AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

A PRIVACY-PRESERVING FRAMEWORK FOR SECURE ANALYTICS OF HEALTHCARE RECORDS IN MULTI-TENANT CLOUD ENVIRONMENTS

Umme Habeeba Fatima[1], Lubna Nausheen[2], Sadaf Jahan[3]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, habeebafatimaumme@gmail.com
[2]Asst Professor, Department of CSE, Shadan Women's College of Engineering and Technology lubnanausheen07@gmail.com
[3]Asst Professor, Department of CSE, Shadan Women's College of Engineering and Technology sadafcse6@gmail.com

ABSTRACT:
Healthcare analytics presents a big difficulty in protecting sensitive data while yet offering insightful information because of the sensitivity of personal health information and the increasing frequency of data breaches. The safe system described in this paper tackles these problems by combining blockchain technology, privacy-preserving parameters, zero-knowledge proofs (zk-SNARKs), and a multi-tenant cloud environment. The system uses state-of-the-art cryptographic techniques, specifically zk-SNARKs, to guarantee that healthcare records are safeguarded during analytics computations without revealing raw data. The privacy-preserving analytics engine uses anonymised medical records and creates zk-SNARKs to verify calculations. These proofs create a visible, impenetrable ledger that ensures secure healthcare transactions when integrated into a blockchain network. In situations like telemedicine, when secure data sharing and processing are crucial, this approach is imperative. The framework's practical value in healthcare analytics is demonstrated by its deployment in a telemedicine app, which offers a scalable and secure solution to an urgent problem.
KEYWORDS: Healthcare security, blockchain, multitenant cloud, privacy-preserving analytics, and zero-knowledge proofs.

1. INTRODUCTION

The development of healthcare analytics has completely changed how we extract meaning from large, complicated datasets. However, protecting sensitive healthcare data privacy continues to be a major concern, especially in collaborative settings. In order to overcome this difficulty, this study suggests a unique architecture for privacy-preserving healthcare analytics that makes use of blockchain technology, a multi-tenant cloud environment, and zero-knowledge proofs (zk-SNARKs). Sensitive information ranging from patient identities to complex medical histories is stored in healthcare records. Amjad Mehmood was the assistant editor who oversaw the manuscript's evaluation and gave it the go-ahead to be published. Conventional encryption techniques are good at safeguarding data while it's at rest, but they frequently fail to protect it while analytics calculations are underway. We incorporate zk-SNARKs into our methodology to offer privacy-preserving analytics, allowing calculation correctness confirmation without disclosing any raw data. This is especially important in multi-tenant cloud systems, where telemedicine, policy-making, and healthcare innovations depend on secure data processing and sharing. Our suggested framework provides a cryptographic approach that guarantees the privacy of medical records while analytics calculations are being performed. Through the integration of zk-SNARKs with blockchain, we establish a transparent and impervious environment that protects privacy without sacrificing the data's integrity or usefulness. This study's main goal is to present and thoroughly examine the suggested method, emphasizing how well it handles the delicate balance between data utility and privacy concerns in healthcare analytics. We will test a telemedicine app use case as part of our investigation, putting the framework to use in a useful, real-world setting. This study offers a clear and safe foundation for cooperative cloud-based applications, which has significant implications for the future of healthcare analytics. By combining blockchain technology with zero-knowledge proofs, we not only protect private health information but also push the limits of innovation in privacy protection while enabling insightful analytics. The literature, our suggested framework's approach, and the outcomes of our testing with a telemedicine app use case are all thoroughly examined in the following sections. We hope that this investigation will provide a solid answer to the urgent problem of privacy in healthcare analytics. Alarming numbers highlight the significance of privacy preservation in healthcare analytics: in 2022 alone, over 50 million Americans were impacted by healthcare data breaches, with an average cost of $10.1 million per incident (source). These violations undermine patient confidence and present significant financial and legal difficulties for healthcare providers. Additionally, the amount of sensitive data being exchanged and processed has skyrocketed due to the expanding use of telemedicine and cloud-based healthcare solutions. The disastrous effects of insufficient privacy protection are also demonstrated by case studies. For example, thousands of patients' personal information was compromised in a well reported breach in a large healthcare system, which led to fines and harm to the organization's reputation. These occurrences demonstrate the critical need for strong privacy-preserving solutions, such as our suggested system, which uses blockchain and zk-SNARKs to address these weaknesses and enable safe, scalable analytics.

