International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

# Revolutionizing Patient Data Security with Blockchain A Dual-Access System for Medical Records

**Mrs. Ch Srivatsa Alivelu Mangatayi[1], Alekhya Siripurapu[2], Dumpala Manasa[3], Nenavath Premlal[4], Gosula Shashaank[5]**

[1, 2, 3, 4, 5]Department of Computer Science and Engineering
ACE Engineering College Medchal, India

**Abstract**

**With the increasing adoption of data outsourcing technologies such as cloud computing, healthcare providers are increasingly implementing electronic Personal Health Records (PHRs) to empower patients in managing their own medical information within scalable and resilient environments. However, PHRs contain highly sensitive personal data, making privacy and security primary concerns. It is essential for data owners to have the ability to flexibly and securely define access policies for their outsourced data. While commercial cloud platforms offer basic security features such as symmetric and public key encryption, these traditional methods face limitations in outsourced settings due to the complexity of key management in symmetric encryption and the high maintenance cost associated with managing multiple ciphertext copies in public key encryption schemes. In this paper, it proposed a secure and fine-grained access control system tailored for outsourced PHRs. Our scheme leverages Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for precise access control and integrates Proxy Re-Encryption (PRE) to support lightweight and efficient access policy updates. To further enhance security and accountability, we introduce a policy versioning mechanism that ensures full traceability of policy modifications. It also perform comprehensive performance evaluations to validate the practicality and efficiency of our proposed solution in real-world healthcare data sharing scenarios.**

**Keywords: PHRs, access control, CP-ABE, policy update, proxy re-encryption, policy versioning, performance evaluation**

## I. INTRODUCTION

In today's increasingly digital healthcare landscape, the need for secure and efficient data storage and sharing mechanisms has become critical. [1]Cloud storage systems have emerged as the preferred solution for both individuals and organizations due to their scalability, cost- effectiveness, and ease of access. Particularly in the context of medical data, where confidentiality, integrity, and availability are paramount, cloud-based solutions are transforming how patient information is handled. However, outsourcing sensitive data such as Personal Health Records (PHRs) to third-party cloud providers

introduces substantial privacy and security challenges. Traditionally, data encryption has served as the first line of defense, protecting patient information from unauthorized access. Yet, encryption alone is not enough to address the full spectrum of security requirements, especially when fine-grained and dynamic access control is necessary.

To enhance access security, Attribute-Based Encryption (ABE) schemes—most notably Ciphertext-Policy ABE (CP-ABE)—have gained attention. [2] CP-ABE enables data owners to define access policies embedded within the ciphertext, allowing only users whose attributes satisfy the policy to decrypt the data. This approach supports one-to- many encryption, reduces communication overhead, and offers flexible, decentralized access control.[3] CP-ABE systems face significant challenges during attribute revocation and policy updates, as these operations often require costly ciphertext re-encryption and key redistribution—processes that are not scalable and place a heavy computational burden on data owners, especially in environments with a large number of users.

To overcome these limitations, it proposes a novel dual- access architecture that combines the efficiency of symmetric encryption for data confidentiality with the policy-driven access control capabilities of CP-ABE, applied specifically to the encryption of the symmetric key. This separation drastically reduces the impact of policy updates, as only the encrypted key needs to be re-encrypted rather than the entire dataset.[4] further optimize the system, this introduces a Proxy Re-Encryption (PRE) mechanism that offloads the computationally intensive re-encryption tasks from the data owner to a trusted proxy, ensuring seamless policy updates with minimal resource consumption.

Additionally, our system leverages blockchain technology to introduce immutable access tracking and smart contract- based policy versioning.[6] This not only enhances transparency and auditability but also ensures that previous access policies are securely recorded and retrievable for compliance and forensic analysis. By employing parallel processing techniques, it further accelerate cryptographic operations, making the system suitable for real-time healthcare environments.

