Secure Med: Enhancing Patient Privacy and Care Through Blockchain

Vivek Jaiswal[1], Aditya Jagtap[2], Viraj Khude[3], Prathmesh Adsul[4], Prof. Richa Agarwal[5]

1Student, Dept. of IT, Trinity College of Engineering and Research, Pune
2Student, Dept. of IT, Trinity College of Engineering and Research, Pune
3Student, Dept. of IT, Trinity College of Engineering and Research, Pune
4Student, Dept. of IT, Trinity College of Engineering and Research, Pune
5Assistant Professor, Dept. of IT, Trinity College of Engineering and Research, Pune

ABSTRACT

In today's healthcare environment, ensuring the privacy, security, and integrity of patient information is critical. Traditional medical systems often face issues with data breaches, inaccessibility, and ineffective management of medical records. Secure Med has announced a new solution that uses blockchain technology to improve patient privacy, security, and overall care. Blockchain's decentralization, immutability, and transparency make it an ideal foundation for a secure medical data exchange system. In Secure Med, patient information is stored in a sensitive ledger, ensuring that only authorized individuals or organizations (such as physicians) have voluntary access to the information. The system creates good scrutiny for all transactions by allowing the patient to con sent to information sharing through encryption and smart contracts. The use of blockchain in healthcare not only increases privacy, but also increases the accessibility and accuracy of patient information between different doctor. This facilitates better diagnosis, treatment decisions, and continuity of care, especially in emergency situations or when patients visit a new clinic.

Keyword: - *Patient privacy, medical data security, blockchain technology, data protection, patient consent, secure data exchange, healthcare, health beliefs.*

1. INTRODUCTION :-

In today's digital age, healthcare systems have transformed into electronic systems for storing, sharing, and accessing patient information. This change has resulted in better health care services, faster communication, more accurate diagnoses, and better patient care. However, this digital revolution also raises serious concerns about the privacy and security of sensitive patient information. Medical records contain confidential information, including personal health history, treatment plans, and insurance details.

The disclosure of this information can lead to serious consequences, such as identity theft, financial fraud, or malicious unauthorized use of personal health information. This can b e a cyberattack, the use of false information, or even unintentional human error. Centralization creates failure; if a system is compromised, a large amount of patient information can be exposed in a single attack. Additionally, patients often have no control over how their medical information is stored, who can access it, or how it is used. Lack of transparency and control undermines trust between

patients and providers, which can discourage patient engagement and lead to poor quality of care. There is an urgent and growing need f or solutions that not only protect patient information, but al so give patients greater control over their information. That's where Secure Med comes in, using the power of blockchain technology to solve these complex problems. Blockchain is a distributed, immutable, and transparent digital ledger that provides a highly secure way to store and manage medical information. Unlike a centralized system, blockchain distributes data across a network of nodes, reducing the risk of data leakage, as there is no single attack. information. Smart contracts are personalization protocols encoded on the blockchain that allow patients to grant or revoke access to their medical information when necessary.

This ensures that doctors can only view patient information with explicit permission, thus ensuring patient privacy is always protected. In addition, the transparency of blockchain allows for immutability of all data access and changes, providing patients with clear information about who has accessed their data and why. Integrated into healthcare, Secure Med not only increases data security, but al so builds trust between patients and doctors. Using a decentralized network ensures data integrity, while smart contracts give patients control over their health information. The transition to patient centric data management heralds a future in which treatment can be effective and safe without compromising patient privacy.

