



Smart Hospital and Healthcare System Using Blockchain

^a Karve Ashutosh, ^b Bhor Ashwini, ^c Pangavhane Viraj, ^d Sangale Vaishnavi, ^e Dr. R. M. Gawande

^a Department of Computer Engineering Matoshri College of Engineering & Research Centre Eklahare , Nashik-422105 , India

^b Department of Computer Engineering Matoshri College of Engineering & Research Centre Eklahare , Nashik-422105 , India

^c Department of Computer Engineering Matoshri College of Engineering & Research Centre Eklahare , Nashik-422105 , India

^d Department of Computer Engineering Matoshri College of Engineering & Research Centre Eklahare , Nashik-422105 , India

^e Project Guide, Computer Engineering Matoshri College of Engineering & Research Centre Eklahare , Nashik-422105 , India

DOI: <https://doi.org/10.55248/genipi.5.0424.0973>

ABSTRACT

Technology has evolved significantly over the years, improving various aspects of our lives. The healthcare sector, too, has benefited from technological advancements, leading to increased average life expectancy. However, several challenges persist in the way the healthcare system functions. Lack of transparency often results in trust issues between patients and hospitals. Patients may not receive proper treatment despite the fees charged, leading to dissatisfaction.

Keywords: Health records, Block chain, Encryption of data

1. Introduction

The concept of a "Smart Hospital" encapsulates the vision of a digitally-driven healthcare ecosystem that leverages cutting-edge technologies to streamline processes, enhance patient care, and fortify data security. At its core, blockchain serves as the foundational framework for this transformation, providing an immutable and decentralized ledger that ensures transparency, integrity, and trust in data transactions. Paired with advanced encryption standards, such as AES (Advanced Encryption Standard), this infrastructure establishes robust safeguards against unauthorized access, tampering, and data breaches.

Blockchain technology, renowned for its inherent characteristics of decentralization, transparency, and immutability, holds immense potential in addressing critical challenges within the healthcare sector. One of the primary pain points it addresses is the fragmentation of patient data across disparate systems and institutions. By creating a unified and interoperable platform for data exchange, blockchain facilitates seamless communication and collaboration among healthcare providers, enabling comprehensive and holistic patient care.

Moreover, the immutable nature of blockchain ensures the integrity and authenticity of medical records, mitigating the risks associated with data manipulation and falsification. This not only enhances the credibility of patient information but also strengthens regulatory compliance and auditability within the healthcare ecosystem. Patients can have greater confidence in the accuracy and security of their medical history, leading to improved trust and satisfaction with the healthcare services they receive.

By implementing AES encryption mechanisms across various touchpoints within the healthcare system, including electronic health records (EHRs), communication channels, and IoT devices, organizations can safeguard confidential patient information from cyber threats and data breaches. Furthermore, the integration of blockchain and advanced encryption standards facilitates secure and efficient transactions of healthcare data, thereby reducing administrative overheads, minimizing errors, and accelerating decision-making processes. Through smart contracts, a feature enabled by blockchain technology, stakeholders can automate and enforce predefined rules and agreements, streamlining workflows and optimizing resource utilization.

The convergence of blockchain technology and advanced encryption standards heralds a new era of innovation and resilience in healthcare. By establishing a foundation of trust, security, and interoperability, smart hospitals equipped with these technologies are poised to deliver superior patient outcomes, drive operational efficiencies, and catalyze advancements in medical research and innovation. As we embark on this transformative journey, it is imperative to harness the full potential of these technologies while prioritizing ethical considerations, privacy concerns, and regulatory compliance to ensure a sustainable and equitable future for healthcare delivery.

2. Literature Survey

The literature survey highlights the growing interest in leveraging blockchain technology and advanced encryption standards to enhance security, privacy, and interoperability in healthcare systems. Researchers emphasize the importance of encryption techniques like AES in protecting sensitive medical data

stored and shared via blockchain networks. While existing studies demonstrate promising results, further research is needed to address challenges such as scalability, regulatory compliance, and integration with existing healthcare infrastructure. Overall, the surveyed literature underscores the potential of smart hospitals and healthcare systems utilizing blockchain and AES algorithms to revolutionize data management and patient care delivery.

[1] “Enhancing Privacy and Security in Healthcare Systems Using Blockchain Technology (2019)” – This paper explores the role of blockchain technology in enhancing privacy and security in healthcare systems. It discusses how blockchain can address vulnerabilities in traditional healthcare infrastructure, such as data breaches and unauthorized access, and presents case studies illustrating the implementation of blockchain-based solutions to improve data integrity, patient consent management, and secure sharing of medical records.

