Secure Data Storage and Data sharing using Blockchain Technology for hospital management

Ms. Geethu Mary George, Praveen Kumar.S, Sahidhullah.H, Kandhan.N, Vinoth Kumar. G
Assistant Professor, Students Department of Information Technology,
Karpagam College of Engineering,Coimbatore

ABSTRACT -The abstract describes a hospital data management system that focuses on data security problems. It focuses on the use of Elliptic Curve Cryptography (ECC) for authentication and data encryption. It covers data security utilizing block chain technology and efficient data processing using edge computing. The suggested system guarantees the secure administration, access, and preservation of healthcare data. To improve data security, use Elliptic Curve Cryptography for authentication and encryption. To protect data secrecy with block chain technology and access control. To improve data retrieval and processing efficiency via edge computing. Create a complete system for safe healthcare data administration and upkeep.

1. INTRODUCTION

The reliance on a centralized key server poses several challenges to the overall system. Notably, the computational and communication costs are heightened, potentially leading to slower performance and increased operational expenses. The necessity for rekeying at the individual level during join/leave operations results in a greater consumption of resources, contributing to inefficiencies. Moreover, the system exhibits high memory usage and employs longer encryption key lengths, further impacting resource utilization. The extended data transmission time and execution duration indicate potential delays, which can be critical in scenarios requiring low latency. Addressing these issues may involve exploring decentralized key management solutions, optimizing encryption processes, and implementing more efficient rekeying mechanisms to enhance overall system performance.

Decentralized storage models offer numerous benefits, revolutionizing traditional data storage paradigms. By distributing data across a network of nodes rather than relying on a centralized server, these models enhance security through cryptographic protocols and eliminate single points of failure. This results in increased resilience to cyberattacks and improved data integrity. Furthermore, decentralized storage promotes user privacy, as individuals retain control over their data and can choose who accesses it. The distributed nature of the storage system also enhances scalability, ensuring efficient handling of growing data volumes without compromising performance. Additionally, decentralized storage models often leverage blockchain technology, fostering transparency and accountability in data management. Overall, the decentralized storage paradigm presents a more secure, scalable, and user-centric approach to handling and safeguarding digital information.

Relying on a centralized key server poses significant challenges, including heightened computational and communication costs, potential performance slowdowns, and increased operational expenses. Individual-level rekeying during join/leave operations contributes to resource inefficiencies, with high memory usage and longer encryption key lengths further impacting overall resource utilization. Extended data transmission times and execution durations introduce critical latency concerns. Addressing these issues necessitates exploring decentralized key management solutions, optimizing encryption processes, and implementing more efficient rekeying mechanisms. In contrast, decentralized storage models revolutionize traditional paradigms by distributing data across a node network, enhancing security through cryptographic protocols, eliminating single points of failure, and improving data integrity. This approach prioritizes user privacy, granting individuals control over their data access. The distributed storage system ensures scalability, efficiently managing growing data volumes without performance compromises. Leveraging blockchain technology enhances transparency and accountability in data management, presenting an overall secure, scalable, and user-centric solution for handling and safeguarding digital information.

2. LITERATURE REVIEW

Hassan Mansur [1] et al. have suggested in this study, the healthcare industry is greatly impacted by the notable rise in the application of block chain technology in healthcare. This report evaluated prior efforts in order to bridge the gap between block chain technologies and the healthcare industry. The distribution of datasets, venues, keywords, and citations were all analyzed bibliometric ally to determine the trend of block chain technology in healthcare. E-health and telecare medical information system case studies were also examined and assessed for security and privacy. This study covered a number of potential future issues, including standards, block chain size, universal interoperability, and scalability and storage capacity. The reasons for using block chain technology in the healthcare sector were emphasized in this work.

Ibtisam et al. [2] have proposed The concealment approach is one of the methods used in information security, where data is stored in another information medium and concealed so that it is not discovered during two-way communicating. In order to protect data from hackers and detection, an algorithm for data concealment and encryption employing many methods was suggested in this research. The shape of a wave of information (one- and two-dimensional data) and its many mathematical formulas were altered using a wavelet transformer. There were two sets of data employed: the first group was used in a covert manner. The second group was taken into consideration as an encryption and embedding method. By extracting the second group's high-value features and deleting them from the mother's information wave, the data is lowered to a level that is sufficient for the modulation process.