Our dual-access model empowers patients to retain control over their medical records, enabling selective sharing with healthcare providers, insurers, or researchers, while maintaining robust security and privacy guarantees. [7] This approach paves the way for a scalable, transparent, and secure healthcare data infrastructure, addressing the critical challenges of modern medical data sharing and access management.

## II. LITERATURE SURVEY

[1] Blockchain technology is increasingly recognized for its potential to revolutionize the healthcare sector, particularly in the areas of data security, interoperability, and operational transparency. This study discusses the diverse applications of blockchain in managing patient records, conducting clinical trials, and overseeing pharmaceutical supply chains. It also introduces a unified framework for integrating blockchain into existing healthcare infrastructures. By leveraging the decentralized nature of blockchain, the research emphasizes its capacity to build trust, minimize costs, and improve the overall efficiency of healthcare services.[2] This review investigates multiple blockchain-driven methodologies aimed at enhancing the security and accessibility of medical records. Emphasis is placed on transparency and decentralized data control, along with the implementation of smart contracts and permissioned ledger systems for secure health information exchange. Real-world applications such as MedRec and [10] Hyperledger are explored, offering practical insights that influenced the

conceptualization and development of the MedEx system—a secure platform for managing and distributing medical reports.[3]Addressing privacy concerns in health data exchange, this paper presents a comprehensive analysis of blockchain solutions tailored for secure and private sharing of healthcare records. It critiques centralized Electronic Health Record (EHR) storage and illustrates how blockchain's immutable and decentralized characteristics mitigate associated vulnerabilities. The study evaluates various architectures that integrate cloud services, cryptographic techniques, and smart contracts, ultimately suggesting that private and consortium blockchain models offer promising avenues for safeguarding sensitive medical information.

[4]A blockchain-enabled system is proposed in this paper to enhance the confidentiality and integrity of medical reports within healthcare networks. The system replaces traditional centralized models with a decentralized structure, employing SHA1 hashing to verify data integrity and prevent tampering. Role-based access through a Flask- based web interface ensures secure interaction among patients, healthcare providers, and administrators. The architecture not only protects sensitive data but also fosters transparency and empowers patients in the information- sharing process. The concept of proactive defense introduced by Garugu et al. [5] emphasizes pre-emptive threat detection through anomaly recognition in dynamic networks. Their system contributes to advancing adaptive network protection strategies and intrusion prevention. [6] This study introduces a robust medical data storage framework utilizing Hyperledger Fabric in combination with Attribute-Based Access Control (ABAC). Smart contracts and the Inter Planetary File System (IPFS) are employed to ensure privacy, precise access control, and secure storage. The proposed system allows for dynamic access management, facilitating efficient, tamper-proof handling of healthcare data. Performance evaluations affirm that the model achieves notable throughput, scalability, and security, making it a strong candidate for next-generation healthcare information systems. Blockchain's ability makes for a sophisticated data storage framework that records a person's whole health history of diagnosis, test reports, prior regimes, and even measurements by intelligent sensors.Garugu et al. [7] survey various ML methods, including classification and regression models, used for diagnosing and predicting rheumatic diseases. It sheds light on how supervised learning can enhance early detection and personalized healthcare.

Focusing on secure EHR sharing in cloud environments, this paper presents a blockchain framework built on Hyperledger Fabric and deployed on AWS. The system resolves critical concerns such as data privacy, platform interoperability, and scalability. It incorporates features like permissioned blockchain access, smart contracts, and a virtual private cloud infrastructure to enhance efficiency. Experimental validation confirms the model's scalability and its practical applicability in managing sensitive healthcare data securely.

The paper explores a decentralized approach to EHR system design, aimed at overcoming challenges related to security breaches, data silos, and inconsistent information flow. Using Ethereum and IPFS, the proposed architecture introduces a role-based access model enforced through smart contracts, allowing fine-grained control over data permissions. In [10], Garugu et al. developed an AI- powered diagnostic system capable of identifying diabetes and associated comorbid conditions. The integration of machine learning algorithms enables early-stage identification with enhanced diagnostic precision, contributing to the domain of AI in preventive healthcare.