2. PROBLEM STATEMENT :-

With the rapid reform of healthcare, digitization of medical records has become more widespread. However, the transition to digital systems also brings significant challenges, especially in terms of patient privacy and security of health information. The routine process of managing patient information often leads to data breaches, inefficient data sharing, and lack of access, all of which hinder the impact on patient privacy and quality of care. Med leverages the power of blockchain technology to create a transparent and highly secure way to manage patient information. By leveraging decentralized, tamper-proof data, Security Med aims to ensure that medical information is both confidential and easily accessible to authorized users, helping to increase patient trust and facilitate treatment. competition. Key issues include the need for extensive resource development to familiarize healthcare professionals with blockchain technology, integration with existing legacy systems, and ensuring consistency with existing medical records. Overcoming these challenges is critical to the successful adoption and transformation of true patient data management in healthcare, but significant barriers to implementation remain, including capacity building, interaction with existing systems, and compatibility.

3. OBJECTIVES:-

The use of blockchain technology in healthcare can improve the management and security of patient information. By using blockchain, information security can be increased, and patient information can be proven and stored correctly. This allows for the secure sharing of information between doctors that is necessary for consistent and effective patient care. Smart cards manage your personal health information. These smart cards increase privacy and support by allowing patients to control access to their sensitive information. This approach also improves the flow of information between hospitals, improving collaboration by providing open and secure information exchange. New and accurate information needed to coordinate treatment plans. The system provides transparent access to patient information on the blockchain, reducing the risk of unauthorized access by ensuring that only authorized sources can access the information. Management provides tamper-proofing, ensuring that data is not altered and returned to its original source. The system not only improves data integrity, but also increases trust between patients and doctors through safe and secure access to important medical information.

4. LITERATURE SURVEY:-

Wan Song (B), Lu Yuliang, Yan Xuehu, Wan Mengpier, and Liu Hanlin Developed strategy for correcting QR code errors This paper examines two strategies for inputting the square meter of QR code. Two different methods are presented for different situations. The main plan is to modify the unlimited space, the preparation of messages in QR codes, and the QR code error correction technology, which can reach the maximum number of errors, and the QR code change when scanning the QR code reader. The second embedding method involves modifying each column in the password area one by one, and it needs to be decoded correctly. Although the second embedding method cannot achieve high performance, it is used in many cases where the first embedding method is not possible. In order to support the analysis of the two proposed common ideas and error correction, we like to write down all the rules of QR code data entry. Potential research. In this paper, a new information processing capability model based on error correcting codes (EEC) is proposed.

The theoretical derivation and response of the ideal case (successful error correction problem) and the negative case (unsuccessful error correction problem) are given, supporting the relationship between them. Review and description of most of the EEC-based data processing algorithms, including their analysis. AET-based information on education. Visual Cryptography (VC) is a powerful technique that combines the concepts of best understanding and secret sharing through cryptography with image generation. VC uses a binary image (secret) and divides it into 2 or more shares, called shares. The key is returned when the stock frame images are overwritten and superimposed on the transparency. Since no laptop is required to participate, there is one of each VC option. VC can be a special machine because the encrypted message is decrypted directly by the Human Sensory System (HVS). In this survey, we will touch on the latest developments in the cryptocurrency field since 1994, highlight the most analyzed concepts in this field, and describe the problems and solutions.

[3] Z. Wang, G. R. Arce, and G. Di Crescenzo, Halftone visual cryptography with error propagation. Halftone Visual Cryptography (HVC) expands the field of visual cryptography by adding advanced technology. Especially in the hidden view sharing scheme, the hidden image is coded as halftone sharing to obtain rich visual information. In this paper, the HVC construction strategy supports the square error diffusion measure of the plan. The main image is simultaneously divided into binary value shares, and these shares measure half of the diffusion error square, , which is the most important power of the halftoning algorithm. The hidden images are reconstructed by stacking appropriate shares without being affected by the shared images. Factors affecting the image quality and contrast between defined images. Simulation results show several examples.

[4] Xie Na, b, c, Liu Dengzhi Shen Jun, Liu Qi, c, Sun Xingming Secure cloud-supported urban data sharing. In this paper, they propose a framework for urban data sharing using behaviorbased cryptography. We like to extend our content to encourage good deeds so that it is suitable for use in major cities in the world. Especially according to performance analysis, our concept is secure and resistant to attacks. Additionally, experimental and comparative results show that our concept is more economical.