Ismail Leila et al. [3] Electronic Health Records (EHRs), as this system has suggested, have gained popularity as a way for hospitals to store and handle patient data. The existing healthcare system is more accurate and economical when these records are shared. The client-server architecture used to store EHRs currently permits hospitals or cloud service providers to maintain stewardship of patient data. Furthermore, heterogeneous databases are used to disperse patient records around several hospitals. As a result, patients struggle to put together a coherent picture of their medical history so they can concentrate on the specifics of their treatment. The healthcare industry has a bright future thanks to the block chain's security characteristics and replication mechanism, which offer answers to the client-server architecture-based EHR management system's complexity, confidentiality, integrity, interoperability, and privacy problems.

Vangelis Malamas et al. [4] there are a number of interconnected stakeholders in the health care ecosystem, each with varying and occasionally competing security and privacy concerns. It can be difficult to share medical data that is occasionally produced by remote medical devices. While there are a number of solutions in the literature that address security and privacy requirements like data privacy and fine-grained access control, as well as functional requirements like interoperability and scalability, striking a balance between them is a difficult task because there are no readily available solutions. Centralized cloud architectures, although offering scalability and interoperable access, are predicated on high trust. Conversely, decentralized block chain-based solutions usually do not support dynamic changes in the underlying trust domains, but they do offer independent trust management and data privacy. In this research, we propose a unique hierarchical multi expressive block chain architecture to fill this need. A proxy block chain allows autonomously run trust authorities to collaborate at the highest level. If a widely accepted domain-wise access policy is followed, end users from various health care domains, such as hospitals or device makers, can access and safely exchange medical data.

Lee Hsiu-An et.al. [5] Traditionally, conventional clinics in this system have provided medical services with an emphasis on treating diseases. But as the world's population ages, there is a growing disconnect between the services that clinics provide and what their patients actually require. This implies that clinics could not have the necessary resources to provide patients with the full spectrum of care, which could lead to avoidable medical harm. In its 2016 Multimorbidity Clinical Assessment and Management Guidelines Report, the National Institute for Health and Care Excellence stressed the value of incorporating patient-centered decision-making techniques for a range of issues, with a particular emphasis on precision medicine. Precision medicine is a disease prevention and treatment approach that takes into account each person's unique genetic, environmental, and lifestyle variations. This information is utilized to identify the dynamic adjustments and individualized care

plans required for both clinical and preventative healthcare. Precision medicine's primary components include historical disease data, daily vital sign data, personal health management, and the exchange of medical records.

3. EXISTING SYSTEM

Cloud-based storage solutions are being used extensively for IoT data storage, processing, and sharing. Regardless of its contribution, the existing cloud-based architecture may result in serious data leakage or compromise user privacy. Meanwhile, the cloud architecture is primarily reliant on a trusted third-party auditor (TPA) and operates under centralized supervision. However, the TPA may not be an entirely trustworthy organization, and a single point of failure might bring the whole system down. Fortunately, with the introduction of block chain technology, the decentralized storage concept has gained prominence. A decentralized storage system successfully eliminates the TPA rule, overcomes the problem of a single point of failure, and offers other advantages over a centralized control architecture, including low storage costs and high throughput. This paper proposes a block chain-based decentralized distributed storage and sharing strategy that includes end-to-end encryption and fine-grained access control. In our proposed IoT Chain concept, fine-grained authorization is based on attribute-based access control (A-BAC) policy, with the Ethereal block chain serving as an auditable access control layer. Smart contracts are designed specifically for the IoT Chain concept, which integrates the Ethereum block chain with the interplanetary file system (IPFS). We utilized an advanced encryption standard (AES) for encryption and the elliptic curve Diffie-Hellman key exchange protocol for secret key sharing between data owners and consumers.

4. SECURITY

Patient data security is of paramount importance in healthcare for several critical reasons. Firstly, patient data contains highly sensitive information, including medical history, treatment plans, and personal identifiers, making it a prime target for cybercriminals seeking to exploit or misuse this data for financial gain or identity theft. Breaches in patient data security not only compromise individual privacy and trust in healthcare providers but also pose significant risks to patient safety and well-being. Moreover, healthcare data breaches can lead to legal and regulatory consequences, including hefty fines and damage to the reputation of healthcare organizations. Ensuring robust security measures, such as encryption, access controls, regular audits, and staff training, is essential to safeguard patient data integrity, confidentiality, and availability, thereby upholding the trust and integrity of the healthcare system as a whole.

