International Journal of Technology and Emerging Sciences (IJTES)
www.mapscipub.com

Volume 05 || Issue 02 || July 2025 || pp. 04-09 E-ISSN: 2583-1925

Secure Blockchain based Framework for Electronic health Record Management with Attribute Based Encryption

Keerthi V T [1]*, Manasa A B [2], Ranjith J [3]

[123] *Department of Information Science and Engineering,*
SJB Institute of Technology, Bengaluru, India

Abstract: *In healthcare data management Safeguarding the security and privacy of Electronic Health Records (EHRs) while enabling efficient access control remains a critical challenge. Blockchain-based solutions provide a promising approach to discourse these encounters by offering decentralization, immutability, and cryptographic enforcement mechanisms. This paper integrates methodologies from two blockchain-based frameworks to propose an enhanced model for secure EHR sharing. The first framework employs a hybrid blockchain-edge architecture that leverages Attribute-Based Signature Aggregation (ABSA) and Multi-Authority Attribute-Based Encryption (MA-ABE), along with Paillier Homomorphic Encryption (HE), to enhance authentication, privacy, and fine-grained access control . The second framework, HA-Med, introduces a blockchain-driven solution utilizing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with hidden policies to prevent unauthorized access while maintaining user privacy. By synthesizing these approaches, the proposed model strengthens data confidentiality, prevents attribute exposure, and optimizes access control enforcement. Performance evaluations indicate improvements in computational efficiency, scalability, and policy enforcement, making it a viable solution for real-world healthcare applications [5,6]. Future research will focus on optimizing hierarchical blockchain structures and improving dynamic attribute-based access control mechanisms.*

Keywords: Blockchain, Attribute-Based Encryption (ABE), Electronic Health Records (EHR), Access Control, Privacy Preservation

1. INTRODUCTION

The rapid advancement of digital healthcare systems has led to an increased reliance on Electronic Health Records (EHRs) for storing and managing patient information. EHRs facilitate continuous health records exchange between healthcare providers, ensuring timely and accurate patient care. However, their widespread adoption introduces significant challenges related to data security, privacy, integrity, also access control [1]. Traditional cloud-based EHR management systems, while offering centralized storage and easy accessibility, are prone to unauthorized access, data breaches, also particular facts of disaster [2]. Patients often lose mechanism above their health records, leading to concerns about data ownership and consent enforcement [3].The safety and confidentiality tasks in healthcare records administration arise from the complexity of medical data sharing, the lack of interoperability between healthcare systems, and the absence of standardized access control mechanisms [4]. Traditional models rely on role-based or identity-based access control, which fail to provide fine-grained security measures and do not adequately guard complex patient records from unauthorized disclosure [5]

Furthermore, existing encryption techniques, while providing a degree of confidentiality, often introduce computational overhead, reduce system efficiency, and limit real-time data accessibility [6].

To overwhelm these problems, blockchain technology has appeared as a anticipative solution due to its decentralized, absolute, and clear nature [7]. Blockchain-based EHR management ensures tamper-proof records, verifiable transactions, and decentralized control, allowing patients and authorized entities to access medical data securely [8]. However, blockchain's inherent transparency raises privacy concerns, as storing access control policies and patient data on a public ledger could expose sensitive information to unauthorized parties [9].

To enhance privacy preservation and secure access control, several cryptographic practices need stayed combined with blockchain technology. One such approach is Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which enables fine-grained access control by permitting records holders to express specific access policies based on user attributes [10]. CP-ABE guarantees that first legal users with matching attributes can decrypt the data, thus enhancing security and confidentiality [11]. However, conventional CP-ABE schemes face limitations, such as high computational complexity and attribute exposure, which necessitate hidden policy enforcement mechanisms [12].

A complementary approach involves using Multi-Authority Attribute-Based Encryption (MA-ABE) and Attribute-Based Signature Aggregation (ABSA) to improve authentication and scalability in blockchain-based medical data sharing [13]. MA-ABE distributes encryption authority among multiple trusted entities, falling the danger of sole ideas of disappointment and ensuring decentralized access control enforcement [14]. Additionally, ABSA strengthens the authentication process by allowing multiple entities to verify user credentials in a privacy-preserving manner [15].