## III. PROPOSED SYSTEM

In the proposed system, this presents a secure and efficient solution for managing patient medical records by integrating blockchain technology with advanced cryptographic techniques. Our methodology is designed to ensure data privacy, integrity, traceability, and controlled access. The key components of this system include block hashing with SHA-256, Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Proxy Re-Encryption (PRE), and a policy versioning mechanism.

Blockchain is employed to store hashed medical records in an immutable and decentralized structure. Each block contains a unique cryptographic hash, generated using the SHA-256 algorithm, which ensures the data within that block has not been altered. SHA-256 generates a 256-bit unique hash for each set of patient data, securing the integrity and preventing unauthorized modification. If even a single bit of data is tampered with, the hash changes, making tampering immediately detectable. This immutability guarantees data authenticity and auditability.

To complement blockchain's immutability, the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is used for securing patient records. In this method, access to encrypted data is granted based on user attributes (e.g., role, organization, purpose). This means only users who meet specific attribute requirements can decrypt and access the data. This encryption model enhances fine-grained access control and ensures data privacy, even in a distributed environment. Furthermore, it incorporate Proxy Re-Encryption (PRE) to enable secure and flexible delegation of decryption rights without exposing sensitive data or private keys. This allows a third-party proxy (like a healthcare data server) to re-encrypt the data for another authorized user based on updated access policies, without learning anything about the underlying data. PRE significantly enhances scalability and supports dynamic access management.

To ensure full traceability and transparency of access control changes, a policy versioning technique is introduced. Every time an access policy is modified, a new version is recorded and linked to the original, enabling a verifiable audit trail of policy evolution. This feature is particularly important in healthcare settings where access requirements may change due to shifts in roles, regulations.

### *A. System Architecture*

The presented architecture represents a secure framework for managing and sharing Personal Health Records (PHRs) within a healthcare ecosystem using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) in conjunction with Proxy Re-Encryption (PRE). This design enables secure storage, controlled access, and dynamic policy updates while preserving the privacy and integrity of sensitive medical data.

The system includes multiple stakeholders such as PHR owners (patients), authorized users (e.g., doctors), attribute authorities, a certification authority, and cloud-based infrastructure. PHR owners are responsible for encrypting their health records using symmetric encryption before uploading them to the storage server. The symmetric key used for this process is further encrypted using CP-ABE, which enforces fine-grained access control policies based on attributes assigned to users.

Attribute Authorities (AAs) are trusted entities that manage the distribution of decryption keys. Each authority is responsible for issuing keys based on the attributes held by users. For example, a medical

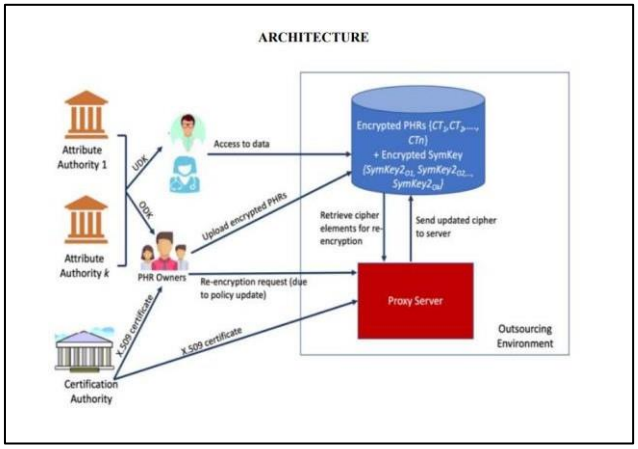
professional may receive keys linked to attributes like "Cardiologist" or "Hospital Staff." These keys are essential for decrypting the symmetric key and, subsequently, the PHR.To maintain authenticity and trust, a Certification Authority (CA) issues X.509 certificates to both data owners and users. These certificates validate the identity of entities interacting with the system and help prevent unauthorized access or impersonation.

