Design A Secure and Efficient Healthcare System Using Blockchain

Mrs.S.KOKILA M.E., Assistant Professor, Department of Computer Science And Engineering,Shree Venkateshwara Hi TechEngineering College, Gobichettipalayam.
Email : kokiyellowever@gmail.com

Ms.K.AKALYA,
Student of
Computer Science And Engineering, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam.
Email : cseakalyak@gmail.com

Ms.B.AATHIRAMOL,
Student of
Computer Science And Engineering,Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam.
Email : aathiramol02@gmail.com

Ms.N.KOWSALYA,
Student of
Computer Science And Engineering, Shree Venkateshwara Hi Tech Engineering College, Gobichettipalayam.
Email: kowsalyanataraj@gmail.com

ABSTRACT

Block chain technology has the potential to completely transform healthcare management systems by enhancing data security, interoperability, and integrity because to its decentralized and unchangeable structure. Sensitive patient information is more difficult for bad actors to breach thanks to the SHA-256 algorithm, which improves data security. Interoperability between diverse healthcare systems is facilitated by smart contracts and standardized data formats. However, issues with user adoption, scalability, and regulatory compliance also face block chain implementation in the healthcare industry. This study offers important insights into the changing environment of healthcare data management by highlighting the possible advantages and challenges of integrating block chain technology in healthcare management systems.Blockchain technology promises to revolutionise traditional management systems by providing unmatched improvements in data security, interoperability, and integrity. This technology is a game-changer for the healthcare sector. Its decentralised and immutable architecture, which radically changes how healthcare data is stored, accessed, and maintained, is at the heart of its capabilities. The strong data security aspects of blockchain, which are mainly made possible by cryptographic hashing algorithms like SHA-256, are one of its main benefits for the healthcare industry. These algorithms greatly lower the risk of data breaches and improve patient privacy by ensuring that patient information is impenetrable and resistant to unauthorised access or change. Additionally, blockchain uses standardised data formats and smart contracts to enable smooth interoperability across different healthcare systems. Smart contracts simplify complicated procedures like supply chain logistics, billing, and patient consent management by automating and enforcing predetermined norms and agreements. Standardised data formats facilitate effective data interchange and collaboration between healthcare providers, insurers, researchers, and other stakeholders by ensuring consistency and compatibility across various platforms.

***Keywords*:** patient monitoring, health, security, EHRs, Block Chain.

1. INTRODUCTION

The use of sensor-based data analytics has become a game-changer in the field of contemporary healthcare, changing patient monitoring in linked healthcare applications.

This paradigm change allows for the real-time gathering and analysis of a variety of patient data, including vital signs and activity levels, by utilizing sophisticated sensor technology. The smooth incorporation of sensors into medical equipment enables an ongoing flow of data, promoting a thorough awareness of a person's health state. This method not only improves patient monitoring's precision and timeliness, but it also gives medical staff members useful information for proactive, individualized actions.

1.1 PATIENT MONITORING

A vital component of modern healthcare is patient monitoring, which is a dynamic and essential method of following and evaluating a person's health. In a time of rapid technological development, patient monitoring has expanded beyond conventional limits to include a wide range of advanced equipment and sensors that continually gather and evaluate critical health data. This attentive observation covers a wide range of physiological parameters, such as blood pressure, oxygen saturation, heart rate, and more, giving medical staff a thorough and up-to-date picture of a patient's health. Continuous patient monitoring has an impact on remote and home-based healthcare in addition to acute care settings. It provides a proactive way to spot possible problems, optimize treatment plans, and eventually promote a more individualized and flexible approach to healthcare delivery.

1.2 HEALTH

A ubiquitous and priceless feature of human existence, health includes people's total physical, mental, and social well-being in addition to the absence of disease. It is a human necessity and a fundamental right that cuts beyond social, cultural, and economic divides. Over time, our knowledge of health has changed, shifting from a solely biological viewpoint to one that takes a more holistic approach and takes into account the complex interactions between social, mental, and physical aspects. The pursuit of health, whether at the individual or societal level, is a dynamic and always changing subject of study and practice because it incorporates many complicated factors, including access to healthcare, the caliber of healthcare services, preventive measures, and the wider determinants of health.

1.3 SECURITY

A vital component of human existence, security is essential to the welfare of people, groups, and society as a whole. It is the guarantee of safety from a plethora of possible dangers and hazards that can interfere with our daily routines. Every aspect of our everyday lives is impacted by security, from the locks on our doors to the encryption on our digital communications. It includes maintaining social order, protecting private information, and ensuring one's physical safety. Security challenges have become more intricate in a more interconnected and dynamic world, requiring a thorough grasp of the constantly changing environment of dangers and the implementation of solutions to mitigate them. This introduction lays the groundwork for a thorough examination of the complex field of security, highlighting the importance of security in our daily lives, the dynamic nature of threats.