5. PROPOSED SYSTEM :-

The architecture represents a secure medical management system based on blockchain technology. The aim of the system is to store, manage and analyze medical information openly and without evidence, as well as to make it easy and secure f or authorized users such as doctors, nurses, patients and administrators.

Patients and administrators: These are the main personnel involved in the system. Each partner has a specific role, such as accessing patient information, updating medical records or managing administrative tasks.

Data Source: This is the main data where all medical data, us er details and other sensitive data are stored. It contains important information such as patient history, treatment, diagnosis.

Blockchain Integration: Blockchain ensures data integrity by making data immutable and secure. When new information is created or updated (like a patient's medical record), it is signed, verified, and added to the blockchain as a new block. Blockchain adds a layer of transparency and security because once data is recorded, it cannot be altered or tampered with, thus establishing trust between parties.

Signing and Verification: Any new information goes through a digital signature and verification process before it is added to the blockchain. o This ensures that only authorized stake holders (like doctors) can change the patient's access data. Smart Cards: o Provide smart cards to all users (such as patients or staff). A smart card contains user information such as name, medical history, or related medical information. o This card has a secure chip that stores information and can be used to enter or update information into the system.

QR Code Generation: The system generates a QR code that can be scanned by the device to quickly retrieve or verify user information. For example, patients who come to the ho spital can scan the QR code to quickly access their medical records with their doctors, reducing paperwork and data entry.

How the system works: When patients interact with doctors, doctors can access their information via a central card or smart card on the blockchain. It makes patient health data immutable and supports collaboration with greater transparency.

High level of collaboration: Blockchain enables seamless and secure data sharing and tracking throughout the process. It allows healthcare professionals to communicate and collaborate bet ter. It also protects patient privacy and consent.

Simplified Trials: A blockchain powered system can securely record trial data to streamline the process. It supports audits and increases transparency while ensuring the confidentiality of patient information. A simple clinical trial can also better protect the patient's identity Improving Medical Equipment: - Blockchain solutions help manufacturers assist pharmaceutical and healthcare providers with supply chain management. The system provides end-to end traceability of drugs and surgical supplies to reduce the risk of counterfeit drugs.