The encrypted health records, along with their encrypted symmetric keys, are stored in a cloud-based repository. This repository forms part of the outsourcing environment where data is securely maintained without giving storage providers access to plaintext information. When access policies change or need updating—such as when user roles are modified—the PHR owner initiates a re-encryption request to the Proxy Server.

The Proxy Server acts as an intermediary during policy updates. It retrieves the required cipher elements from the storage, performs re-encryption using updated policies, and returns the revised cipher to the storage system. Importantly, the proxy does not have access to the original data or decryption keys, preserving end-to-end data confidentiality.

Authorized users with valid attributes and matching policies can request access to the encrypted records. If their credentials satisfy the embedded access policy, they are able to decrypt the symmetric key and access the medical data securely.This architectural model ensures robust access control, efficient policy updates, and secure data management in outsourced environments. It is particularly suited for healthcare systems where frequent updates to user roles, policies, and data access rights are necessary, and privacy is paramount.

**Fig 1. System Architecture**




### *B. Block Hashing for Data Integrity*

In the context of blockchain-based systems, block hashing refers to the process of generating a unique, fixed- size cryptographic value that represents the contents of a block. This is accomplished using cryptographic hash functions, with SHA-256 (Secure Hash Algorithm - 256 bit) being one of the most widely adopted in secure systems. The hash value acts as a digital fingerprint for the block, encapsulating key elements such as the transaction data, timestamp, and the hash of the previous block.

Even a minor alteration in the block's data results in a completely different hash, thereby ensuring that the integrity of the block and, by extension, the entire blockchain, is preserved.

Block hashing plays a vital role in maintaining data integrity and non-repudiation for electronic medical records. Each time a new set of medical data is recorded, it is embedded in a block and hashed using the SHA-256 algorithm. This process generates a unique hash key, which serves as an immutable identifier for that specific block of data. These unique keys are then used to track, retrieve, and verify records within the decentralized ledger. The chaining of blocks through cryptographic hashes ensures that any unauthorized modification to one block would invalidate the entire chain of hashes, immediately flagging the tampering attempt.

This approach not only secures the medical data but also enhances the traceability and accountability within the healthcare information system. By assigning a distinct hash to each medical transaction, our system ensures that patient records are immutable, securely stored, and only accessible to authorized entities. This robust mechanism significantly reduces the risk of data breaches and aligns with the growing demand for secure and transparent health data management infrastructures.

### *C. Use of SHA-256 in Data Security*

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function that produces a fixed-length output of 256 bits (64 hexadecimal characters) from any given input. It belongs to the SHA-2 family, developed by the National Security Agency (NSA), and is widely recognized for its robustness and collision resistance. The primary function of SHA-256 is to convert input data into a unique, irreversible hash value, which serves as a digital signature for the original data. This makes it an essential tool in applications where data integrity and authenticity are critical, such as blockchain technology and secure communications.

In the proposed medical record system, SHA-256 is employed to generate unique hash values for each block of patient data stored on the blockchain. The algorithm ensures that each medical record block is assigned a distinct hash, making it practically impossible to replicate or tamper with the data without detection. Even the smallest modification in the input data results in a significantly different hash output, thereby enhancing the system's ability to detect and prevent unauthorized changes. By utilizing SHA-256, our system ensures that patient records are both verifiable and immutable, providing a strong foundation for trust, security, and accountability in healthcare data management.

### *D. Implementation*

The implementation of the proposed blockchain-based medical record management system was carried out with a focus on secure, role-based access and optimized performance across different user types, as depicted in the system architecture. The platform integrates cryptographic security, blockchain immutability, and role-specific functionality to ensure reliable storage, access, and traceability of patient data.