International Journal of Technology and Emerging Sciences (IJTES)
www.mapscipub.com

Volume 05 || Issue 02 || July 2025 || pp. 04-09 E-ISSN: 2583-1925

To further optimize blockchain-based EHR systems, homomorphic encryption (HE) methods need stayed joined to assist safe additions on encrypted medical data without requiring decryption [16]. This enhances data confidentiality while allowing healthcare providers to perform medical analytics and decision-making securely [17]. Moreover, integrating edge computing with blockchain-based EHR management improves system efficiency by reducing latency, optimizing storage requirements, and enabling real-time access control enforcement [18].

By leveraging Multi-Authority Attribute-Based Encryption (MA-ABE) and Attribute-Based Signature Aggregation (ABSA), this approach ensures robust authentication, secure data sharing, and privacy-preserving access control. Additionally, the usage of with edge computing with blockchain improves system efficiency by reducing latency and computational overhead while maintaining security standards .This paper emphasises blockchain-based medical data-sharing frameworks to develop an enhanced privacy-preserving and secure EHR management system. By combining hidden access control policies from CP-ABE with the decentralized authentication mechanisms of MA-ABE and ABSA, the proposed framework strengthens data confidentiality, reduces computational overhead, and ensures scalability [19]. The combination of homomorphic encryption and edge computing further enhances performance, building this method appropriate for real-world healthcare applications [20].

The other part of this article is ordered as follows: Section 2 discusses the methods and background related to blockchain-based medical data sharing. Section 3 presents the results and discussions, evaluating the routine of the anticipated framework. Section 4 concludes the paper, highlighting key findings and future research directions.

2. RELATED WORK

A significant body of research has been dedicated to securing medical data through cryptographic techniques, access control models, and blockchain integration. Early methods primarily relied on role-based access control (RBAC) and identity-based encryption, but these lacked flexibility and often placed trust in a central authority .To enable fine-grained access control, Goyal et al. introduced Attribute-Based Encryption (ABE), where access policies are tied to user attributes rather than identity. However, these early systems used single-authority ABE, making them vulnerable to key compromise and limiting scalability.

To address the issue of central trust, Lewko and Waters proposed Multi-Authority ABE (MA-ABE), allowing independent authorities to manage subsets of attributes. This significantly improved decentralization and fault tolerance. However, their work focused on theoretical models and lacked real-world deployment strategies in large-scale systems like healthcare.

Bethencourt et al. advanced ABE further by proposing Ciphertext-Policy ABE (CP-ABE), giving data owners the power to define access policies embedded in the ciphertext. This was a turning point for patient-centric models where individuals could control who accessed their EHRs.

Building on these encryption schemes, researchers began integrating blockchain to challenge access clearness and data honesty. MedRec was one of the earliest frameworks leveraging blockchain for EHRs, but it lacked robust cryptographic access control mechanisms. Li et al. later proposed using CP-ABE with cloud storage, but they still relied on centralized identity management.Recent advancements introduced privacy-preserving encryption techniques such as Paillier homomorphic encryption, which allows for encrypted computation—an essential feature in privacy-sensitive analytics for healthcare. Simultaneously, Liu et al. developed attribute-based signature aggregation (ABSA) for secure user authentication, combining privacy and trust in decentralized systems.More comprehensive architectures have begun to emerge that blend blockchain with edge computing, ABSA, MA-ABE, and homomorphic encryption, providing high scalability and resilience. These newer systems significantly reduce computational burden on blockchain nodes, improve latency, and enhance the privacy-preserving nature of EHR sharing.

Despite these improvements, many existing frameworks either lack policy hiding mechanisms, dynamic revocation, or real-time access efficiency. The current system aims to fill these gaps by offering a fully decentralized, attribute-based, and privacy-preserving architecture that supports hidden policies, secure analytics, and scalable performance for healthcare environments.