1.4 EHRs

EHRs, or electronic health records, have become a major influence in modern healthcare, changing the way that patient data is collected, maintained, and disseminated. They signify a fundamental change from conventional paper-based medical records to digital systems that improve healthcare data accessibility, accuracy, and efficiency. EHRs are intended to be all-inclusive databases that hold a person's test results, treatment plans, medical history, and more, providing medical professionals with a comprehensive picture of a patient's health journey. An overview of the vital role electronic health records (EHRs) play in healthcare is given

in this introduction, which also highlights the importance of EHRs in facilitating interoperability across healthcare systems, enhancing clinical decision-making, and expediting patient treatment.

1.5 BLOCKCHAIN

Blockchain is a distributed ledger technology that makes it possible to record transactions over a network of computers in a safe, transparent, and decentralised manner. Every block in the chain includes a cryptographic hash of the one before it, resulting in an unchangeable and impenetrable record of the contents. Its transparent and decentralised structure makes it perfect for applications like supply chain management, safe data sharing, and financial transactions because it removes the need for middlemen, lowers the danger of fraud, and guarantees the integrity and reliability of transactions.

1.6 PROBLEM STATEMENT

Significant obstacles stand in the way of the growing interest in using clinically validated AI applications to improve healthcare services. These obstacles include the absence of standardised medical records, restricted access to curated datasets, and strict ethical and regulatory requirements protecting patient privacy. The low adoption of AI-based solutions in clinical settings, despite substantial global research, calls for creative data-sharing strategies to facilitate AI integration while protecting patient privacy. Thus, it is imperative to develop privacy-preserving strategies and remove any obstacles preventing AI from being widely used in healthcare. Only then can AI-driven solutions be implemented in practical, ethical, and efficient ways in real-world medical settings.

2. LITERATURE REVIEW

According to what 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 chaintechnology in the healthcare sector were emphasized in this work.

In this paper, 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.

According to VANGELIS MALAMAS [4] et al., 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. RELATED WORK

A growing number of people are interested in utilizing clinically verified applications of artificial intelligence (AI) research to enhance the effectiveness, efficiency, and capacity of healthcare services. Very few AI-based solutions have been effectively introduced into clinics, despite much research being conducted globally. The adoption of clinically verified AI applications in the medical field is hindered by several factors, such as non-standardized medical records, a scarcity of curated datasets, and strict ethical and regulatory constraints to protect patient privacy. In order to build AI-based healthcare applications, it is imperative that new data-sharing techniques be devised in the era of artificial intelligence while maintaining patient privacy. Creating privacy-preserving methods and resolving the obstacles preventing AI deployment in a real healthcare

setting have received a lot of attention in the literature. In order to do this, the report provides an overview of the most recent methods for protecting privacy in AI-based healthcare systems. Leading privacy-preserving methods, such Federated Learning and Hybrid Techniques, are described in detail along with possible privacy threats, security issues, and next steps.

4. METHODOLOGY

The suggested solution seeks to create a safe, effective, and transparent data ecosystem by utilizing block chain technology to transform the healthcare sector. Our suggested Sha-256 methods will produce an unchangeable ledger with strong data security and integrity for patient medical records. Furthermore, the system will make it easier for medications to be tracked from producers to consumers, improving medication safety and lowering counterfeiting. It will also make it possible to store and exchange clinical trial data, which will promote cooperation and quicken medical research. The suggested solution aims to capitalize on the significant advantages of block chain technology in healthcare, while recognizing the obstacles related to acceptance, regulation, and technology. In the end, this will enhance patient care, data management, and industry efficiency.

A. Patient Block Chain Record

Patients ought to have command over who can get to their wellbeing data. They ought to have the option to concede or disavow admittance to their information, and have the option to follow who has gotten to it. Block chain's permanence highlight guarantees that once a patient's wellbeing data has been recorded on the block chain, it can't be messed with or erased. This is fundamental for keeping up with the honesty of patient wellbeing data. To guarantee that medical services suppliers can undoubtedly get to patient data across various frameworks and organizations, the Patient block chain record module ought to Be interoperable with other medical care frameworks.