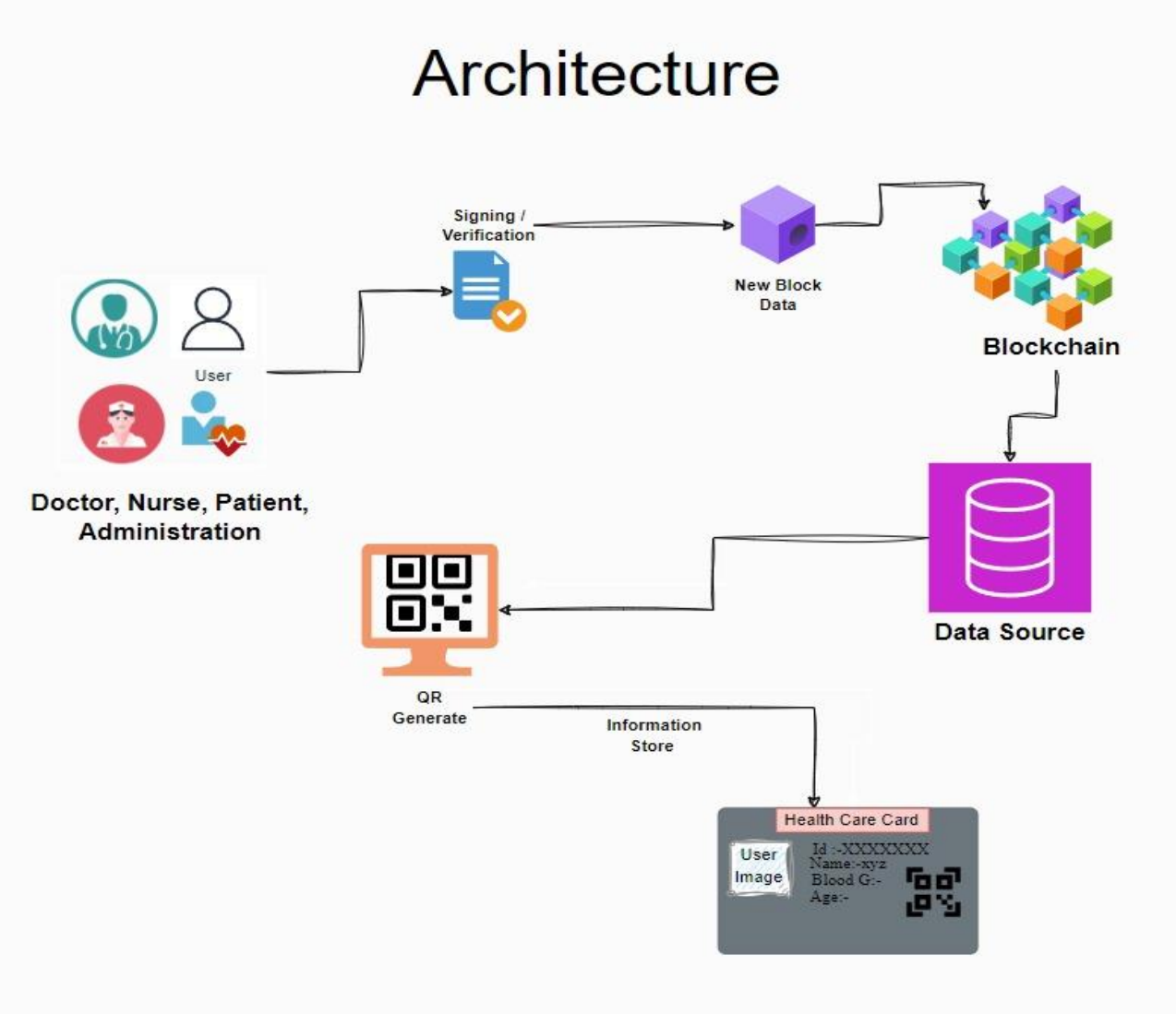
Data Security: This technology offers the best and most powerful options when it comes to patient data security and authentication. This secure patient information ensures data integrity by preventing unauthorized access or

tampering.

Fraud Detection: This technology provides users with a transparent and irreversible way to search for online transactions. It can save organizations a lot of money by helping pre vent healthcare fraud such as insurance fraud and identity fraud.

Advantages: Security and trust: Blockchain ensures that medical information cannot be tampered with and can only be changed by authorized personnel. burden.

Transparency: Blockchain allows all stakeholders to verify information, ensuring everyone has access to accurate and up to-date information.



6. RESULT:-

Enhanced data security: With the use of blockchain technology, all medical information and sensitive medical data are securely encrypted and stored in an integrated system. This advanced security system ensures patient confidentiality by reducing the risk of unauthorized access, tampering or data deletion. The decentralized structure of blockchain protects the system against cyberattacks and vulnerabilities found in central databases, ensuring that there is no failure.

This feature ensures that once a file is saved, it cannot be changed or deleted without leaving a trace. This ensures the integrity of medical information and increases the trust of all parties involved (patients, doctors and administrators). With proven, irreplaceable information, doctors can confidently make important decisions based on accurate, up-to date information and reduce the risks associated with information or errors. The integration of QR codes allows doctors to instantly store or update patient information with a simple scan. This seamless process streamlines work flow, reduces time spent on manual documentation, and minimizes human error.