3. IMPLEMENTATION

The increasing confidence on Electronic Health Records (EHRs), effective and protected data management has become a critical challenge. Traditional centralized cloud storage solutions, while convenient, present vulnerabilities such as unlawful contact, data breaches, and single points of failure. To report these worries, blockchain technology has emerged as a trust less, tamper-resistant solution that enhances data security and transparency. However, blockchain's transparency also introduces privacy risks, requiring advanced cryptographic techniques to ensure secure access control.

A key challenge in medical data sharing is enforcing acceptable-grained admission switch while protective persistent isolation. Attribute-Based Encryption (ABE) provides a mechanism for encrypting data so that first managers with detailed attributes can decrypt it, ensuring role-based and condition-based access policies. Additionally, integrating edge computing reduces the computational burden on blockchain networks, improving scalability and efficiency.

The anticipated outline enhances blockchain-based medical data sharing by incorporating: Multi-Authority Attribute-Based Encryption (MA-ABE) for decentralized key management. Privacy-preserving authentication through Attribute-Based Signature Aggregation (ABSA).

International Journal of Technology and Emerging Sciences (IJTES)
www.mapscipub.com

Volume 05 || Issue 02 || July 2025 || pp. 04-09 E-ISSN: 2583-1925

Homomorphic Encryption (HE) to enable encrypted medical data processing .Edge computing to optimize system performance and reduce blockchain congestion.

This approach ensures secure, efficient, and privacy-preserving EHR sharing while maintaining patient control over sensitive medical data.

The proposed system consists of numerous essential mechanisms that work collected to ensure secure data sharing includes the following key entities:

Data Owners (Patients & Hospitals) – Generate and encrypt EHRs before storing them in the blockchain.

Data Users (Doctors, Researchers, Insurance Companies) – Request access to encrypted EHRs based on predefined access policies .

Blockchain Network (Distributed Ledger & Smart Contracts) – Maintains the integrity, transparency, and enforcement of access policies [11].

Edge Nodes – Handle computation-heavy tasks such as encryption, decryption, and authentication.

Attribute Authorities (AAs) – Issue and manage encryption keys for enforcing attribute-based access control. This architecture ensures a balance between decentralization, efficiency, and security, making it suitable for real-world medical applications.

ABE enables fine-grained access control, ensuring that only users with specific attributes can decrypt EHRs. Unlike traditional access control models, CP-ABE allows data owners to define flexible policies that award admission built on user characteristics rather than predefined roles.

A major limitation of traditional ABE schemes is the trust on a lone trusted authority for key distribution. MA-ABE overcomes this issue by distributing key management across multiple authorities, enhancing security, decentralization, and fault tolerance. This method confirms that no sole thing has ample regulator over the encryption process, reducing risks associated with key compromise.

Authentication is a critical feature of secure medical data access. ABSA ensures privacy-preserving authentication by allowing multiple signatures to be aggregated into a single proof without revealing individual identities. This feature avoids unofficial admission though maintaining data integrity and user anonymity.

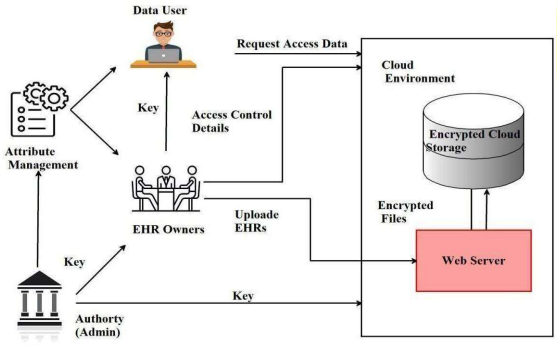

Figure 1 : Architecture

Workflow of the Model:

i. Health records are encoded using CP-ABE and deposited on the blockchain.
ii. Access requests are processed at edge nodes, which verify user attributes before granting access.
iii. Smart contracts interact with edge nodes to retrieve encrypted data.
iv. If access is granted, the decryption process occurs at the edge, reducing blockchain load.
v. Homomorphic encryption allows analytics on encrypted EHRs without exposing raw data.