B. Doctor Block Chain Record

Likewise, with the patient block chain record module, block chain’s changelessness highlight guarantees that once a specialist's data has been recorded on the block chain, it can't be altered or erased. This is fundamental for keeping up with the honesty of specialist explicit data. The specialist block chain record module could give a way to medical care associations to check a specialist's subtleties. The module ought to be intended to guarantee the protection and security of specialist explicit data, while likewise permitting approved gatherings to get to it on a case by case basis. The specialist block chain record module ought to be interoperable with other medical care frameworks and organizations to guarantee consistent access and sharing of data.

C. Key Generation

Key age alludes to the most common way of making a couple of cryptographic keys for use in encryption and decoding. In broad daylight key cryptography, which is regularly utilized in block chain innovation, the key pair comprises of a public key and a confidential key. The confidential key is created by choosing an irregular number that meets specific measures characterized by the cryptographic calculation. The confidential key is kept mystery and ought to never be shared.

D. Uploaded Ehr

Key age alludes to the most common way of making a couple of cryptographic keys for use in encryption and decoding. In broad daylight key cryptography, which is regularly utilized in block chain innovation, the key pair comprises of a public key and a confidential key. The confidential key is created by choosing an irregular number that meets specific measures characterized by the cryptographic calculation. The confidential key is kept mystery and ought

to never be shared. Both general society and confidential keys ought to be shielded from unapproved access or use, as they are basic for secure correspondence and encryption.

E. Sha 256 Encryption and Hash Generation

SHA-256 (Secure Hash Algorithm 256-bit) is a widely used cryptographic hash function that generates a 256-bit (32-byte) hash value. It is commonly used in block chain technology and other cryptographic applications to provide a secure way to verify data integrity. The message is padded with additional bits to ensure that the message has a fixed length that can be processed by the SHA-256 algorithm. The first step is to input the message that needs to be hashed, which can be any data, such as text, numbers, or binary data. The hash value can be used to verify the integrity of the original message, as any change to the message will result in a different hash value.SHA-256 is a one-way function, meaning that it is computationally infeasible to determine the original message from the hash value. This makes it a secure way to protect sensitive information.

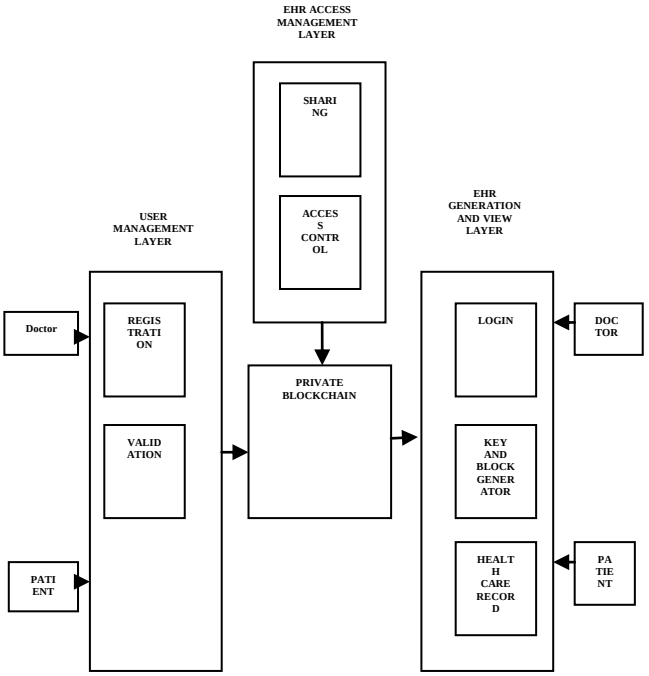

Figure 1.Block diagram

5. ALGORITHM DETAILS

A. Sha256 Hashing Algorithm

SHA 256 algorithm (sometimes called digest) is a kind of signature for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. A hash is not' encryption'–it cannot be decrypted back to the original text (it is a cryptographic' one-way' feature, and is a fixed size for any source text size). This makes it ideal when comparing' hashed' versions of texts, rather than decrypting the text to obtain the original version

Basic Initialization will be done for 8 items

Step 1: Information is an array 8 things in length where everything is 32 bits.

Step 2: out is an array 8 things in length where everything is 32 bit.