5. BLOCKCHAIN TECHNOLOGY

Blockchain technology has emerged as a promising solution for secure and transparent data storage, offering decentralized and immutable ledgers that enhance trust and reliability. By leveraging distributed consensus mechanisms, blockchain enables the creation of tamper-proof records, making it ideal for storing sensitive information such as financial transactions, medical records, and supply chain data. Its decentralized nature eliminates the need for intermediaries, reducing the risk of single points of failure and enhancing data resilience. Moreover, smart contracts embedded within blockchain networks automate storage and retrieval processes, streamlining operations and ensuring compliance with predefined rules and protocols. As the demand for secure and efficient data storage solutions continues to rise, blockchain technology stands poised to revolutionize the way organizations manage and safeguard their valuable information assets.

6. ELLIPTIC CURVE CRYPTOGRAPHY ALGORITHM

Elliptic Curve Cryptography (ECC) stands out as a powerful encryption algorithm renowned for its efficiency and robust security features. Leveraging the mathematical properties of elliptic curves, ECC offers a compelling advantage over traditional cryptographic systems by providing strong encryption with smaller key sizes. This efficiency is particularly valuable in resource-constrained environments such as mobile devices and IoT devices. ECC's ability to deliver high levels of cryptographic strength while conserving computational resources makes it an attractive choice for securing sensitive data in diverse applications, ranging from secure communication channels to digital signatures and authentication protocols. Its widespread adoption underscores its reliability and effectiveness in safeguarding information against unauthorized access and malicious threats in the digital realm.

6.1 KEY GENERATION IN ELLIPTIC CURVE CRYPTOGRAPHY

In Elliptic Curve Cryptography (ECC), key generation plays a pivotal role in ensuring the security and integrity of cryptographic operations. The process involves selecting a random private key, which is a large integer typically generated within a specific range determined by the curve's parameters. From this private key, a corresponding public key is computed using scalar multiplication of a base point on the elliptic curve. The resulting public key, which consists of coordinates on the curve, is then made available for use in encryption, digital signatures, or other cryptographic tasks. The strength of ECC lies in the difficulty of deriving the private key from the public key, a process known as the elliptic curve discrete logarithm problem (ECDLP). Through proper key generation techniques and adherence to recommended security practices, ECC provides robust cryptographic mechanisms for securing sensitive data and communications in various digital environments.

6.1.1 STEPS INVOLVES IN KEY GENERATION

- Select a Curve: Choose an elliptic curve defined over a finite field. The curve equation typically takes the form: $y^2 = x^3 + ax + b$ where a and b are parameters defining the curve.
- Select a Base Point (Generator Point): Choose a point G on the selected elliptic curve. This point serves as the generator for the elliptic curve group. Its coordinates G = (x G , y G) must satisfy the curve equation.
- Determine the Order of the Base Point: Calculate the order n of the base point G. The order is the number of times G must be added to itself (using elliptic curve point addition) until it returns to the identity element (usually denoted as O).
- Select a Private Key: Choose a random integer d from the interval [1, − 1] [1, n−1]. This integer serves as the private key.
- Compute the Public Key: Compute the public key P, which is the result of multiplying the base point G by the private key d. This is done using scalar multiplication on the elliptic curve: P=d·G
- The public key P is a point on the elliptic curve.
- Encode the Public Key: Depending on the application, the public key P may need to be encoded into a specific format for transmission and use.
- Keep the Private Key Secure: The private key d must be kept secret by the owner and should not be shared.

6.2 DATA ENCRYPTION IN ELLIPTIC CURVE CRYPTOGRAPHY

In Elliptic Curve Cryptography (ECC), encryption involves transforming plaintext data into ciphertext using elliptic curve operations and key pairs. To encrypt data, the sender typically generates a random value, known as an ephemeral key, and performs scalar multiplication of the recipient's public key with this value. The resulting point on the elliptic curve is combined with the plaintext data using mathematical operations to produce the ciphertext. The security of ECC encryption relies on the computational complexity of the elliptic curve discrete logarithm problem (ECDLP), which makes it infeasible for an attacker to derive the plaintext from the ciphertext without knowledge of the private key associated with the recipient's public key. Through its efficient use of mathematical properties, ECC encryption offers a secure and scalable solution for protecting sensitive data in various digital communication channels.