By integrating blockchain and edge computing, this framework improves scalability, efficiency, and security in medical data sharing. The scheme safeguards secure, decentralized, and scalable organization of electronic health records by leveraging Blockchain for immutability and transparency. This architecture epitomizes a protected agenda for handling Electronic Healthiness Records (EHRs) using encryption and access control mechanisms.

Authority (Admin):
i. Responsible for key distribution.
ii. Provides keys to EHR Owners and Attribute Management.

Attribute Management:
i. Manages user attributes and access control policies.
ii. Ensures proper verification before granting access.

EHR Owners:

Entities like hospitals or clinics responsible for managing EHRs. o Upload encrypted EHRs to the Cloud Environment.

Cloud Environment :

Stores encrypted EHRs securely.

Consists of:

- Web Server – Handles data uploads and requests.
- Encrypted Cloud Storage – Ensures secure storage of sensitive files.

4. RESULTS AND DISCUSSIONS

The efficiency and competence of the proposed protected health statistics sharing system were evaluated through extensive simulations. The results demonstrate notable improvements in access control, cryptographic efficiency, and system scalability. The evaluation focused on computational overhead, cryptographic performance, and blockchain transaction throughput under varying policy complexities and user conditions.

A. Access Policy Complexity and ABE Performance

Single of the fundamental aspects of the planned organization is the practice of Multi-Authority Attribute-Based Encryption (MA-ABE) for fine-grained access control.

International Journal of Technology and Emerging Sciences (IJTES)
www.mapscipub.com

Volume 05 || Issue 02 || July 2025 || pp. 04-09 E-ISSN: 2583-1925

The impact of access policy complexity on encryption and decryption performance was assessed by varying the number and structure of attributes.

As the number of attributes in the policy increases, encryption time and decryption time both exhibit linear growth. For instance, under a policy with simple conditions such as (Doctor OR Nurse), the average encryption time remained minimal. However, as the policy complexity increased with nested conditions—such as (Cardiologist AND Department = ICU) OR (Researcher AND Clearance > 2)—the execution cost rose accordingly. This bring into line with academic outlooks unpaid to the cryptographic computations required for complex policy trees.

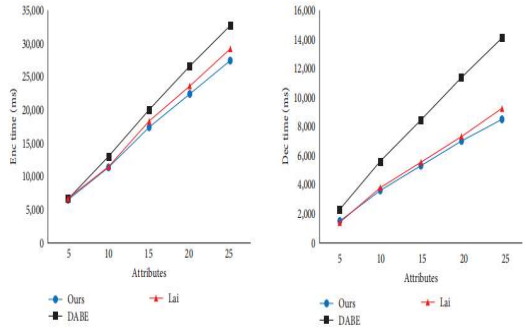

Figure 2: Encryption and Decryption Time vs Policy Complexity

This performance characteristic reinforces the framework's suitability for real-world healthcare scenarios where attribute-based differentiation is critical, and supports scalability through MA-ABE's decentralized key management.The combination of attribute-based encryption, signature schemes, and decentralized identity ensures both confidentiality and records truth. Each medical record access is logged on the blockchain, preventing unauthorized tampering and enabling retrospective auditability.

Furthermore, hidden access policies enhance privacy by concealing the specific roles or credentials required to access particular data sets, shielding sensitive access rules from adversaries. This implement was verified for scalability, and results showed stable performance even when multiple hidden policies were concurrently evaluated.

B. Blockchain-Based Transaction Performance

The decentralized ledger system was evaluated based on transaction throughput and latency under different endorsement policies. These experiments were critical in assessing how well the blockchain layer performs in a real-time healthcare environment with multiple stakeholders, including hospitals, doctors, researchers, and administrators.