The system is developed with modular components for each role: Patient, Doctor, Management, Authority, and Proxy. Each user is required to register and log in using secure credentials. Patients can make appointments, upload medical records, and request predictions (possibly based on AI or rule-based diagnostics). Doctors, upon logging in, can view appointments, upload reports, and access authorized patient data. Management serves as a central administrative layer that verifies appointments, doctor data, and report status. Meanwhile, Authority and Proxy roles facilitate secure key management and access delegation using Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Proxy Re-Encryption

(PRE).

At the core of the system, SHA-256 is used to generate a unique hash for each patient record block before storing it on the blockchain. This ensures tamper-resistance and provides a verifiable digital fingerprint for every data entry. The block hashing mechanism not only aids in data integrity verification but also serves as a method to create unique identifiers for data tracking and retrieval. Any alteration to the original data automatically results in a completely different hash, making unauthorized changes easily detectable.

To handle access control efficiently, CP-ABE is applied during the encryption process. This enables fine-grained access control, ensuring that only users with matching attributes (e.g., doctors from a specific department) can decrypt and access the data. The inclusion of Proxy Re- Encryption adds flexibility by allowing encrypted records to be securely re-encrypted for another user without exposing the raw data or original private keys. This is particularly useful when access policies change or when temporary access needs to be granted (e.g., a consulting specialist).

For optimization, the system uses asynchronous request handling and database indexing to reduce latency during user interactions such as login, data uploads, and report access. Additionally, lightweight cryptographic operations were chosen where possible to ensure that the system remains responsive even under high user load. The use of SHA-256, while computationally intensive, is optimized through batch processing during hash generation and validation.

Overall, the system achieves a balance between security, accessibility, and performance. The modular architecture ensures ease of maintenance and scalability, while the integration of blockchain and cryptographic techniques significantly enhances the reliability and auditability of healthcare data handling.

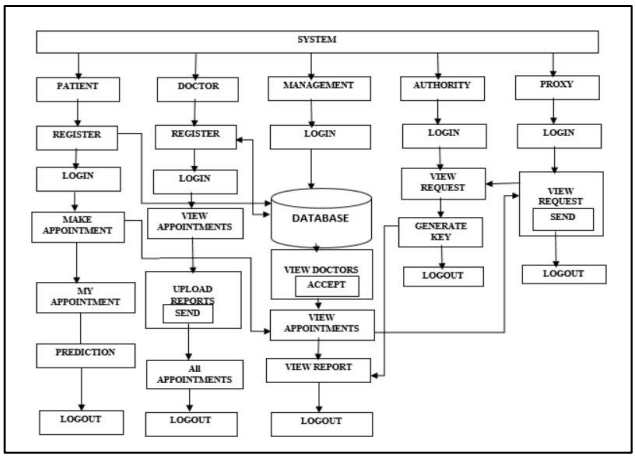



**Fig 2. Functional Flow Diagram of the Dual Access Medical Record System**

### *E. Access Control using CP-ABE and Proxy Re- Encryption*

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) serves as a highly effective access control mechanism. CP- ABE enables data owners to define flexible access policies that are embedded directly within the ciphertext. Only users whose attribute sets satisfy the embedded policy are able to decrypt the data. This model is particularly well-suited for environments such as healthcare, where access needs to be controlled based on roles, specializations, or affiliations (e.g., "Doctor", "Radiologist", or "Hospital Staff").

CP-ABE decouples the encryption process from the identity of the users, focusing instead on descriptive attributes. When a patient's medical report is encrypted using CP- ABE, access is granted to any authorized user whose attributes align with the specified policy. This approach provides fine-grained access control, ensures that patient privacy is maintained, and reduces the need for manual user authentication.

However, a challenge arises when access control policies need to be modified, such as when roles change or when user permissions are updated. To address this, Proxy Re- Encryption (PRE) is integrated into the system. PRE allows a semi-trusted proxy (such as a cloud server) to transform an existing ciphertext into a new one that conforms to an updated policy—without revealing the underlying plaintext. This means the data does not need to be decrypted and re- encrypted by the data owner, which greatly improves system efficiency and scalability.

