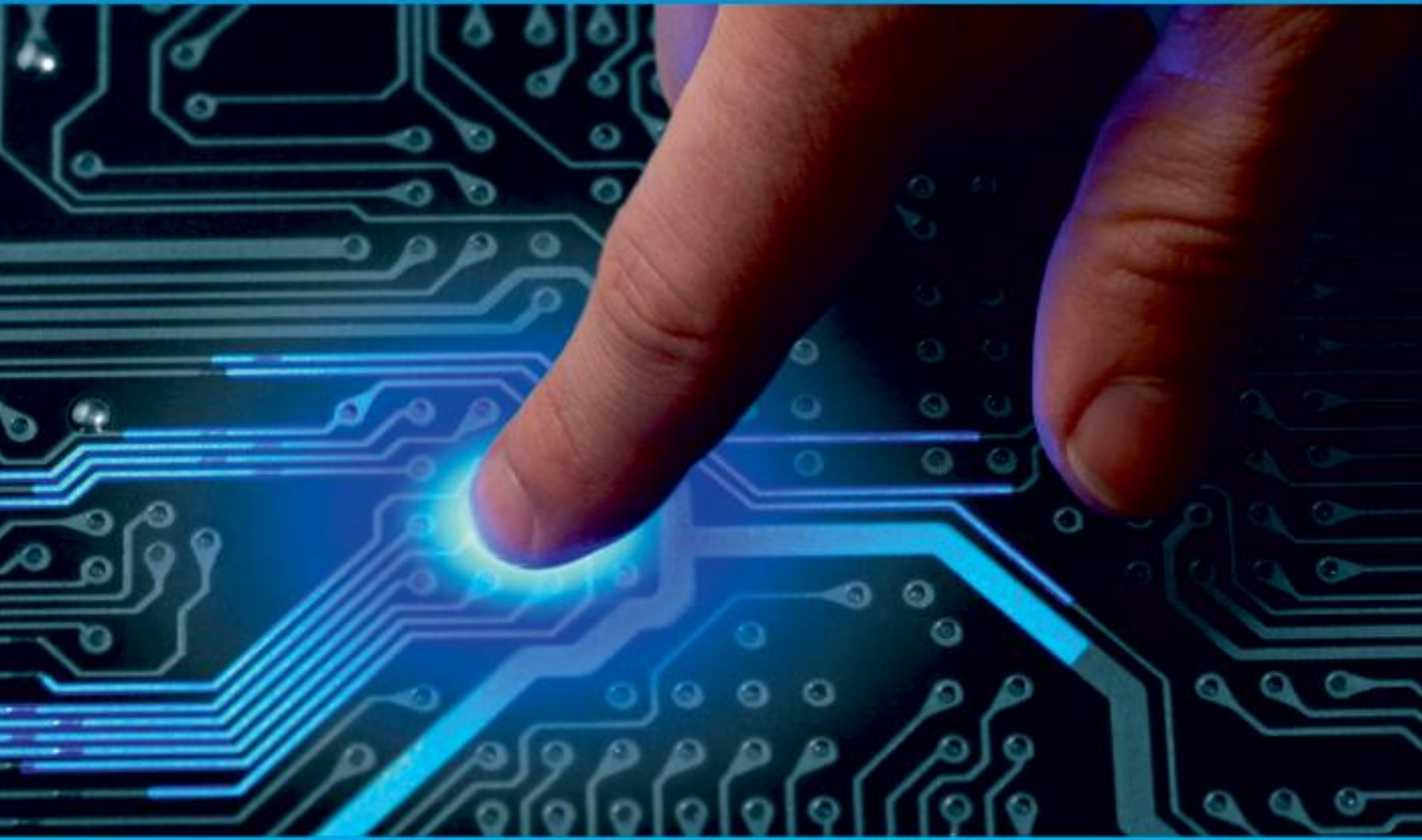
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1205165 |

Data Privacy Protection using Secure Hash Algorithm – 256 in BlockChain

Arunraj S, Arshad Ahamad J, Gowsick R, Sathish Kumar T

Department of Information Technology, K.S. R College of Engineering, Tiruchengode, India

Department of Information Technology, K.S. R College of Engineering, Tiruchengode, India

Department of Information Technology, K.S. R College of Engineering, Tiruchengode, India

Assistant Professor, Department of Information Technology, K. S. R College of Engineering, Tiruchengode, India

ABSTRACT: Block chain technology's decentralised and immutable nature gives it the opportunity to dramatically improve healthcare management systems by improving data security, interoperability, and integrity. Data security is enhanced with the SHA-256 algorithm, which makes it harder for malicious actors to access sensitive patient information. Standardised data formats and smart contracts enable interoperability amongst disparate healthcare systems. However, block chain implementation in the healthcare sector also faces challenges related to user uptake, scalability, and regulatory compliance. This research highlights the possible advantages and difficulties of incorporating block chain technology into healthcare management systems, providing significant new insights into the dynamic landscape of healthcare data management.