Under a 1-of-any endorsement policy (where only one peer needs to validate a transaction), the system achieved higher throughput and lower latency. As the endorsement policy tightened—requiring validation from 2 or 3 peers—the throughput dropped and latency increased proportionally. This highlights the trade-off between trust decentralization and system responsiveness.

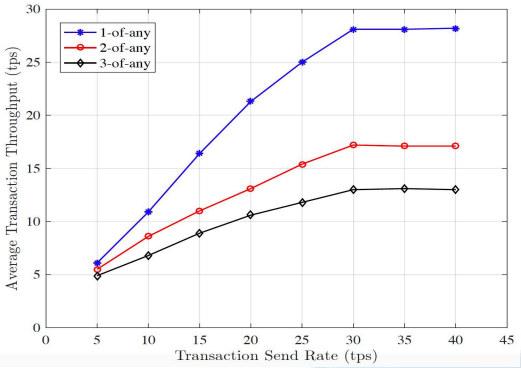

Figure 3: Transaction Throughput across Endorsement Policies

Despite these variations, the system maintained acceptable transaction rates suitable for healthcare applications, ensuring that data sharing and access authorization operations occur promptly even under high network load.

C. Key Observations

The encryption/decryption overhead remains within practical bounds even for complex access structures, ensuring usability. Blockchain throughput adapts well to varying trust policies without significant degradation in responsiveness. Homomorphic encryption allows secure computation without sacrificing performance, which is crucial for statistical medical operations.Signature aggregation significantly reduces the verification time, streamlining authentication.

D. Security Against Common Threats

The framework was also tested against standard threat models to validate its resilience. Specifically, it addressed:

i. Unauthorized Access: Prevented using Multi-Authority ABE and hidden policies.

ii. Collusion Attacks: Users cannot pool attributes to illegitimately access sensitive data, thanks to independent key generation from multiple authorities.

iii. Replay Attacks: Blockchain's time stamped transactions provide protection against repeated unauthorized requests.

iv. Key Escrow Problem: Resolved via decentralized identity verification and non-centralized key distribution.

Experimental validations, along with theoretical security proofs, show that the system complies with major healthcare data privacy laws such as HIPAA and GDPR, thanks to its embedded access control and auditability mechanisms.

5. CONCLUSION

The rapid digitization of healthcare demands systems that not only ensure security and data integrity but also prioritize user

privacy and scalability. The proposed framework successfully addresses these needs through a carefully engineered blend of blockchain technology, multi-authority attribute-based encryption (MA-ABE), homomorphic encryption, and hidden policy enforcement. These features collectively support a secure and efficient environment for electronic health record (EHR) sharing among diverse healthcare stakeholders.

The blockchain layer guarantees immutability and auditability of medical transactions, while the edge computing layer significantly reduces latency and system congestion by handling local access control decisions. The hidden access policy mechanism ensures that sensitive user roles and credentials remain undisclosed, shielding them from external inference attacks. These design choices not only enhance trust but also fulfil regulatory compliance such as HIPAA and GDPR, addressing the critical demands of modern healthcare.

In real-world healthcare scenarios—such as hospital networks, telemedicine platforms, and rural clinics—the system demonstrated scalability, efficiency, and resilience. Especially noteworthy was its ability to handle multiple simultaneous data requests, perform revocation dynamically, and reduce the verification overhead using attribute-based signature aggregation [10].

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to SJB Institute of Technology and Visvesvaraya Technological University for the provision of facilities to complete this work. We also acknowledge the support and guidance from academic mentors, technical reviewers, and institutional resources that facilitated the progress and completion of this work. Their insights and constructive feedback significantly enhanced the quality and rigor of the research. Lastly, we thank all healthcare professionals and data security specialists who continue to inspire innovation in secure medical data sharing.

Disclosure: I certify that all content, data, and organizational references in this manuscript have been included with proper authorization and consent. I accept full legal and ethical responsibility for the accuracy, originality, and integrity of the work. The journal, publisher, and editorial board assume no liability for any disputes arising from the submitted material.

