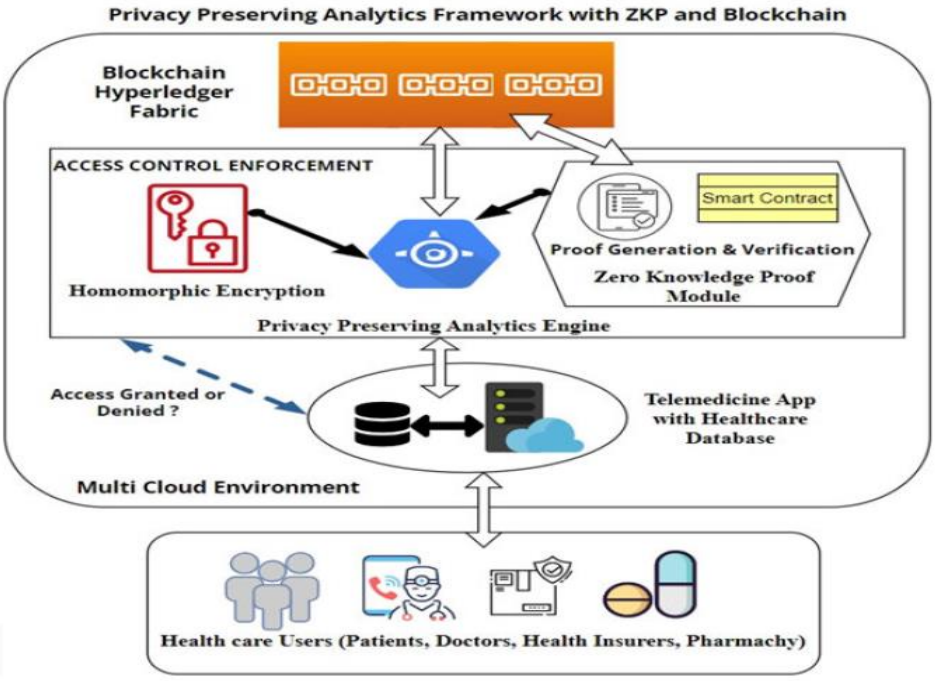
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13378

System Architecture



The system architecture of the proposed healthcare security framework is designed to ensure secure, private, and efficient management of medical data across multiple stakeholders, including patients, doctors, authority, pharmacy, and insurers. It consists of modular layers integrating Blockchain**,** Zero-Knowledge Proofs (zk-SNARKs)**,** Homomorphic Encryption**,** and SHA-256 to provide data integrity, confidentiality, and verifiable computation. The Patient Layer enables registration, appointment booking, and encrypted file upload, while the Doctor Layer allows access to approved requests, viewing encrypted reports, and generating prescriptions. The Authority Layer verifies and approves actions to maintain system validity, and the Pharmacy and Insurer Layers manage prescriptions and insurance claims securely. All sensitive data is encrypted using Homomorphic Encryption and validated via SHA-256, while Blockchain and IPFS provide decentralized storage and immutability. zk-SNARKs ensure that computations and validations can be performed without exposing private data. The architecture employs secure IoT communication channels and cloud storage for redundancy, enabling a scalable, reliable, and tamper-proof healthcare ecosystem with end-to-end security and traceability.

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.

DOI: 10.17148/IARJSET.2026.13378

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 privacy-preserving medical data sharing scheme based on blockchain,'' IEEE J. Biomed. Health Informal, 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 cutting-edge 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-knowledge proofs and proxy re-encryption,'' in Proc. 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.

[7]. T. Bai, Y. Hu, J. He, H. Fan, and Z. An, ''Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof,'' Sensors, vol. 22, no. 20, p. 7716, Oct. 2022, doi: 10.3390/s22207716.

[8]. A. Diro, L. Zhou, A. Saini, S. Kaisar, and P. C. Hiep, ''Leveraging zero-knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities,'' J. Inf. Secur. Appl., vol. 80, Feb. 2024, Art. no. 103678, doi: 10.1016/j.jisa.2023.103678.

[9]. X. Shang, L. Tan, K. Yu, J. Zhang, K. Kaur, and M. M. Hasan, ''Newton-interpolation-based zk-SNARK for artificial Internet of Things,'' Ad Hoc Netw., vol. 123, Dec. 2021, Art. no. 102656, doi: 10.1016/j.adhoc.2021.102656.

[10]. R. Zhang, R. Xue, and L. Liu, ''Security and privacy for health care blockchains,'' IEEE Trans. Services Comput., vol. 15, no. 6, pp. 3668–3686, Nov. 2022, doi: 10.1109/TSC.2021.3085913.

[11]. R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, ''Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions,'' Trans. Emerg. Telecommun. Technol., vol. 35, no. 1, pp. 1–48, Oct. 2023, doi: 10.1002/ett.4884.