[2] “Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related(2019)” – Focusing on the potential of blockchain technology in health data management, this study examines its applicability in health IT and healthcare-related research. It discusses the advantages of blockchain, such as data immutability and decentralized control, and evaluates its feasibility in addressing key challenges in healthcare, including data interoperability, patient consent, and security.

[3] “A Review of Blockchain Technology and Its Applications in Healthcare(2020)”:-

This comprehensive review explores the evolution of blockchain technology and its diverse applications in healthcare. It examines the technical aspects of blockchain, such as consensus mechanisms and smart contracts, and assesses its potential to transform healthcare delivery by improving data integrity, interoperability, and patient-centric care models.

[4] “A Blockchain-Based Smart Contract System for Healthcare Management (2016)”:-

A Blockchain-Based Smart Contract System for Healthcare Management. This study introduces a blockchain-based smart contract system for healthcare management, aiming to automate and secure healthcare transactions while ensuring compliance with regulatory requirements. It discusses the design and implementation of the system, highlighting its potential to streamline administrative processes, improve data accuracy, and enhance patient-provider interactions.

[5] “A Comprehensive Review and Directions for Future Research (2018)”:-

This review provides a comprehensive overview of blockchain applications in healthcare, emphasizing its potential to improve data integrity, security, and interoperability. While the paper discusses various use cases, it highlights the need for further research into privacy-preserving mechanisms, including encryption standards like AES.

[6] “Blockchain-Based Data Sharing in Healthcare (2019)”:-

Conduct an in-depth survey on blockchain-enabled data sharing in healthcare, discussing challenges, opportunities, and existing solutions. They emphasize the importance of encryption for secure data sharing and suggest AES as a suitable algorithm for ensuring confidentiality and integrity of medical data within blockchain networks.

[7] “A Blockchain-Based Approach for Secure Data Sharing in Healthcare Applications (2016)”:-

Azaria et Propose a blockchain-based framework for secure data sharing in healthcare, focusing on patient-centric data management and access control. The paper discusses the integration of encryption techniques, including AES, to protect sensitive medical records stored on the blockchain.

[8] “Enhancing Health Data Exchange with Blockchain and Data Encryption (2020)”:-

This review examines the potential of blockchain and encryption technologies to improve health data exchange systems. Rathi et al. discuss various encryption algorithms, including AES, and their role in ensuring data confidentiality and integrity within blockchain-based healthcare systems.

3. Software Specification Requirement

3.1 Framework

.Net Framework

3.2 Language

C#

3.3 Database

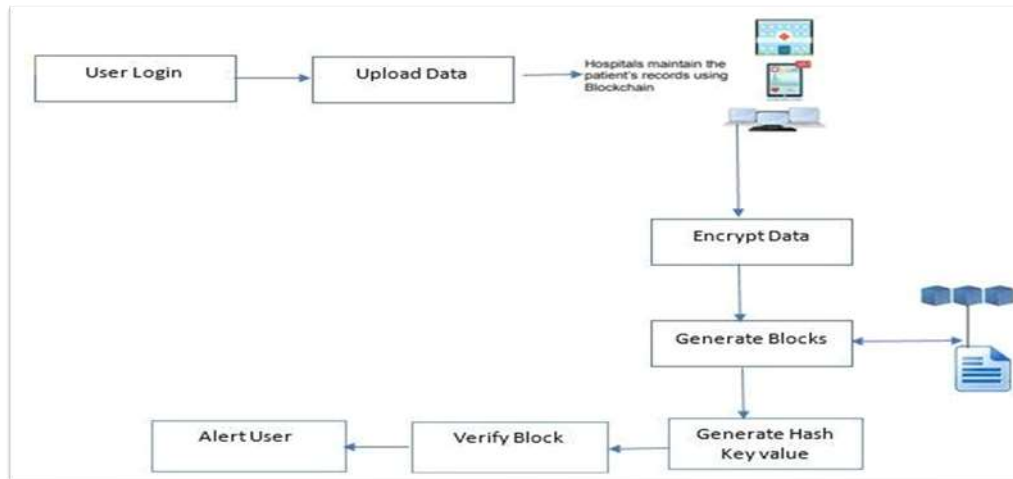
Sql Database Server

3.4 Operating System

Windows 10/11

4. Design of System

4.1 System Architecture



We illustrate the architecture to facilitate access control of EHR data by using both blockchain and edge nodes. Firstly, there is a registration process for patients in hospitals. After that, they log in to the system. The hospital inserts the patient records into the system. Then, records are encrypted with the AES algorithm for security purposes. A hash value will be generated for the particular record, and using blockchain, the record is stored in the cloud. In the cloud, both the hash value and original records are stored. If another hospital needs records, they send a request to the cloud for access to the records using a special access key. The request goes to the patient, and they give access to their record. After that, the record is sent to the hospital, and at the time of the transaction, the hash value gets verified for the particular record. If there are no changes in the record, it is successfully sent to the requested hospital. If any changes occur in the blocks at the time of the transaction, then the record is flagged as tampered with, and an alert message will be sent to the hospital through email.