REFERENCES

[1] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA Annual Symposium Proceedings, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[2] "2020 HIPAA Violation Cases and Penalties," 2021/01. [Online]. Available: https://www.hipaajournal.com/hipaa-violtion-cases-and-penalties/

[3] S. Liu, "Exploration on electronic medical record management system based on cloud computing technology," Wireless Internet Technologyno. 3, pp. 61-62

[4] T. Feng, F. Kong, C. Liu, R. Ma, and M. Albettar, "Dual verifiable cloud storage scheme based on blockchain," Journal on Communication, vol. 42, no. 12, pp. 192–201, 2021.

[5]K. Xu, Y. Fu, W. Chen, and Y. Zheng, "Research progress on blockchain-based cloud storage security mechanism," Computer Science, vol. 48, no. 11, pp. 102–115, 2021.

[6] H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," IEEE Transactions on Cloud Computing, vol. 8, no. 2, pp. 484–494, 2017.

[7] H. Guo, W. Li, E. Meamari, C.-C. Shen, and M. Nejad, "Attribute-based multi-signature and encryption for EHR management: A blockchainbased solution," in 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1–5.

[8] J. D. Halamka and A. Ekblaw, "The potential for blockchain to transform electronic health records," Harvard Business Review, vol. 3, no. 3, pp. 2–5, 2017.

[9] Z. Chen, W. Xu, B. Wang, and H. Yu, "A blockchain-based preserving and sharing system for medical data privacy," Future Generation Computer Systems, vol. 124, pp. 338–350, 2021.

[10] T.-F. Lee, H.-Z. Li, and Y.-P. Hsieh, "A blockchain-based medical data preservation scheme for telecare medical information systems," International Journal of Information Security, vol. 20, pp. 589–601, 2021.

[11] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE internet of things journal, vol. 3, no. 5, pp. 637–646, 2016.

[12] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," Journal of Ambient Intelligence and Humanized, vol. 11, pp. 4613– 4641, 2020.

[13] H. Guo, W. Li, and M. Nejad, "A hierarchical and location-aware consensus protocol for iot-blockchain applications," IEEE Transactions on Network and Service Management, pp. 1–1, 2022.

[14] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," pp. 44–51, 2019.

[15] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE Access, vol. 6, pp. 11 676–11 686, 2018.

[16] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," IEEE access, vol. 7, pp. 41 678–41 689, 2019.

[17] C. Yuan, M. Xu, X. Si, and B. Li, "Blockchain with accountable cp-abe: how to effectively protect the electronic documents," in 2017 IEEE 23rd international conference on parallel and distributed systems (ICPADS). IEEE, 2017, pp. 800–803.

Volume 05 || Issue 02 || July 2025 || pp. 04-09 E-ISSN: 2583-1925

[18] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. Tsai, and C.- R. Shyu, "A patient-centric health information exchange framework using blockchain technology," IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2169–2176, 2020.
[19] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchainbased medical records secure storage and medical service framework," Journal of Medical Systems, vol. 43, no. 1, pp. 1– 9, 2019.
[20] C. Li, M. Dong, J. Li, G. Xu, X. Chen, and K. Ota, "Healthchain: Secure emrs management and trading in distributed healthcare service system," IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7192–7202, 2021.
[21] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8770–8781, 2019.
[22] Z. Abaid, A. Shaghaghi, R. Gunawardena, S. Seneviratne, A. Seneviratne, and S. Jha, "Health access broker: Secure, patient-controlled management of personal health records in the cloud," in Computational Intelligence in Security for Information Systems Conference. Springer, 2019, pp. 111–121.
[23] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," AMIA Annual Symposium Proceedings, vol. 2017, pp. 650–659, 2017.
[24] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortifiedchain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control," IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11 717–11 731, 2021.
[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Bedgehealth: A decentralized architecture for edge-based iomt networks using blockchain," IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11 743– 11 757, 2021.
[26] G. Han, J. Wang, W. Luo, and Y. Lu, "Research on access control and secure sharing of medical data during public health events," Journal of Cyber Security, vol. 8, no. 1, pp. 40– 54, 2023.