Healthcare analytics solutions must handle issues with data integrity, auditability, and regulatory compliance in addition to privacy concerns, especially under frameworks like HIPAA and GDPR. A safe and private framework for conducting analytics on medical records kept in multi-tenant cloud settings is proposed in this research. Sensitive patient data is protected throughout the analytics lifecycle because to the system's use of blockchain technology and cutting-edge cryptography techniques. Zero-knowledge proofs (zk-SNARKs), which allow calculations to be validated without disclosing the underlying raw data, are a crucial part of the system. A privacy-preserving analytics engine anonymizes and processes medical records, producing zk-SNARK proofs to confirm the accuracy of analytical findings. A blockchain ledger is used to preserve these proofs, resulting in an unchangeable and impenetrable record of every calculation. Blockchain technology improves accountability, transparency, and trust among many healthcare ecosystem players. In situations like telemedicine, when safe data exchange and remote computing are essential, the framework is very helpful. The suggested approach offers a scalable and workable way to protect healthcare data in contemporary cloud infrastructures by combining privacy, security, and verified analytics.

2. STIMULATING

The scope of this project encompasses the design and development of a secure and privacy-preserving analytics framework for healthcare records in a multi-tenant cloud environment. It includes the implementation of zero-knowledge proofs (zk-SNARKs) to enable verification of analytics results without exposing raw patient data. The project also integrates blockchain technology to ensure immutability, auditability, and tamper-proof logging of healthcare transactions and analytics proofs. The framework supports anonymized data processing, secure data sharing, and multi-tenant access control, ensuring strict separation of tenant data in shared cloud environments. Additionally, the project evaluates the performance, scalability, and security of the proposed architecture through a telemedicine application use case. It focuses on protecting sensitive health information during computation, storage, and transmission while maintaining efficiency for real-time analytics. The scope further includes identifying key vulnerabilities in conventional cloud-based healthcare analytics and demonstrating how the proposed solution mitigates them. Overall, the project delivers a robust, scalable, and privacy-preserving model suited for real-world healthcare analytics scenarios.

3. OBJECTIVE

The goal of this project is to use cutting-edge cryptographic techniques to design and implement a secure, scalable, and privacy-preserving framework for healthcare analytics in multi-tenant cloud systems. The goal of this project is to guarantee the complete protection of sensitive healthcare records during data processing, sharing, and analysis, particularly in settings where several organizations share cloud infrastructure. Using zero-knowledge proofs—more especially, zk-SNARKs—to confirm the accuracy of analytics calculations without disclosing patient data is a primary goal. The initiative also aims to incorporate blockchain technology to produce a visible, unchangeable, and impenetrable ledger that documents secure healthcare transactions and analytics data. Another goal is to use robust isolation and access-control measures to eliminate the possibility of data leakage, unwanted access, and cross-tenant interference. The project's goal is to facilitate the processing of anonymized data so that valuable insights can be obtained without jeopardizing patient privacy. By offering verifiable cryptographic verification of data integrity and calculation accuracy, the goal is also to increase confidence between patients, healthcare professionals, and telemedicine platforms. Through a telemedicine app use case, this work also aims to illustrate the framework's practical applicability and show how secure analytics may be applied in actual healthcare situations. By implementing privacy-by-design principles, the initiative also seeks to address the growing worries about health data breaches and regulatory compliance. The goal is to present a next-generation safe healthcare analytics solution that can adjust to future data demands by integrating cloud computing, blockchain, and zero-knowledge proofs. The project's ultimate goal is to provide a reliable, effective, and privacy-preserving model that promotes safe decision-making, safeguards private medical information, and encourages advancements in healthcare technology.

