IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 5, October, 2024, pp. 2279-2286
Journal homepage: http://iieta.org/journals/ts

A Novel IoT-Blockchain Methodology to Augment Conviction in Electronic Health Records Management

Narendra Kumar[1*], Vikas Goel[2], Raju Ranjan[3], Mohamed M. Hassan[4], Tushar Kumar Pandey[5], Akhilesh Dwivedi[6]

[1] Department of CSE, Galgotias College of Engineering and Technology, Greater Noida 201310, India
[2] Department of IT, Kiet Group of Institutions, Ghaziabad 201206, India
[3] School of Computing Science and Engineering, Galgotias University, Greater Noida 203201, India
[4] Department of Biology, College of Science, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia
[5] College of Community Science, Central Agricultural University (Imphal), Tura, Meghalaya 794005, India
[6] Department of Electrical & Electronics Engineering, IES College of Technology, Bhopal 462044, India

Corresponding Author Email: narendrakumar@galgotiacollege.edu

https://doi.org/10.18280/ts.410505

Received: 5 October 2023
Revised: 18 March 2024
Accepted: 20 August 2024
Available online: 31 October 2024

Keywords:
HER, Internet of Things (IoT), SHA256 verifiable key, chest X-ray MedPix

ABSTRACT

There is an absolute necessity for healthcare providers, including hospitals and primary care physicians, to keep patient data secure inside their existing healthcare systems. These systems incorporate electronic health records (EHRs), which store detailed medical histories including diagnoses, treatments, and diagnostic tests as well as demographic information like gender, weight, age, and insurance coverage. Sharing this sensitive medical data securely while avoiding unauthorized access and potential breaches is the biggest challenge. One possible solution to this problem is the use of the cryptographic hashing algorithm SHA256 in conjunction with the IoT. By making it difficult for enemies to understand hashed information, SHA256 strengthens data security. To top it all off, SHA256 works well with verified keys, so you can quickly compare created passwords to existing ones to be sure they're legitimate. Better performance metrics are shown by proposed procedures that use SHA256 compared to existing techniques. The average block creation time, total execution time, and blockchain memory capacity are all significantly lower with these new approaches than with their predecessors, which bodes well for healthcare system efficiency and scalability. Essentially, healthcare systems implementing SHA256 represent a significant step toward improving data security and protecting patient information, leading to a more trustworthy healthcare system overall.

1. INTRODUCTION

Whenever it comes to creating health care delivery systems, even doctors and hospitals need to pitch in. A database that may store information about a person's health and be accessible electronically is called an electronic health record (EHR). Therefore, securing the secure transmission of medical information without compromising patient privacy is one of the greatest difficulties currently facing healthcare institutions worldwide [1]. X-ray Participants in the planned study would exchange medical information via MedPix images taken from the EHR.

Essential duties in the healthcare system include the keeping and sharing of health records. More dire consequences, such as a patient's death, could result from a breach in a health monitoring system's security than would result from a breach in the system's integrity alone. It is crucial that electronic health records be kept safe because they contain personal and sensitive information [2]. Block chain technology has gained popularity in recent years due to its greater flexibility in comparison to other options. Data kept on other servers, however, might be illegal or stolen, depending on the specifics of the situation [3].

The current medical data management system does not guarantee the accuracy or completeness of patient information. This is a serious shortcoming. Under the current medical data management system, which is primarily focused on medical institutions, there is no guarantee of the integrity and trustworthiness of patient data [4]. The risks of medical data loss and hacking must be recognised, and the obtained data is always vulnerable to data security breaches, personal privacy violations, and other challenges.

Despite blockchain technology's brief existence (less than a decade), it has already attracted the interest of many industries. Participating sectors include the private and public sectors as well as energy and healthcare [5]. This article presents a comprehensive review of the literature on blockchain's potential applications in healthcare, as well as suggestions for future study. The speed of current research in this sector shows no signs of slowing down. This study has identified several blockchain-based use cases that are today considered to be cutting edge in their respective fields [6].

Sharing medical records digitally, monitoring patients remotely, managing the distribution of medications, and many other uses are all made possible by this technology. We have concluded the discussion by focusing on the limitations of the approaches that have been taken thus far and proposing a number of unanswered research questions and promising directions for further study [7].

