Blockchain-enabled Personal Health Record Management

M.R. Surekha[1], Kabilraj M.B[2]. Satheesh Raj R P[2] and Vishal Dani W [2]
Assistant Professor[1], Final year[2]
Department of Information Technology
St.Joseph College of Engineering
Sriperumbudur , Chennai-602 117

***Abstract*—** The broad acknowledgment of blockchain-based administrations in the medicinal services area has brought about financially savvy and helpful trade of Personal Health Records (PHRs) among a few taking part entities of the e-Health frameworks. By the by, putting away the secret wellbeing data on cloud servers is helpless to disclosure or robbery and requires the advancement of methodologies that guarantee the protection of the PHRs. Along these lines, we propose a system leveraging Attribute-Based Encryption (ABE) for the secure sharing of PHRs in the cloud. The ABE methodology guarantees fine-grained, attribute-driven control over the PHRs while preserving their confidentiality. Patients store encrypted PHRs on untrusted cloud servers and define attribute-based access policies to selectively grant access to different types of users for specific portions of the PHRs. A trusted authority is introduced to manage key generation, attribute distribution, and policy enforcement. Furthermore, the methodology is secure against insider threats and ensures both forward and backward access control. The functioning of the ABE-based approach is formally analyzed and validated using High-Level Petri Nets (HLPN). Performance evaluation regarding time consumption demonstrates that the ABE-based system is a promising solution for securely sharing PHRs in the cloud.

I. INTRODUCTION

The rapid digitization of healthcare services has led to the extensive generation and storage of Personal Health Records (PHRs), enabling more efficient and patient-centric care. While these records offer significant benefits in terms of accessibility and medical coordination, they also raise serious concerns regarding data privacy, security, and unauthorized access. Blockchain technology has emerged as a promising solution for ensuring data integrity, transparency, and decentralization in health information systems. However, blockchain's inherent transparency can pose privacy challenges, especially when handling sensitive medical data. To address these issues, this paper proposes a robust framework that combines blockchain with Ciphertext-Policy Attribute-Based Encryption (CP-ABE). This hybrid approach enhances the confidentiality and access control of PHRs by ensuring that only authorized users with appropriate attributes can decrypt and access the information. The proposed method aims to offer a secure, scalable, and privacy-preserving system for PHR sharing that aligns with the needs of modern healthcare infrastructure.

II. SYSTEM STUDY

The system leverages open-source tools such as Java, MySQL, and blockchain frameworks, which significantly reduce software licensing and development costs. Additionally, cloud-based infrastructure eliminates the need for expensive on-premise servers, providing a cost-efficient and scalable platform. The minimal investment required in hardware and software resources makes the proposed solution financially viable and practical for healthcare institutions with limited budgets.

A. Economical feasibility study

The economical feasibility of the proposed system evaluates whether the project is financially viable and sustainable. Developing a secure, blockchain-based PHR sharing platform requires investment in development, deployment, and maintenance. However, the system leverages widely available open-source tools and technologies, such as Java, MySQL, and blockchain frameworks, significantly reducing development costs. Additionally, cloud infrastructure allows for scalable storage and computing resources without the need for large upfront capital. As a result, the project remains within a reasonable budget and is considered economically feasible for institutions aiming to enhance data privacy and security.

B. Technical feasibility study

The technical feasibility analysis examines whether the existing technology and resources can support the proposed system. The system is designed using established and reliable technologies such as Java, NetBeans IDE, MySQL, and Attribute-Based Encryption (ABE), all of which are compatible with modern IT infrastructures. Moreover, the system's architecture is

modular and scalable, allowing it to integrate seamlessly with existing healthcare systems. The use of cloud servers and blockchain technology ensures efficient data management, access control, and secure storage. These factors confirm that the system is technically feasible and can be implemented without significant changes to current technical environments.

C. Social feasibility study

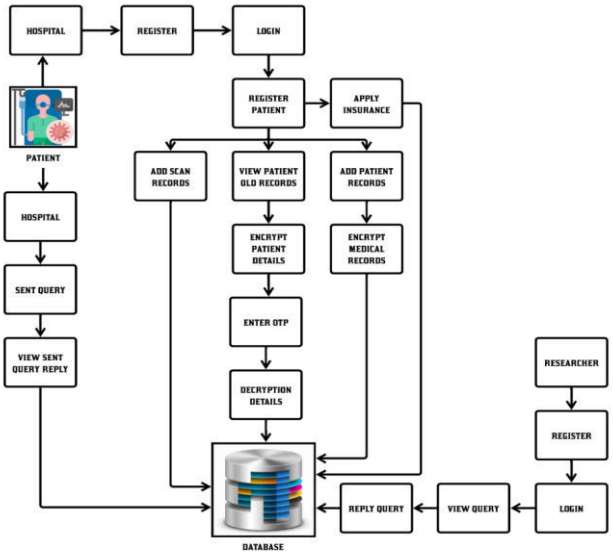
Social feasibility considers the acceptance of the proposed system by its intended users, including patients, healthcare providers, and administrative personnel. The system emphasizes user empowerment by giving patients control over who accesses their personal health data through attribute-based access policies. This patient-centric approach aligns with the growing demand for transparency and privacy in digital health solutions. With adequate training and user-friendly interfaces, stakeholders are likely to trust and adopt the system. Furthermore, by addressing privacy concerns and enhancing security, the solution fosters confidence among users, indicating strong social feasibility for deployment in healthcare settings.

III. ARCHITECTURE DIAGRAM

The process begins with registration, where both hospitals and researchers must register and log in to access the system. Hospitals can register patients, apply insurance, and manage health records. Upon registering a patient, hospitals can add scan reports, medical records, or view previous records. To ensure security, both patient details and medical records are encrypted before being stored in the database. An OTP (One-Time Password) mechanism is used to authorize access, followed by decryption for legitimate viewing.