3.1 What The Project Is About

In order to glean valuable insights from enormous amounts of medical data, healthcare organizations are depending more and more on cloud-based analytics. However, this change presents serious privacy and security issues. The possibility of data leakage, illegal access, and cross-tenant privacy breaches becomes a significant problem in multi-tenant cloud settings where numerous entities share computational resources. Because data must frequently be decrypted before analysis, which exposes it to possible threats, traditional encryption techniques are unable to secure sensitive patient information during computation. Additionally, the increasing incidence of global healthcare data breaches shows how inadequate the security measures in place are for protecting private medical records. Additionally, current methods cannot confirm computations without disclosing raw data, which undermines trust between processing companies and data owners. The lack of an open and impenetrable system for recording healthcare analytics is another serious issue that makes it challenging to guarantee accountability and integrity in shared settings. Secure data exchange between patients, physicians, and

healthcare providers has become crucial as telemedicine platforms grow quickly. However, traditional methods cannot ensure privacy-preserving analytics at scale. Furthermore, it is difficult for multi-tenant cloud systems to effectively separate tenant data, which leaves gaps that bad actors might take advantage of. The dependability of analytics outputs is further complicated by the lack of compute processes that can be verified cryptographically. Although there are blockchain-based solutions, their capacity to safeguard data during analytics is limited because many of them do not integrate with zero-knowledge proofs. Therefore, to enable privacy-preserving analytics on healthcare records without disclosing sensitive data while maintaining transparency, trust, and integrity in a multi-tenant cloud environment, a strong, scalable, and cryptographically secure framework is required. In order to provide a next-generation solution for safe healthcare analytics, this project proposes a combination method employing zk-SNARKs, blockchain, and cloud security measures.

4. EXISTING SYSTEM:

- In the realm of healthcare analytics, preserving the privacy of sensitive data while enabling valuable insights poses a significant challenge, particularly given the increasing prevalence of data breaches and the sensitivity of personal health information.
- Numerous sensitive pieces of information, including patient names and complex medical histories, are stored in healthcare records.
- Conventional cryptographic techniques are useful for protecting data while it's at rest, but they frequently don't work well for protecting data while analytics calculations are being performed.
- Reference uses blockchain to improve EHR security, but its scalability, gas consumption, and AES encryption complexity limit its wider use.
- Similarly proposes a blockchain paradigm for IoT smart cities, enhancing privacy; but, scalability and regulatory obstacles continue to be major obstacles.
- Although it suggests a dual blockchain approach for the Medical Internet of Things (MIoT), performance constraints and flexibility are not specifically addressed.

4.1Existing System Disadvantages:

- A secure and scalable solution to an urgent issue.
- In healthcare analytics, there is less balance between data utility and privacy.

4.2 THE PROPOSED SYSTEM

- Our suggested framework provides a cryptographic solution that guarantees the confidentiality of medical records while analytics calculations are being performed.
- Through the integration of zk-SNARKs with blockchain, we establish a transparent and unchangeable environment that protects privacy without sacrificing the data's integrity or usefulness.
- This study offers a clear and safe foundation for cooperative cloud-based applications, which has significant implications for the future of healthcare analytics.
- By combining blockchain technology with zero-knowledge proofs, we not only protect private health information but also push the limits of innovation in privacy protection while enabling insightful analytics.
- The difficulty of striking a balance between data utility and privacy concerns in the field of healthcare analytics is addressed by the suggested framework for privacy-preserving analytics in medical records.
- It makes use of cutting-edge technologies to protect private health information while providing insightful information.
- This framework's main elements include blockchain technology, a multi-tenant cloud environment, zero-knowledge proofs (zk-SNARKs), and privacy-preserving parameters.

4.2.1 Proposed System Advantage

- Homomorphic encryption algorithms are used to securely encrypt healthcare data.
- Healthcare analytics: striking a balance between privacy and data utility.