Many professionals in academia and business, as well as members of the general public, now view blockchain technology as one of the most promising developments of the past decade. since then, the researcher has amassed a lot of admirers all across the globe [8]. Bitcoin's decentralised and distributed immutable ledger is a peer-to-peer network that facilitates the secure recording of transactions across a large number of computers without the intervention of a central authority.

Enhancing the accuracy of EHRs and linking disparate systems together should be priorities in the quest to better manage health data. Although the phrases are often used interchangeably in the same sentence, EHRs and electronic medical records (EMRs) are distinct [9]. The original concept behind EMRs was to find a digital replacement for the paper charts that doctors traditionally kept. Each patient's medical and treatment history is stored in an EMR at one clinic. However, EHRs examine the patient's overall care and prioritise that over traditional clinical data obtained in the provider's office [10].

Patients' health is monitored remotely by collecting data from their mobile devices, body area sensors, and IoT devices as shown in Figure 1. A growing amount of remotely received biological data is being stored, shared, and retrieved using blockchain technology [11]. In recent years, people have begun using medical sensors to monitor their own health, thanks in large part to the proliferation of IoT devices. When patients are in critical condition, it is essential to gather and send a vast amount of health data generated by these sensors in a safe and reliable manner [12].

As was previously mentioned, the primary advantage of blockchain technology is that it is a decentralised system. What does this mean for us as people? There is no need to involve a central administration or a third party in order to address this issue. Because of this, a centralised authority is superfluous, and the participants in the Blockchain can collectively make decisions [13].

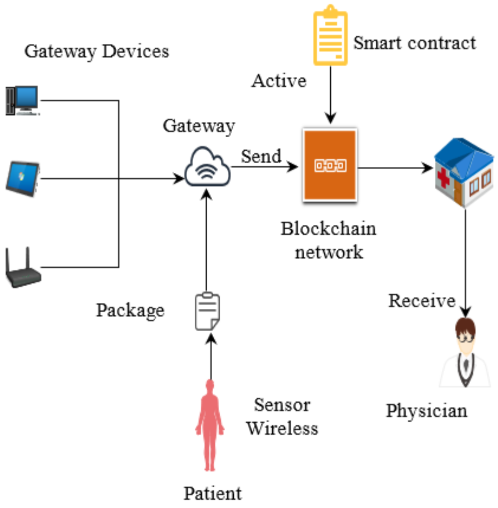

Figure 1. Enterprise of secluded body region administrations (WBANs) for patient observing

The next part serves as a framework for the rest of the study. Part 2 of this publication provides an overview of the associated tasks. This section presents a summary of the studies and research that have already been conducted on this subject. In the next section, we will discuss the research approach and theoretical underpinnings that guided our work in this area. The purpose of this section is to lay forth the methodology and guiding principles that informed this study. The simulation findings and analyses will be presented in Section 4. In this research paper's final part, dubbed "key findings," we seek to provide a brief summary of the most important results.

2. THE EXISTING WORK DONE

Applying the framework of innovation theory, the authors analysed the influence of internal and external factors on the spread of blockchain technology. The study revealed that the anonymity, immutability, and transparency provided by the blockchain were the most valuable features [14]. The primary specialised factors influencing the adoption of blockchain technology are presumably its perceived benefits, complexity, interoperability, information security, development, and relative benefit. The scope of the business, the level of administrative support, and the preparedness of the company are all factors that, according to blockchain's proponents, work in the technologies favour [15]. When formulating a plan of action for implementation in the real world, it's important to take into account the regulatory climate, market factors, industry competition, and government backing. The findings of this review help us better understand the role that an organization's strengths play as a catalyst for adoption. Based on their analysis, researchers have concluded that blockchain technology has a number of clear and improved norms that have an impact on the healthcare sector [16]. Authentication, interoperability, the transfer of medical data, and mobile health are a few of the topics addressed by these guidelines. The aforementioned standards and regulations are at the heart of the current problems facing the healthcare sector [17]. Lack of principles, decentralised capacity and security breaks, key administration, adaptability, and the burden of the IoT are just few of the challenges that the architects of this technology look into.