KEYWORDS: patient monitoring, health, security, EHRs, Block Chain

I. INTRODUCTION

The integration of sensor-based data analytics has revolutionized contemporary healthcare by enabling real-time gathering the review and analysis of patient data., including vital signs and activity levels. This paradigm shift improves the precision and timeliness of patient monitoring, empowering medical staff with actionable insights for proactive, individualized actions.

Patient monitoring has evolved beyond conventional limits, incorporating advanced equipment and sensors to continually gather and evaluate critical health data. This comprehensive observation covers various physiological parameters, facilitating a thorough understanding of patients' health states and enabling proactive interventions across diverse healthcare settings.

Health, as a fundamental human necessity, encompasses the holistic well-being of individuals and transcends social, cultural, and economic divides. This dynamic pursuit involves complex interactions between biological, social, mental, and physical aspects, influencing healthcare access, service quality, preventive measures, and broader determinants of health.

Security is paramount to the welfare of individuals and society, guaranteeing safety from various dangers and hazards. In an interconnected world, addressing security challenges requires a nuanced understanding of evolving threats and the implementation of effective solutions to mitigate risks, emphasizing the importance of security in daily life.

Electronic Health Records (EHRs) have transformed patient data management, transitioning from paper-based records to digital systems. EHRs enhance data accessibility, accuracy, and efficiency, providing comprehensive insights into patients' health journeys and supporting clinical decision-making and interoperability among healthcare systems.

In conclusion, blockchain consensus algorithms offer a cutting-edge solution for enhancing confidentiality, integrity, and interoperability in the medical field. By ensuring transparent and secure collaboration between stakeholders, blockchain technology has the potential to improve patient outcomes, reduce administrative inefficiencies, and drive groundbreaking research in healthcare. Embracing digitization and data-driven decision-making, the future of healthcare will be shaped by blockchain technology, paving the way for better, safer, and more efficient healthcare delivery systems.

II. RELATED WORKS

[1] According to a study by Hassan Mansur et al., the healthcare business is likely to be significantly impacted by the notable rise in the application of blockchain technology in healthcare. This study evaluated past efforts to bridge the blockchain's technological gap with the healthcare industry. A bibliometric analysis was conducted to determine the trend of block chain technology in healthcare by examining the distribution of datasets, venues, keywords, and citations. The security and privacy of case studies involving medical information systems for telemedicine and e-health were also examined. This study examined a broad array of prospective future difficulties, including standards, block chain size, universal interoperability, scalability, and storage capacity. The advantages of applying blockchain technology to the healthcare sector were emphasised in this work.

[2] Ibtisam et al have suggested in this paper One information security technique is the concealment strategy, in which data is hidden and stored in a different information medium to prevent detection during two-way communication. This research proposed an algorithm for data hiding and encryption using multiple techniques to safeguard data from hackers and detection. A wavelet transformer was used to change the shape of a wave of information (one- and two-dimensional data) as well as its numerous mathematical formulas. Two data sets were utilised: the first was used in a clandestine manner. The second group was considered as an embedding and encryption technique. The second group's high-value features are extracted and removed from the mother's information wave, bringing the data down to a level appropriate for the modulation procedure.

[3] Leila Ismail and others, As this system has indicated, hospitals are increasingly using Electronic Health Records (EHRs) to process and preserve patient data. When these records are exchanged, the current healthcare system operates more efficiently and accurately. EHRs are currently stored on client-server architectures, which allow hospitals or cloud service providers to retain patient data stewardship. Additionally, patient records are distributed among multiple hospitals using heterogeneous databases. Patients thus find it difficult to piece together a coherent picture of their medical history, making it difficult for them to focus on the details of their treatment. The security features and replication mechanism of the block chain, which provide resolutions for the intricacies, confidentiality, integrity, interoperability, and privacy concerns within the client-server architecture-based EHR management system, portend great things for the healthcare sector.