In this combined framework, the original ciphertext is stored in a secure repository, and the proxy server performs re-encryption only when a policy update is required. This ensures that the system can support dynamic access control while preserving the confidentiality of medical records. Additionally, the proxy server is unable to access the actual content of the data, maintaining the security guarantees of the original encryption scheme.

Together, CP-ABE and PRE provide a powerful foundation for secure and flexible access control in blockchain- integrated healthcare systems. They enable attribute-based authorization, support efficient policy updates, and eliminate the need for continuous manual intervention by data owners—all while preserving data integrity and privacy.

## IV. RESULT AND DISCUSSION

The proposed system has been successfully implemented as a secure and interactive web-based healthcare management platform. The interface supports multiple stakeholders such as doctors, patients, and hospital administrators, while integrating a secure access control mechanism based on Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and proxy re-encryption. The implementation was evaluated based on functionality, usability, and the system's ability to maintain security and data privacy in healthcare record exchange.

The Proceed Page demonstrates a clear and organized categorization of medical departments including Dentistry, Cardiology, ENT, Orthopedic, Neuroanatomy, and Dermatology. This department-wise structure allows patients and hospital authorities to easily navigate through the system and choose appropriate services. It also helps in routing the access requests and encrypting the data based on department-specific policies.

The Doctor Registration Page allows medical professionals to sign up by entering their personal and professional information. This includes department selection, age, contact number, and email. Once registered, doctors are subject to approval by hospital authorities. This manual validation mechanism ensures only certified professionals can access sensitive medical data, aligning with the security goals of the system. The Doctor Request and Doctors List pages provide administrators with tools to view incoming requests and track approved users.

The Hospital Management Interface plays a crucial role in overseeing doctor registration and department

management. Hospital authorities can securely log in to a dedicated admin panel, monitor user activity, and approve or reject doctor registration requests. The interface reflects the system's emphasis on centralized oversight while preserving decentralized access via encryption policies.

Similarly, the Patient Registration and Login Pages enable patients to create accounts by submitting basic demographic details. Once registered, they can log in and view departmental services, allowing them to book appointments or initiate data exchange. Importantly, patient health records are encrypted and access is granted only when attribute- based conditions are met, as enforced by CP-ABE and re- encryption policies.


*Fig 1. Home Page*

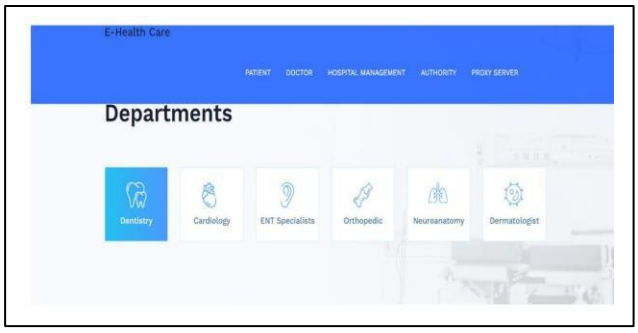



*Fig 2. Doctor Login Page*


*Fig 3. Hospital Management Login Page*

*Fig 4. Patient Appointment*


*Fig 5. Patient Unique key*


*Fig 6. Patient Report*

## V. CONCLUSION

In this work, it proposed an innovative policy update scheme based on policy outsourcing and proxy re-encryption techniques. Our scheme effectively offloads the policy update cost to an outsourced server, ensuring that administrators or data owners do not need to directly manage the re-encryption process.

The integration of multi-threaded re-encryption further enhances scalability and optimizes system performance. To validate our approach, we developed a GUI-based tool for CP-ABE (Ciphertext-Policy Attribute-Based Encryption) policy updates. This tool allows data owners to upload encrypted files and associated policies to outsourced storage, streamlining the management of access control and policy updates.