Encryption technique is used to send confidential data over communication. The process of encryption requires two things an encryption algorithm and key.

Encryption is happened at the sender side. Encrypted algorithm is made to make information unreadable by all intended receivers.

Encrypt (plaintext, key) = cipher text

6.3 DATA DECRYPTION IN ELLIPTIC CURVE CRYPTOGRAPHY

In the decryption part of Elliptic Curve Cryptography (ECC), the recipient uses their private key to retrieve the original plaintext from the ciphertext. The recipient begins by applying scalar multiplication of their private key with the ciphertext received from the sender. This process generates a shared secret point on the elliptic curve.

The recipient then extracts the original plaintext by combining this shared secret point with the ciphertext using appropriate mathematical operations. The strength of ECC lies in the difficulty of deriving the private key from the public key, ensuring that only the intended recipient possessing the correct private key can decrypt the ciphertext and retrieve the original message. This robust cryptographic mechanism provides a secure means of communication and data transfer, safeguarding sensitive information from unauthorized access and interception.

Decryption is the reverse process of encryption. It is technique to convert the encrypted data to its original data that is now readable. Decryption technique need separate Decryption algorithm and a key. Encryption and Decryption algorithm are same.

Decrypt (cipher text, key) = plaintext

7. METHODOLOGY

In our study, we address the significant privacy risks associated with cloud-based storage by employing a methodology that prioritizes data encryption and secure upload mechanisms. Specifically, we utilize elliptic curve cryptography to encrypt patient data, ensuring confidentiality and integrity throughout transmission and storage processes. Furthermore, we implement a blockchain-based framework for secure upload, leveraging its decentralized architecture and cryptographic principles to enhance data security and prevent unauthorized access. This methodology not only mitigates the inherent risks of cloud-based storage but also establishes a robust foundation for protecting sensitive patient information in healthcare environments.

8. PROPOSED SYSTEM

The proposed system leverages Elliptic Curve Cryptography (ECC) for lightweight authentication and secure sharing of healthcare data. By utilizing ECC, the system ensures robust cryptographic strength while minimizing key sizes, thus enhancing overall security. Additionally, edge computing technology is integrated to store medical reports, enabling rapid data access and retrieval. Authenticated users can efficiently decrypt and process the data, ensuring seamless and secure access to critical healthcare information.

8.1 BLOCK DIAGRAM

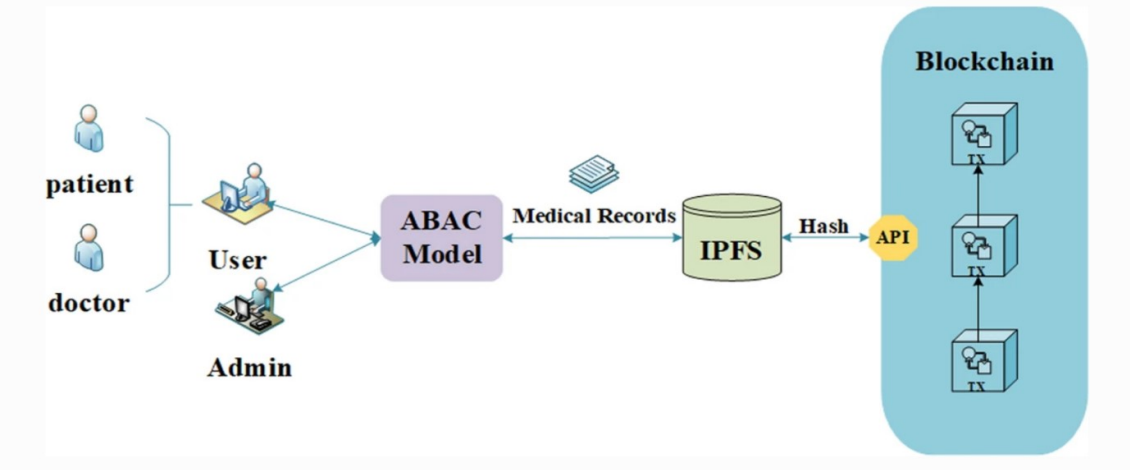

Figure 2 Block diagram of the model

8.2 REGISTRATION

The registration page for hospital management offers a streamlined process for healthcare professionals and staff to create accounts. Users can securely input personal and professional information, including credentials and contact details.