5.METHODOLOGIES

1. Design of User Interfaces

The user must enter their username and password in order to connect to the server. The user can log in to the server directly if they have previously left; otherwise, they must register their information, including their username, password, email address, city, and country. To manage upload and download rates, the database will create an account for every user. The user ID will be used as the name. To access a certain page, you typically need to log in. The query will be searched and displayed.

2. Doctor

Physicians can view and handle patient requests using the Doctor module. Physicians are able to diagnose patients, check submitted medical papers, and review patient health information. They create and distribute digital prescriptions to patients following examination. This module guarantees safe prescription administration and accurate medical advice. It serves as the system's main interface for healthcare providers.

3. Patient

Patients can communicate online with healthcare services using the Patient module. Patients can upload medical reports, seek consultations, and view doctor-written prescriptions. On the basis of recommended therapies, they might also file insurance claims. Access to medical records and healthcare services is enhanced by this module. It offers a practical means of communication between patients and physicians.

4. Authority

To guarantee security and compliance, the Authority module supervises and keeps an eye on system operations. It can examine what physicians and patients do and take the appropriate administrative action. The authority guarantees adherence to healthcare policies and laws. Additionally, it oversees system governance, validations, and approvals. This module improves the healthcare system's accountability and openness.

5. Pharmacy

Pharmacists can examine doctor-issued prescriptions using the Pharmacy module. Pharmacists are able to change prescription statuses and deliver medications based on the information of the prescription. It guarantees that drugs are only administered in accordance with legitimate prescriptions. The module keeps track of prescription fulfillment and medication delivery. This enhances patient safety and medication administration.

6. Insurance

Verification of health insurance and processing of claims are handled by the Insurance module. Insurance companies are able to verify treatment data and examine patient claims. The module assesses claim eligibility and verifies policy coverage. Based on prescription and treatment records, approved claims are processed quickly. This expedites and streamlines the insurance reimbursement procedure.

6.TECHNIQUE USED

6.1 Proposed Algorithm

- **Zero-knowledge proofs (zk-SNARKs), blockchain technology)**

Blockchain technology and Zero-Knowledge Proofs (zk-SNARKs) provide safe, confidential, and verifiable data processing without disclosing sensitive information. When a user or healthcare provider submits data for analysis, the procedure starts. The technology processes the actual data securely and keeps it encrypted. Once the computation is finished, a zk-SNARK proof is produced to demonstrate mathematically that the computation was done correctly. The original data, intermediate values, and private information utilized in processing are not disclosed by this proof. Only the proof is given to the verifier, who can promptly confirm that the computation is accurate. The evidence and associated transaction metadata are stored on the blockchain after verification. These records are kept on the blockchain in unchangeable blocks connected by cryptographic hashes. Without having access to private medical information, any member of the network can confirm the veracity of the stored proofs. Access control and validation processes can be automated with smart contracts. Blockchain's decentralized structure reduces reliance on a single, reliable authority and guards against illegal record change. Any effort to change stored data would be instantly discovered and render the blockchain's cryptographic linkages invalid. In multi-tenant cloud healthcare systems, this combination method enables safe analytics while guaranteeing data protection, integrity, openness, and accountability. It is especially helpful for safeguarding private medical data while preserving confidence in system functionality and analytical outcomes.

6.2 Existing Algorithm

- **Attribute-Based Encryption (ABE)**

A cryptographic access control mechanism called Attribute-Based Encryption (ABE) encrypts data based on user traits rather than personal identities. The algorithm starts by establishing a collection of characteristics, like administrator, researcher, physician, or nurse. The system's master secret keys and public parameters are created by a reliable authority. Private keys are given to users according to their approved qualities. The data owner establishes an access policy that specifies the attribute combinations needed to access the data when it is submitted. The public parameters and the designated access policy are then used to encrypt the data. Without disclosing its contents, the encrypted data can be safely kept in dispersed or cloud environments. The system determines whether the characteristics linked to the user's private key meet the access policy contained in the ciphertext when a user requests access. The decryption operation is successful and the original data is recovered if the necessary characteristics meet the policyThe data is safeguarded and decryption is refused if the characteristics don't meet the rules. Without requiring unique encryption for every user, the technique guarantees fine-grained access control. In large-scale systems, it also lessens the complexity of key management. ABE improves data confidentiality, secure sharing, and privacy protection, which makes it ideal for blockchain-based, cloud computing, IoT, and healthcare applications where sensitive data must only be accessed by authorized users.