Moreover, the system facilitates transparent and efficient policy management, enabling updates anytime and anywhere via the web-based interface. Additionally, we introduced a policy versioning technique, which provides a mechanism for reconstructing historical policies, making it suitable for rigorous auditing and compliance requirements. Our experimental results demonstrate the significant performance gains achieved through multi-threaded re- encryption, as compared to single-threaded approaches, confirming the effectiveness and efficiency of our proposed scheme.

## VI. REFERENCES

[1] Parchani, C., Ali, G. M., Ghume, R., & Trivedi, V. (2023). "MedEx: Secured Medical Report Management System using Blockchain Technology." Vivekanand Education Society's Institute of Technology, Mumbai, Maharashtra.

[2] Jacob, B. M., Mohan, D., Shereef, S., Nair, V. S. V., & Pallathu, S. T. (2020). "Medical Report Management and Distribution System on Blockchain", St. Thomas College of Engineering & Technology, Kerala, India.

[3] Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). "Blockchain technology applications in healthcare: An overview."

[4] S. Garugu, P. V. Vihari, M. P. Reddy, and R. Chethan, "Proactive Network Defense," Int. J. Prog. Res. Eng. Manag. Sci., vol. 5, no. 1, pp. 1691– 1699, Jan. 2025.

[5] Shahnaz, A., Qamar, U., & Khalid, A. (2019). "Using Blockchain for Electronic Health Records." National University of Science and Technology (NUST), Pakistan; Queen's University Belfast, U.K.

[6] Mustafa Tanrıverdi, "A Systematic Review of Privacy-Preserving Healthcare data sharing on Blockchain",2020

[7] S. Garugu, U. Davulury, and D. Anusha, "A Survey of Machine Learning Techniques in Rheumatic Disease," Int. J. Anal. Exp. Modal Anal., vol. 12, no. 3, pp. 2492–2504, Mar. 2020.

[8] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Proc. 24th Annu. Int. Conf. Appl. Cryptograph. Technique (EUROCRYPT) (Lecture Notes in Computer Science). Berlin, Germany: Springer, May 2015, pp. 457–473.

[9] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attribute-based encryption,'' in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

[10] S. Garugu, D. H. S. Nangunuri, R. Srujana, and S. Srivastava, "Comorbid Systematic Health Analyzer: A Comprehensive AI-Driven Diagnostic Tool for Predicting Diabetes and Comorbid Conditions," Int. J. Sci. Res. Arch., vol. 14, no. 1,pp. 1252–1263, 2025, doi: 10.30574/ijsra.2025.14.1.0183.

[11] L. Cheung, J. Cooley, R. Khazan, and C. Newport, ''Collusion resistant group key management using attribute-based encryption,'' Cryptol. ePrint Arch., Tech. Rep. 2007/161. [Online].

[12] S. Belguith, N. Kaaniche, and G. Russello, ''PU- ABE: Lightweight attribute-based encryption supporting access policy update for cloud assisted IoT,'' in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 924–927.

[13] S. Garugu, Ch. P. Sri, and Ch. P. Reddy, "Personal Digital Detox Evaluator: Machine Learning Model for Prediction of Smartphone Addiction," Int. J. All Res. Educ. Sci. Methods, vol. 13, no. 1, pp. 1952– 1958, Jan. 2025.

[14] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A Blockchain-based Framework for Integrity and Privacy-preserving Data Sharing in Smart Cities,"Jun. 2020.

[15] K. Sultan, U. Ruhi, and R. Lakhani, "Conceptualizing Blockchains: Characteristics and Applications," in 11th IADIS International Conference on Information Systems, 2018

[16] "Blockchain Distributed Ledger Market Size by Type, End-User," Allied Market Research Report, 2017.

[17] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing

of Mobile Cloud Based E-Health Systems," IEEE Access, vol. 7, pp. 66792–66806, 2019