All encrypted records are securely stored in a centralized database. Patients can interact with hospitals by sending queries, which hospitals can respond to, and the replies are viewable to patients. On the other hand, researchers follow a similar process: they must register, log in, view query data, and are allowed to reply to queries as well, depending on their access privileges. The use of encryption and role-based workflows ensures privacy, controlled access, and integrity of sensitive medical data throughout the system.

To access this encrypted information, an OTP (One-Time Password) is used, followed by a decryption process that ensures only authorized personnel can view the data. The system also supports viewing of old patient records, which follows the same secure decryption mechanism. Additionally, the platform allows hospitals to initiate queries related to patient data and view replies from the system. Patients, on their part, interact with the hospital to access services, send queries, and view query responses. Meanwhile, researchers can register and log in to the system to submit and view queries, contributing to data analysis while maintaining privacy. Overall, the system ensures a secure and controlled environment for managing and sharing PHRs by leveraging encryption, authentication, and access control mechanisms.



IV. LIST OF MODULES

1. Admin Modules
2. Unique Id And Key verification
3. Reports Upload
4. Doctor Counseling
5. User Entry Checking
6. Database Report Search

A. Admin Modules

In this Module , an User must Authorised in an our application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users... Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information.

B. Unique Id And Key verification

In this module, when an every provider must have an unique hospital details and doctor list. When an User comes under in an application and accepts the Provider for further Proceeding Comes under in the booked Provider alone.

C. Reports Upload

In this module, When an User booked his Provider along with Hospitality Functions and Doctor Specialist in an application...Once an User come back for further Process They made an counselling to Particular Doctor

D. Doctor Counseling

We consider the server to be semi-trusted, That means the server will try to find out as much secret information in the stored PHR files aspossible, but they will honestly follow the protocol in general. On the other handsome users will also try to access the files beyond their privileges. For example; A pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits.

E. User Entry Checking

In this Module, we had implemented main goal of the Project it denotes security for viewing our personal information to all roles in an application...To prevent that we had proposed to use Attribute Based Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view By others

F. Database Report Search

In this module, admin can able to view overall users report,Users personal Records and User Counselling Records....In Such Case, User had made encrypted their information it will visualization in cipher text format and age display in the K-Anonymity format.

V. SCOPE FOR FUTURE DEVELOPMENT

The proposed framework of integrating attribute-based encryption (ABE) with blockchain for secure personal health record (PHR) sharing presents numerous opportunities for future development. One potential avenue lies in the integration of artificial intelligence and machine learning algorithms to dynamically assess and adjust access policies based on user behavior and risk levels. Additionally, the system can be expanded to support interoperability with various healthcare information systems and electronic health record (EHR) platforms, enabling seamless data exchange while maintaining security and privacy.

Future research could also focus on reducing the computational overhead and latency associated with encryption and blockchain operations, thereby improving scalability and performance. Moreover, incorporating decentralized identity (DID) solutions and zero-knowledge proofs can further enhance user anonymity and data confidentiality. As regulatory frameworks around health data evolve, aligning the system with global compliance standards such as HIPAA and GDPR will also be crucial for widespread adoption and trust.

VI. CONCLUSION

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access provided by the patients. We implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we formally analyzed and verified the working through the HLPN, SMT-Lib, and the solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability to securely share the PHRs in the cloud environment.

VII. REFERENCE

[1] ANTONIO LOPEZ MARTINEZ , MANUEL GIL PEREZ , AND ANTONIO RUIZ-MARTINEZ, “A Comprehensive Model for Securing Sensitive Patient Data in a Clinical Scenario,” VOLUME 11,September 2023.

[2] HUA SHEN,“EnhancingDiagnosis Prediction in Healthcare With Knowledge-Based Recurrent Neural Networks.,” VOLUME11, September 2023.

[3] VISHWA AMITKUMAR PATEL , PRONAYA BHATTACHARYA , SUDEEP TANWAR , RAJESH GUPTA , GULSHAN SHARMA , PITSHOU N. BOKORO AND RAVI SHARMA “Adoption of Federated Learning for Healthcare Informatics: Emerging Applications and Future Directions” VOLUME 10, September 2022.

[4] ABDULLAH AL MAMUN, SAMI AZAM AND CLEMENTINE GRITTI.,“Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction.” VOLUME 10, January 18 2022.

[5] ALAA HADDAD, MOHAMED HADI HABAEBI , MD. RAFIQUL ISLAM , NURUL FADZLIN HASBULLAH AND SURIZA AHMAD ZABIDI.., “Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems.,” VOLUME 10, September 2022

[6] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, ‘‘BinDaaS, ‘‘Blockchain-based deep-learning as-a-service in healthcare 4.0 applications,’’ IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1242–1255, Apr. 2021.

[7] A. AwadAbdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O’Connor,

and J. Laughton, ‘‘MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchang,’’ IEEE Internet Things J., vol. 8, no. 21, pp. 15762–15775, Nov. 2021.

[8] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, ‘‘A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud,’’ IEEE Access, vol. 8, pp. 170713–170731, 2020.

[9] V. Jaiman and V. Urovi, ‘‘A consent model for blockchain-based health data sharing platforms,’’ IEEE Access, vol. 8, pp. 143734–143745, 2020.

[10] S.Cao, J. Wang, X. Du,X. Zhang, and X. Qin, ‘‘CEPS: A crossblockchain based electronic health records privacy-preserving scheme,’’ in Proc. IEEE Int. Conf. Commun. (ICC), Jun. 2020, pp. 1–6.