7.SYSTEM ARCHITECTURE

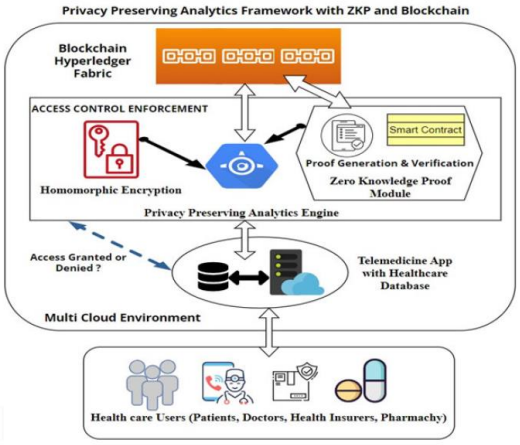
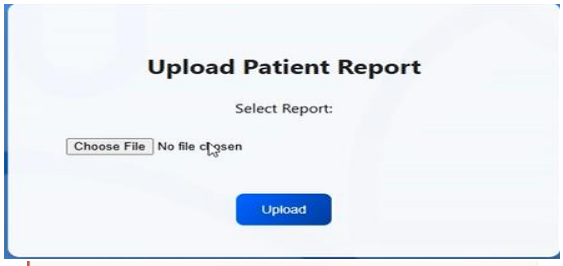


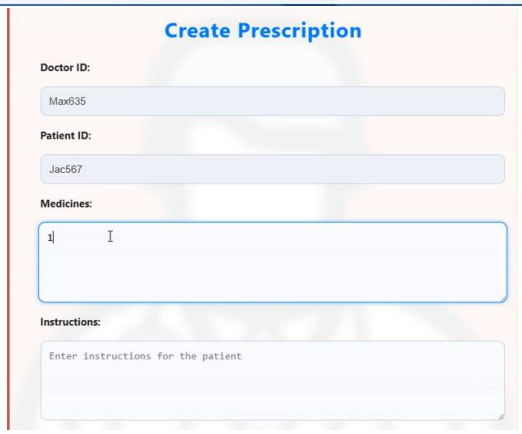
FIG:7 System Architecture

The Blockchain Network, Privacy-Preserving Analytics Engine, Multi-Cloud Environment, and Healthcare Users are the four primary tiers of the system design. Healthcare users, such as patients, doctors, health insurers, and pharmacies, interact with

the system to access or submit healthcare data. The medical records are stored in a multi-cloud architecture that provides distributed and scalable storage facilities. Access control limitations are implemented before any analytics activities to ensure that only authorized persons can access sensitive medical data. The framework's core processing unit is the Privacy-Preserving Analytics Engine. It employs homomorphic encryption algorithms to allow computations on encrypted healthcare data without revealing the original records. A Zero-Knowledge Proof (ZKP) module is used to create cryptographic proofs that verify the veracity of analytics results while safeguarding data privacy. The validity and reliability of these proofs are then verified. Access control, verification procedures, and transaction management are all automated via smart contracts. The blockchain layer, which is developed using Hyperledger Fabric, stores transaction records, access logs, and proof verification results in an immutable ledger. This ensures transparency, traceability, and protection against unauthorized modifications. The analytics results are only returned if authorization and verification processes are successfully finished. The telemedicine application communicates with the healthcare database and analytics engine to provide safe healthcare services. The architecture guarantees the confidentiality, integrity, accountability, and privacy of medical records while enabling safe analytics in a multi-tenant cloud environment. All things considered, the architecture combines blockchain, smart contracts, encryption, and zero-knowledge proofs to provide a secure and private healthcare analytics platform.