[4] A multitude of interrelated parties are involved in the health care ecosystem, each with different as well as occasionally conflicting security and privacy concerns, according to VANGELIS MALAMAS et al. Sharing medical data that is occasionally generated by distant medical equipment might be challenging. Finding a solution that strikes a balance between functional requirements like interoperability and scalability and security and privacy requirements like data privacy and fine-tuned access control is a challenging task, even though there are many solutions in the literature that address these requirements. While centralised cloud architectures provide interoperability and scalability, they are very trust-dependent. On the other hand, decentralised block chain-based solutions typically provide independent data privacy and trust management, but they usually lack support for dynamic alterations in the foundational trust realms. To meet this demand, we provide in this research a novel hierarchical multi expressive block chain architecture. High-level collaboration between independently operated trust authorities is made possible by a proxy block chain. Hospitals and device manufacturers, among other end users from the health care domain, can securely access and exchange medical data if a generally recognised domain-wise access policy is adhered to.

[5] Hsiu-An Lee and others , In this system, traditional clinics have traditionally offered medical care with a focus on illness treatment. However, there is a widening gap between the services that clinics offer and what their patients genuinely need as the world's population ages. This suggests that clinics might not have the resources available to offer patients the whole range of care, which could result in needless medical harm. The National Institute for Health and Care Excellence emphasised the importance of using patient-centered decision-making strategies for a variety of conditions, with a focus on precision medicine, in its 2016 Multi morbidity Clinical Assessment and Management Guidelines Report. Precision medicine is an method for disease prevention and treatment that considers the individual genetic, environmental, and lifestyle-related differences of each patient. With the use of this data, customised care plans and dynamic modifications are identified as being necessary for both clinical and preventative healthcare. The main elements precision medicine involves the sharing of medical information, daily vital sign data, personal health management, and historical disease data.

III. EXISTING SYSTEM

The potential to improve the efficacy, capacity, and efficiency of healthcare services through clinically validated applications of artificial intelligence (AI) research is attracting increasing attention. Despite extensive worldwide research, very few AI-based solutions have been successfully implemented in clinics. The medical industry faces various obstacles to the adoption of clinically verified AI applications, including non-standardized medical records, a lack of curated datasets, and stringent ethical and legal obligations to safeguard patient privacy. It is essential to develop new patient privacy-preserving data-sharing strategies amidst the era of artificial intelligence in order to develop AI-based healthcare apps. The literature has focused heavily on creating techniques that preserve privacy and removing the barriers to AI use in an actual healthcare context. The paper offers a summary of the most recent techniques for maintaining privacy in AI-based healthcare systems in order to achieve this. Prominent techniques for protecting privacy, like Federated Learning and Hybrid Techniques, are thoroughly explained along with potential privacy risks, security concerns, and future actions.

IV. PROPOSED SYSTEM

The proposed approach uses block chain technology to revolutionise the healthcare industry by establishing a transparent, safe, and efficient data environment. For patient medical records, our recommended Sha-256 techniques will result in an immutable ledger with robust data security and integrity. In addition, the system will facilitate the tracking of pharmaceuticals from manufacturers to end users, enhancing medicine security and reducing counterfeiting. Additionally, it will enable the sharing and storing of clinical trial data, fostering collaboration and accelerating medical research. The proposed approach acknowledges the challenges associated with adoption, regulation, and technology, while attempting to use the noteworthy benefits of Blockchain technology within the healthcare sector. Ultimately, this will improve industrial efficiency, patient care, and data management.

V. SYSTEM DESIGN

A. Patient Block Chain Record

Patients should be in control of who possesses access to their health information. They should be able to track who has access to their information and choose to accept or reject entry to it. The permanence feature of the block chain ensures that once patient health information is stored there, it cannot be altered or removed. Maintaining the integrity of patient wellness data requires this. The Patient Block Chain Record Module should be compatible with other medical care frameworks to ensure that providers of medical services can obtain patient data across multiple frameworks and organisations.

B. Doctor Block Chain Record

Similarly, the changelessness feature of the block chain ensures that, once a specialist's data is stored on the block chain, it cannot be changed or removed when used with the patient block chain record module. Maintaining the integrity of specialised explicit data requires this. The medical care associations may be able to verify a specialist's subtleties with the use of the specialist block chain record module. The module should be designed to ensure expert explicit data security and protection, while also granting authorised parties case-by-case access to it. To ensure consistent data access and sharing, the specialised block chain record module should be compatible with different healthcare frameworks and organisations.