[12]. G. S. Gaba, M. Hedabou, P. Kumar, A. Braeken, M. Liyanage, and M. Alazab, ''Zero-knowledge proofs based authenticated key agreement protocol for sustainable healthcare,'' Sustain. Cities Soc., vol. 80, May 2022, Art. no. 103766, doi: 10.1016/j.scs.2022.103766.

[13]. J. Scheibner, M. Ienca, and E. Vayena, ''Health data privacy through homomorphic encryption and distributed ledger computing: An ethical legal qualitative expert assessment study,'' BMC Med. Ethics, vol. 23, no. 1, pp. 1–13, Dec. 2022, doi: 10.1186/s12910-022-00852-2.

[14]. O. Kocabas, T. Soyata, J.-P. Couderc, M. Aktas, J. Xia, and M. Huang, ''Assessment of cloud-based health monitoring using homomorphic encryption,'' in Proc. IEEE 31st Int. Conf. Comput. Design (ICCD), Oct. 2013, pp. 1–12, doi: 10.1109/iccd.2013.6657078.

[15]. K. Sinha, P. Majumder, and S. K. Ghosh, ''Fully homomorphic encryption based privacy-preserving data acquisition and computation for contact tracing,'' in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS), Dec. 2020, pp. 1–6, doi:10.1109/ANTS50601.2020.9342834.

[16]. B. Wang, H. Li, Y. Guo, and J. Wang, ''PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data,'' Appl. Soft Comput., vol. 146, Oct. 2023, Art. no. 110677, doi: 10.1016/j.asoc.2023.110677.

[17]. X. Dong, D. A. Randolph, and C. Weng, ''Developing high performance secure multi-party computation protocols in healthcare: A case study of patient risk stratification,'' in Proc. AMIA Jt Summits Transl. Sci., May 2021, pp. 200–209.

[18]. A. V. Kumar, M. S. Sujith, K. T. Sai, G. Rajesh, and D. J. S. Yashwanth, ''Secure multiparty computation enabled e-healthcare system with homomorphic encryption,'' IOP Conf. Ser., Mater. Sci. Eng., vol. 981, no. 2, Dec. 2020, Art. no. 022079, doi: 10.1088/1757-899x/981/2/022079.

[19]. U. Kose, D. Gupta, A. Khanna, and J. J. P. C. Rodrigues, Interpretable Cognitive Internet of Things for Healthcare. London, U.K.: Springer Nature, 2023. [Online].
Available: http://books.google.ie/books?id=hbjHEAAAQBAJ&pg=PA57&dq

[20]. P. Jangde and D. K. Mishra, ''A secure multiparty computation solution to healthcare frauds and abuses,'' in Proc. 2nd Int. Conf. Intell. Syst., Model. Simul., Phnom Penh, Cambodia, Jan. 2011, pp. 139–142, doi: 10.1109/ISMS.2011.75.

DOI: 10.17148/IARJSET.2026.13378

[21]. S. Vijayalakshmi, ‘‘Attribute based encryption in healthcare application,’’ in Proc. Int. Conf. Autom., Comput. Renew. Syst. (ICACRS), Dec. 2022, pp. 1–8, doi: 10.1109/ICACRS55517.2022.10029259.

[22]. H. Wang, J. Liang, Y. Ding, S. Tang, and Y. Wang, ‘‘Ciphertext policy attribute-based encryption supporting policy-hiding and cloud auditing in smart health,’’ Comput. Standards Inter., vol. 84, Mar. 2023, Art. no. 103696, doi: 10.1016/j.csi.2022.103696.

[23]. S. Roy, J. Agrawal, A. Kumar, and U. P. Rao, ‘‘Mh-abe: Multi-authority and hierarchical attribute based encryption scheme for secure electronic health record sharing,’’ Cluster Comput., vol. 27, no. 5, pp. 6013–6038, Feb. 2024, doi: 10.1007/s10586-024-04283-z.

[24]. N. Ni and Y. Zhu, ‘‘Enabling zero-knowledge proof by accelerating zk-SNARK kernels on GPU,’’ J. Parallel Distrib. Comput., vol. 173, pp. 20–31, Mar. 2023, doi: 10.1016/j.jpdc.2022.10.009.

[25]. K. Zala, H. K. Thakkar, N. Dholakia, M. Shukla, and D. Thumar, ‘‘Designing an attribute-based encryption scheme with an enhanced anonymity model for privacy protection in e-health,’’ Social Netw. Comput. Sci., vol. 5, no. 2, p. 2, Jan. 2024, doi: 10.1007/s42979-023-02541-2.

[26]. A. Sharma, S. Kaur, and M. Singh, “A Comprehensive Review on Blockchain and Internet of Things in Healthcare,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 10, p. e4333, 2021.