So doctors can make timely decisions that will improve patient care while increasing the overall effectiveness of treatment. Manage your personal medical records. This empowerment allows people to easily share their medical history with doctors when needed, without the nee d for medical records. Patients gain autonomy over their health information, improving their ability to make informed medical choices while maintaining privacy. Essentially, reduce administrative burden. Eliminates data duplication, prevent s errors related to data collection, and speeds up data retrieval and identification of patient data. This automation not only saves time, but also optimizes resources, resulting in cost savings and easy healthcare management.

7. CONCLUSION:-

Blockchain greatly improves Medicare's healthcare system by improving security, data integrity, and transparency. Tools like Block.js and Blockchain.js can protect sensitive medical information. Once patient information is entered, it cannot be changed without pro per authorization to ensure accuracy. This increases t rust between the patient and the doctor because medical history is protected from unauthorized changes. Blockchain also increases transparency by recording al l updates, making them easier to verify and audit. Doctors can access information in real time to make mor e informed decisions and reduce the risk of errors. Patients have more control over their information, allowing them to control access rights. Blockchain can make healthcare more secure and patient centered by addressing risks such as data breaches, fraud, and privacy violations.

8. FUTURE SCOPE:-

Patient data will be protected with encryption technology very sad Unauthorized access will be prevented. Hospitals and clinics can provide secure patient information. Privacy policy will be strictly followed to ensure data protection Patients will have more control over who can access their medical records. Doctors will take care of the patient's health immediately. This helps in detecting health issues at an early stage and providing rapid intervention. Early diagnosis can improve treatment outcomes. Automation can simplify the management of tasks such as billing, scheduling, and insurance. This will reduce human error and save time. Doctors can provide personalized care bas ed on individual needs. Patients can choose to share only the necessary information, thus maintaining confidentiality while receiving the best possible care. This is especially beneficial for travelers or immigrants.

International collaboration between health researchers will be easier as patient information can be shared securely across borde. It will be valuable to manage many hospitals and medical centers while remaining affordable. Telemedicine will be fully implemented, enabling consultations in remote areas without compromising patient safety. Blockchain will play a significant role in reducing fraud by correcting the truth. Insurance com patient approve treatments based solely on medical record. Important information can be provided instantly, even without communication. This can lead to faster decisions and better patient care.

9. REFERENCES:-

1.Privacy-Preserving Medical Data Sharing Scheme Based on Two-Party Cloud-Assisted PSI (IEEE INTERNET OF THINGS JOURNAL, VOL. 11, NO. 9, 1 MAY 2024).

2. Analysis and Secure Medical Data Transmission Using Wireless Network with QR Code (© September 2023| IJIRT| Volume 10 Issue 4 | ISSN: 2349-6002.

3.Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives (Received 19 April 2021; Revised 1 May 2021; Accepted 6 May 2021; Published 25 May 2021) https://doi.org/10.1155/2021/7608296.

4. System Level Design of a Secure Healthcare Smart Card System (Proceedings of the 2011 IEEE Systems and Information Engineering Design Symposium, University of Virginia. Charlottesville, VA, USA, April 29, 2011).

5.Design Recommendations for Gate Security Systems and Health Status: A Systematic Review (Received 16 October 2023, accepted 10 November 2023, date of publication 20 November 2023, date of current version 29 November 2023. Digital Object Identifier 10.1109/ACCESS.2023.3335115.

6. Enhancing data privacy in wireless sensor network : investigating techniques and protocols to protect privacy of data transmitted over wireless sensor networks in critical applications of healthcare and national security International Journal of Network Security and Applications (I N S A) Vol.16, No.2, March 2024.

7.A System on E- Health Care Card Using QR Code (5th International Conference on Communication and Information Processing (ICCIP-2023) Available on: SSRN (SSRN is an open-access online preprint community, owned by Elsevier).

8.Implementation of Blockchain Consortium to Prioritize Diabetes Patients' Healthcare in Pandemic Situations (received November 13, 2021, accepted November 23, 2021, date of 9 Enhancing Medical Data Privacy and Security in Wireless Network via Smart Card and QR Code publication December 3, 2021, date of current version December 16, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3132302).