Step: 3 Compute all the capacity boxes and store those qualities. Allude to them by work name

Step: 4 Store input, right moved by 32 bits, into out. Now, in the out exhibit, E is an inappropriate worth and A is unfilled

Step: 5 Store the capacity boxes. Presently we have to compute out E and out A. note: Supplant the modulo orders with a bitwise AND 2^(32-1)

Step: 6 Store (Input I + CH + ((XT+YT) AND 2^31)) AND 2^31 As Mod1

Step: 7 Store (Sum1 + Mod1) AND 2^31 as Mod2

Step: 8 Store (b + Mod2) AND 2^31 into out E Presently Out E is right and all we need is out A

Step: 9 Store (NA + Mod2) AND 2^31 as Mod3

Step: 10 Store (Sum0 + Mod3) AND 2^31 into output A

6. RESULT ANALYSIS

algorithm	accuracy
existing	75
proposed	88

Table 1. Comparison Table

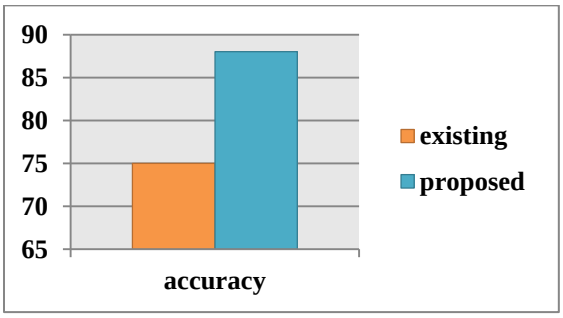

Figure 2. Comparison graph

The table shows an algorithm accuracy comparison between a suggested system that shows an enhanced accuracy of 88% and an existing system that reaches a level of 75%. The phrase "algorithm accuracy" describes how well and precisely the algorithms used in these systems produce accurate results or forecasts. The 75% accuracy in the context of the current system indicates a reasonable level of operational dependability. However, with an accuracy rate of 88%, the suggested system shows a significant increase, suggesting a greater level of accuracy and efficacy in its algorithmic operations. This progress indicates that the suggested algorithmic method may surpass the current one, demonstrating a notable improvement in the system's capability to provide precise outcomes. This comparison highlights the advantages of using the suggested approach since it shows a higher degree of accuracy, which may be especially important in situations where accuracy and precision are critical. When assessing the overall efficacy and viability of applying the suggested method in real-world circumstances, it's crucial to take additional aspects like scalability, resource needs, and real-world applicability into account.

7. CONCLUSION

To sum up, block chain consensus algorithms are an innovative and game-changing tool for the healthcare industry. These algorithms enable more secure and transparent collaboration between healthcare practitioners, patients, and researchers by guaranteeing data security, integrity, and interoperability. The implementation of block chain technology in the healthcare industry has the potential to improve patient outcomes, decrease administrative inefficiencies, and stimulate ground-breaking research, whether via Proof of Work, Proof of Stake, or other novel consensus mechanisms. Block chain technology and its consensus algorithms will become more and more important in influencing the future of healthcare as the sector embraces digitization and data-driven decision-making. This will eventually result in better, safer, and more effective healthcare delivery systems.

REFERENCES

1. "Blockchain technology in the healthcare industry: Trends and opportunities," by H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman Art. no. 100217, J. Ind. Inf. Integr., vol. 22, June 2021.

2. "Combination of hiding and encryption for data security," I. Aljazaery, H. T. S. Alrikabi, and M. R. Aziz, Int. J. Interact. Mobile Technol., vol. 14, pp. 34–47, Jan. 2020.

3. "BlockHR: A blockchain-based framework for health records management," by L. Ismail and H. Materwala, in Proceedings of the 12th International Conference on Computer Modeling and Simulation, June 2020.

4. "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.

5. "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.

6."Adecentralized 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.

7. T Senthil Prakash, V CP, RB Dhumale, A Kiran., "Auto-metric graph neural network for paddy leaf disease classification" - Archives of Phytopathology and Plant Protection, 2023.

8. T Senthil Prakash, G Kannan, S Prabhakaran., "Deep convolutional spiking neural network fostered automatic detection and classification of breast cancer from mammography images",2023.

9. TS Prakash, SP Patnayakuni, S Shibu., "Municipal Solid Waste Prediction using Tree Hierarchical Deep Convolutional Neural Network Optimized with Balancing Composite Motion Optimization Algorithm" - Journal of Experimental & Theoretical Artificial …, 2023

10. TS Prakash, AS Kumar, CRB Durai, S Ashok., "Enhanced Elman spike Neural network optimized with flamingo search optimization algorithm espoused lung cancer classification from CT images" - Biomedical Signal Processing and Control, 2023.

11. R. Senthilkumar, B. G. Geetha, (2020), Asymmetric Key Blum-Goldwasser Cryptography for Cloud Services Communication Security, Journal of Internet Technology, vol. 21, no. 4 , pp. 929-939.

12. Senthilkumar, R., et al. "Pearson Hashing B-Tree With Self Adaptive Random Key Elgamal Cryptography For Secured Data Storage And Communication In Cloud." Webology 18.5 (2021): 4481-4497