8.3 DATA ENCRYPTION

Patient data is encrypted using the ECC algorithm, ensuring robust cryptographic protection with minimal key sizes. This method enhances data security while facilitating efficient storage and transmission of sensitive medical information. ECC's mathematical properties make it well-suited for encrypting patient data, providing a balance between security and computational efficiency. Through ECC encryption, patient confidentiality and privacy are upheld, maintaining the integrity of healthcare systems.

8.4 DATABASE STORAGE

The encrypted healthcare data is securely stored in the database utilizing blockchain technology. This ensures immutability and transparency, enhancing the integrity and trustworthiness of the stored information. Users can access and verify the encrypted data on the blockchain, ensuring secure and reliable sharing of healthcare records.

8.5 SHARE THE DATA TO THE PATIENT

The decrypted healthcare data is securely shared with the patient, ensuring transparency and accessibility to their medical information. Through a user-friendly interface, patients can access and review their reports, empowering them to make informed healthcare decisions. This streamlined process enhances patient engagement and fosters trust in the healthcare system.

CONCLUSION

In conclusion, our study underscores the critical importance of addressing privacy concerns in cloud-based storage systems, particularly in healthcare settings. By employing elliptic curve cryptography to encrypt patient data and leveraging blockchain technology for secure upload and access control, we mitigate the inherent risks associated with storing sensitive information in the cloud. This approach not only safeguards patient privacy but also enhances data integrity and security, thereby fostering trust in the healthcare ecosystem.

REFERENCES

[1] "A hierarchical multi blockchain for fine grained access to medical data," by V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester IEEE Access, volume 8, 2020, pages 134393–134412.

[2] . "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," J. Med. Internet Res., vol. 22, no. 6, Jun. 2020, Art. no. e16748, was written by H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu.

[3] . "A decentralized blockchain-based architecture for a secure cloud-enabled IoT," by M. Marwan, A. A. Temghart, F. Sifou, and F. AlShahwan J. Mobile Multimedia, Nov. 2020, vol. 2020, pages. 389–412.

[4] . A safe charging method for electric vehicles with smart communities in energy blockchain, Z. Su, Y. Wang, Q. Xu, M. Fei, Y.-C. Tian, and N. Zhang IEEE Internet Things Journal, June 2019, vol. 6, no. 3, pp. 4601–4613.

[5] . "Performance analysis of the raft consensus algorithm for private blockchains," by D. Huang, X. Ma, and S. Zhang Jan. 2020; IEEE Transactions on Systems, Man, Cybern., Syst., vol. 50, no. 1, pp. 172–181.

[6] "A comprehensive review of blockchain consensus mechanisms," by Lashkari and P. Musilek IEEE Access, volume 9, 2021, pages 43620–43652.

[7] 10. "Digital health in physicians' and pharmacists' offices: A comparative study of e-prescription systems' architecture and digital security in eight countries," by Aldughayfiq and S. Sampalli. In February 2021, OMICS, J. Integrative Biol., vol. 25, no. 2, pp. 102–122.

[8] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372, Dec.2012.

[9] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[10] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor & Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011.

[11] C.Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[12] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis and Implementation of 89C51 Controller Based Solar Tracking System with Boost Converter" Journal of VLSI Design Tools & Technology. 2022; 12(2): 34–41p.

[13] C. Nagarajan, G.Neelakrishnan, R. Janani, S.Maithili, G. Ramya "Investigation on Fault Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[14] G.Neelakrishnan, K.Anandhakumar, A.Prathap, S.Prakash "Performance Estimation of cascaded h-bridge MLI for HEV using SVPWM" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:750-756

[15] G.Neelakrishnan, S.N.Pruthika, P.T.Shalini, S.Soniya, "Perfromance Investigation of T-Source Inverter fed with Solar Cell" Suraj Punj Journal for Multidisciplinary Research, 2021, Volume 11, Issue 4, pp:744-749

[16] C.Nagarajan and M.Madheswaran, "Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation" has been presented in ICTES'08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007

[17] M Suganthi, N Ramesh, "Treatment of water using natural zeolite as membrane filter", Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
[18] M Suganthi, N Ramesh, CT Sivakumar, K Vidhya, "Physiochemical Analysis of Ground Water used for Domestic needs in the Area of Perundurai in Erode District", International Research Journal of Multidisciplinary Technovation, pp: 630-635, 2019