C. Key Generation

Key age refers to the most widely used technique for generating a pair of cryptographic keys that are needed for decryption and encryption. Widely used in block chain innovation, broad daylight key cryptography uses a key pair consisting of a public key and a secret key. By selecting an irregular number that satisfies the requirements defined by the cryptographic computation, the confidential key is generated. The secret key is kept under wraps and should never be disclosed.

D. Uploaded EHR

Key age refers to the most commonly utilized technique for generating a pair of cryptographic keys that are needed for decryption and encryption. Widely used in block chain innovation, broad daylight key cryptography uses a key pair consisting of a public key and a secret key. By selecting an irregular number that satisfies the requirements defined by the cryptographic computation, the confidential key is generated. The secret key is kept under wraps and should never be disclosed. Since Public and private cryptographic keys are essential for encrypted communication and security, they should be protected from unauthorised use and access.

E. Sha 256 Encryption and Hash Generation

A popular cryptographic hash function called SHA-256 (Secure Hash Algorithm 256-bit) produces a 256-bit hash value (equivalent to 32 bytes). It is frequently utilised to offer a safe means of confirming data integrity in block chain technology and other cryptographic applications. To guarantee that the message has a set length that the SHA-256 algorithm can execute, the message is padded with extra bits. The message that has to be hashed must first be entered. This message can be any type of data, including text, numbers, or binary data. Since a hash value is modified whenever a message is altered, it can be used to confirm the original message's integrity. Since SHA-256 is a one-way algorithm, extracting the original message derived from the hash value is not computationally viable.

F. SHA 256 Hashing Algorithm

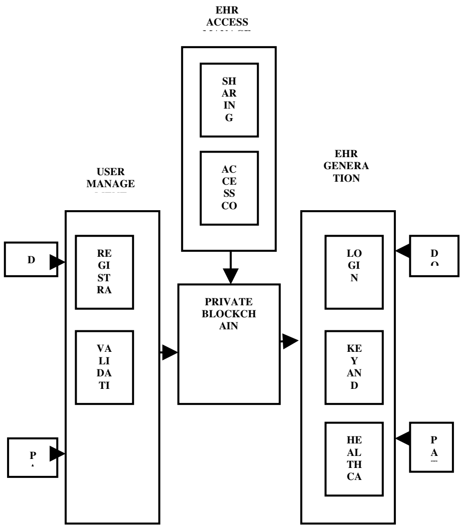


Figure 1. Block diagram

A text or data file can be signed using the SHA 256 algorithm, often known as a digest. A text can be signed with a nearly unique 256-bit (32-byte) signature using SHA-256. A hash is a cryptographic "one-way" characteristic that has a fixed size for all source text sizes; unlike "encryption," it cannot be decoded back to the original text. Because of this, it's perfect for comparing "hashed" copies of texts instead of decrypting them to get 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 the input, shifted right by 32 bits, into the output. Presently, within the output display, 'E' holds an improper value and 'A' remains empty.
Step 5: Store the capacity boxes. Presently, we need to calculate out E and out A. Note: Replace the modulo instructions with a bitwise AND of 2 raised to the power of (32-1).
Step 6: Store the result of (Input I + CH + ((XT + YT) AND 2^31)) bitwise AND 2^31 as Mod1.
Step 7: Store the result of (Sum1 + Mod1) bitwise 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 the result of (Sum0 + Mod3) bitwise AND 2^31 into output A.

G. Result Analysis
Inputs for Edge Computing

Inputs for Secure Hash Algorithm -256

S.NO	ACCURACY	PRECISION	RECALL
1	0.88	0.78	0.68
2	0.91	0.82	0.72
3	0.87	0.79	0.69
4	0.89	0.81	0.71
5	0.86	0.77	0.67

S.NO	ACCURACY	PRECISION	RECALL
1	0.65	0.55	0.75
2	0.72	0.61	0.82
3	0.68	0.58	0.78
4	0.71	0.63	0.80
5	0.69	0.57	0.77

Comparison of Evaluation Metrices

METRIC	Edge Computing	SHA - 256
Accuracy	0.69	0.882
Precision	0.588	0.794
Recall	0.784	0.694