5. Algorithm

The AES (Advanced Encryption Standard) algorithm is pivotal in ensuring data security within blockchain networks. With fixed block sizes of 128, 192, or 256 bits, AES encrypts sensitive information before it is stored on the blockchain. AES plays a crucial role in securing transactions, smart contract data, and personal information on the blockchain. Its widespread adoption underscores its effectiveness in safeguarding digital assets and sensitive data. By integrating AES encryption, blockchain networks uphold privacy, enhance trust, and mitigate cyber threats. The combination of AES encryption and blockchain technology offers a robust solution for securing data in various applications.

Data Encryption: AES encrypts sensitive data, such as transactions, smart contract data, and personal information, stored on the blockchain. Each piece of data undergoes encryption using AES before integration into the blockchain, ensuring confidentiality and security.

Privacy Protection: By encrypting data with AES, blockchain networks can safeguard the privacy of users and sensitive information. Encrypted data on the blockchain remains indecipherable without the corresponding decryption key, ensuring a high level of confidentiality.

Secure Transactions: AES encryption adds an additional layer of security to transactions conducted on the blockchain. When users initiate transactions, their data undergoes encryption with AES, preventing unauthorized access and tampering during transmission.

6. Results & Snapshots

Hospital Registration

ID:

NAME:

ADDRESS:

MOBILE-NO:

USERNAME:

PASSWORD:

REGISTER CLEAR

Hospit id	Hospital Name	Address	Mobile Number	UserName	Password
1	Sankrupa	lamroad	123456789	sankrupa	sankrupa
2	SMBT	dharamgach	234567891	smbt	smbt



Doctor Registration

Doctor ID:

Doctor Name:

Address:

Gender:

Date of Birth:

Education:

Age:

Blood Group:

Marital Status:

REGISTER LOGIN CLEAR

Hospital	Doctor	Doctor	Address	Gender	DOB	Education	Age	Blood	Marital	Marital	Doctor	Register
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	2	2	2

Patient Registration

Patient ID:

Patient Name:

Address:

Gender:

Date of Birth:

Education:

Age:

Blood Group:

Marital Status:

REGISTER LOGIN CLEAR

ID	Hospital	Patient	Patient	Address	Gender	DOB	Education	Age	Blood	Marital	Marital	Doctor	Register
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2

Validate Data

Enter Doctor ID:

Enter Patient ID:

Patient Name:

Get Data

Block 1:

Block 2:

Block 3:

Block 4:

Block 5:

Block 6:

Proceed For Validation

Classify Data

7. Conclusion

The integration of blockchain technology and advanced encryption standards into smart hospital and healthcare systems holds promise for enhancing security, transparency, and efficiency in the healthcare industry. Utilizing advanced encryption standards adds an extra layer of security, ensuring that patient information remains protected against unauthorized access or tampering. This not only fosters trust between patients and healthcare providers but also aids in compliance with regulatory requirements such as HIPAA. Moreover, implementing smart contracts on the blockchain can automate various healthcare processes, streamlining administrative tasks, reducing errors, and enhancing overall operational efficiency. Consequently, this could lead to cost savings for healthcare providers and ultimately contribute to improved patient outcomes. Nevertheless, it's essential to acknowledge that the adoption of blockchain technology and advanced encryption standards in healthcare systems faces challenges. These include scalability, interoperability, regulatory compliance, and the necessity for widespread industry collaboration.

REFERENCES

- [1] <http://medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d>
- [2] <http://hackernoon.com/stablecoins-designing-a-price-stable-cryptocurrency-6bf24e2689e5>.
- [3] <http://medium.com/@argongroup/stablecoins-explained-206466da5e61>.
- [4] <http://www.investopedia.com/terms/f/fungibility.asp>.
- [5] <http://www.w3.org/Protocols/Design/Interevol.html>.
- [6] <https://ischoolblogs.sjsu.edu/blockchains/useful-links/blockchain-bibliography/>.
- [7] <https://www.investinblockchain.com/estonia-blockchain-model/>.
- [8] <http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning>
- [9] <https://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf?sfvrsn=2ISO/IEC>
- [10] <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/>