8. RESULTS





blockchain_id	report_id	patient_id	sha256_hash
1	15	Ram677	a5dfb5233bd8aed6ffeb0e8b617bb90270778b37be1d868134222b6986bcb45
2	16	Jac567	0624cc3a91357646928d2dd6a74952799b729dd9c9812da7642de61ed2824f8

9. CONCLUSION

In summary, the suggested architecture for Secure and Private Analytics of Healthcare Records in Multi-Tenant Cloud Environments Using Blockchain effectively guarantees decentralized trust, transparent verification, and robust privacy protection in healthcare data analytics. The technology addresses important issues with data breaches and illegal access by merging zero-knowledge proofs (zk-SNARKs) with blockchain to validate analytics computations without disclosing any raw patient data. Several healthcare organizations can conduct secure analytics at the same time by utilizing a multi-tenant cloud platform, which improves scalability and resource efficiency. In situations like

telemedicine, where data confidentiality is crucial, blockchain technology creates an unchangeable and tamper-proof ledger where zk-SNARK proofs are kept, ensuring trust, accountability, and secure sharing of medical insights. Structured interactions and safe computation throughout the network are ensured by the modular design, which involves stakeholders like as physicians, patients, insurers, pharmacists, and trusted authorities. Even when managing anonymised datasets at scale, the framework exhibits dependable validation, excellent security, and effective performance. Overall, by fusing cryptographic innovation with decentralized infrastructure, this study makes a substantial contribution to the development of privacy-preserving healthcare analytics. In addition to facilitating smooth integration with upcoming technologies like AI-driven analytics, edge computing, and sophisticated zero-knowledge systems, it provides a solid basis for next-generation healthcare ecosystems that place a high priority on patient privacy, secure interoperability, and auditability.

9.2 FUTURE ENHANCEMENT

The blockchain-enabled privacy-preserving healthcare analytics framework's intelligence, scalability, security, and usefulness in contemporary healthcare ecosystems can all be further enhanced in the future. Predictive healthcare analytics, illness risk assessment, individualized therapy recommendations, and real-time clinical decision assistance can all be made possible while maintaining patient privacy with the integration of sophisticated AI and ML models. Future iterations might include federated learning strategies, which let several healthcare facilities work together to train AI models without exchanging private patient information. To lower latency and boost responsiveness for telemedicine and emergency healthcare applications, the framework can be expanded to function in multi-cloud, edge computing, and fog computing settings. To lower computational overhead and speed up proof creation and verification procedures, next-generation zero-knowledge proof systems and more effective and lightweight zk-SNARK protocols can be used. Stronger authentication, safe credential management, and user-controlled access restrictions can be achieved by integrating Decentralized Identity (DID) and Self-Sovereign Identity (SSI) technologies. In order to enable safe cross-institutional data sharing and analytics, the blockchain network can be extended to link hospitals, labs, pharmacies, insurance companies, and research institutions. Collaboration and data exchange can be further enhanced by interoperability with electronic health record systems and international healthcare standards. Healthcare activities like processing insurance claims, managing consent, and controlling access to medical records can be automated by sophisticated smart contracts. Adopting cryptographic techniques that are resistant to quantum computing can offer long-term defense against potential threats. To spot suspicious activity and unwanted access attempts, real-time monitoring and anomaly detection systems can be incorporated. Continuous patient monitoring and safe real-time health data analytics are made possible by integration with wearable health sensors and Internet of Medical Things (IoMT) devices. Additionally, automatic compliance verification can be added to blockchain-based audit trails to comply with changing privacy standards and healthcare legislation. Healthcare activities like processing insurance claims, managing consent, and controlling access to medical records can be automated by sophisticated smart contracts.

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 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 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-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.

[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. Has san, ‘‘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 homo morphic 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.
[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 anonymitymodelforprivacyprotectionine-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.