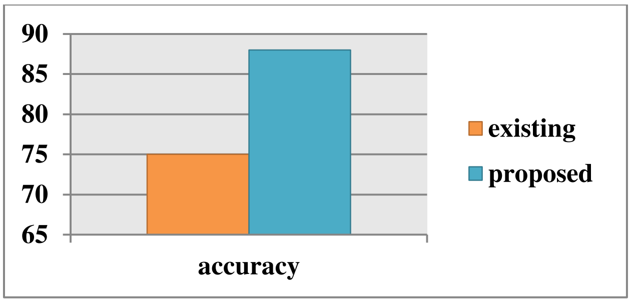


Figure 2 : Comparison Graph

A comparison of algorithm accuracy is presented in the table between a current system that achieves a level of 75% and a suggested system that demonstrates an enhanced accuracy of 88%. The term "algorithm accuracy" refers to the degree to which these systems' algorithms generate precise and accurate forecasts or results. Given the current technology, the accuracy of 75% suggests a respectable level of operational reliability. Nonetheless, the proposed system exhibits a notable improvement, indicating a higher degree of precision and effectiveness in its algorithmic functions, with an accuracy rate of 88%. This development suggests that the proposed algorithmic approach could outperform the existing one, exhibiting a significant enhancement in the system's ability to yield accurate results. Since the comparison demonstrates a better degree of accuracy—which may be particularly significant in circumstances where accuracy and precision are crucial—it highlights the benefits of utilising the recommended approach. Scalability, resource requirements, and practicality should all be considered when evaluating the overall effectiveness and feasibility of implementing the recommended approach in actual situations.

VI. CONCLUSION

In conclusion, block chain consensus algorithms represent a cutting-edge and revolutionary instrument for the medical field. These algorithms ensure data confidentiality, integrity, and interoperability, facilitating more transparent and safe collaboration between researchers, patients, and healthcare professionals. Whether through Proof of Work, Proof of Stake, or other cutting-edge consensus techniques, the application of blockchain technology in the healthcare sector has unlocking the possibilities to enhance patient outcomes, reduce administrative inefficiencies, and foster ground breaking research. The future of healthcare will be increasingly shaped by blockchain technology and consensus algorithms as the industry embraces digitization and data-driven decision-making. Better, safer, and more efficient healthcare delivery systems will eventually come from this.

VII. FUTURE WORK

The focus of future research on the use of blockchain consensus algorithms in healthcare should be on finding solutions for scalability and regulatory compliance problems. To manage the growing volume of medical data, sharing and second-layer protocol scalability solutions must be implemented and improved. Additionally, it is imperative that legislators, regulatory bodies, and corporate stakeholders collaborate to establish a framework that ensures compliance with data protection laws and promotes the widespread application of blockchain technology in the healthcare industry. Furthermore, continuous research into the development of consensus algorithms suited to the particular needs of clinical trials, telemedicine, and patient records is necessary to maintain the highest levels of efficiency and security.

REFERENCES

1. H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," J. Ind. Inf. Integr., vol. 22, June 2021, Art. no. 100217.
2. "Combination of encryption and hiding 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. Ding, Yuanming, Wei Kang, Jianxin Feng, Bo Peng, and Anna Yang. 2023. “Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network.” IEEE Access: Practical Innovations, Open Solutions 11: 83680–91.
3. According to L. Ismail and H. Materwala, "BlockHR: A blockchain-based framework for health records management," will be presented at the 12th International Conference on Computer Modelling and Simulation in June 2020, with pages 164–168.
4. V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, "A hierarchical multi blockchain for fine grained access to medical data," IEEE Access, issue 8, 2020, pages 134393–134412.
5. . H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu wrote "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.
6. By M. Marwan, A. A. Temghart, F. Sifou, and F. AlShahwan, "A decentralised blockchain-based architecture for a secure cloud-enabled IoT," Nov. 2020; J. Mobile Multimedia, vol. 2020; pp. 389–412.
7. An energy blockchain-based safe charging technique for electric cars with intelligent communities N. Zhang, Z. Su, Y. Wang, Q. Xu, M. Fei, and Y.-C. Tian IEEE Internet Things Journal, volume 6, issue 3, pages 4601–4613, June 2019.
8. Huang, X. Ma, and S. Zhang, "Performance analysis of the raft consensus algorithm for private blockchains," Jan 2020; vol. 50, no. 1, pp. 172-181, IEEE Transactions on Systems, Man, Cybern., Syst.
9. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," Pages 43620–43652, IEEE Access, volume 9, 2021.
10. "Digital health in physicians' and chemists' offices: A comparative study of e-prescription systems' architecture and digital security in eight countries," written by Aldughayfiq and Sampalli OMICS, J. Integrative Biol., vol. 25, no. 2, pp. 102–122, February 2021.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details