A thorough survey was carried out to find solutions to the problems mentioned above. Our own differs from those lately disseminated evaluations in terms of approach and goals, despite the fact that there are a few interesting investigations in the writing that are pertinent to this topic. According to a study [18], Blockchain Technology has been implemented in several forms within the healthcare industry. Guard time, for example, uses a blockchain-based medical care stage to verify patients' identities, while the MedRec project aims to streamline the process involved in monitoring privileges, authorizations, and the exchange of patient information among medical organisations [19-22]. The authors also provide a list of "eminent" organisations using blockchain technology to improve healthcare. These groups have substantial authority in a wide range of medical care applications, including the identification of prescription medicine extortion and the creation of patient-focused clinical records [23]. The authors provide examples of blockchain-based applications and businesses in the fields of general health administration, clinical research, and medicine duplication in the pharmaceutical industry. Researchers have compiled a paper outlining the main benefits of blockchain technology over conventional databases for use in healthcare [24-26]. According to the authors of this piece, these benefits could be put to use in enhancing clinical record administration, developing protection guarantee processes, working on clinical examination, and establishing medical services information records [27].

A game-changing architecture for blockchain models with modifications, perfect for blockchain-based IoT devices. In addition to taking into account the asset limits imposed by the IoT, the recommended architecture may solve most security and protection challenges [28]. Despite several dangers, like modification assaults, dropping assaults, refusal of administration (DoS) attacks, etc., the resource limitations of the (IoT) provide significant barriers [29].

A secure, low-overhead authentication mechanism is used to protect sensitive health information while also guaranteeing the confidentiality of all communications. The new approach successfully decreased the access overhead while achieving a high key generation time relative to the transfer and verification times. The massive amount of data is too much for the current technology, so a new approach is needed [30-32].

A complete, personal, and lightweight layout has been given to Blockchain Technology based on the IoT. High degrees of security, anonymity, and availability are provided by the combination of Blockchain Technology with terminal devices that make up the backend system [33]. Despite these technologies' significant dedication to the next industrial revolution, automation and data processing across diverse production systems remains the greatest obstacle.

3. THE OBJECTIVE OF THE RESEARCH WORK

Decisions made by AI might be recorded on a blockchain, allowing for more accurate analysis and explanation of AI behaviour and, ultimately, more trust in AI decision-making.

Reducing energy consumption while boosting processing speed and efficiency requires the creation of a blockchain system that maintains anonymity.

An optimization-based strategy should be created to reduce the lag time between the blockchain's encryption and decryption processes.

4. THE PROPOSED METHOD

Procedures for implementing the suggested algorithm and its associated work flow are outlined below. Using a block chain-based health records monitoring system, we can observe how four problems are addressed and resolved: data fragmentation, delayed access to data, a standardised set of monetary values for medical data, system interoperability, and enhanced data quality. Additional elements of the system include data integrity, individual agency with respect to record authenticity, data exchange, and auditability.

For the research work, we have used a multi-core processor (Intel Core i5+), minimum 8GB RAM, SSD storage (256GB+), stable internet, Windows, IDEs, Docker, with security measures, and backups.

The data stored within a block chain ledger is unchangeable and can be authenticated by anyone with network access. Blockchain networks fall into three primary categories: public, consortium, and private. In a public blockchain, accessible to all users, the ledger is openly shared across all nodes. Conversely, private blockchains are restricted to specific entities, typically private companies. Consortium blockchains operate under the governance of participating organizations, dictating access and permissions for accounting, reading, and writing data.

Considering the reliability of a transaction relies on the inclusion of a hash of the first square in every square thereafter, it is challenging to remove any square from the network without compromising reliability. When a transaction is successfully completed, a permanent record of it is added to the public blockchain network, where it may be accessed by any node in the organisation. Public-key cryptography is used to authenticate all business transactions in this system. Thus, the public square chain became the focus of this inquiry.

Blockchain networks, which rely on a Proof of Work consensus system, found SHA-256's hashing calculation to be fast enough to use for transaction verification as shown in Figure 2. It's crucial to keep in mind that Bitcoin wasn't the first Proof of Work system. HashCash is widely regarded as the primary implementation of the Proof-of-Work mechanism for generating hashes.

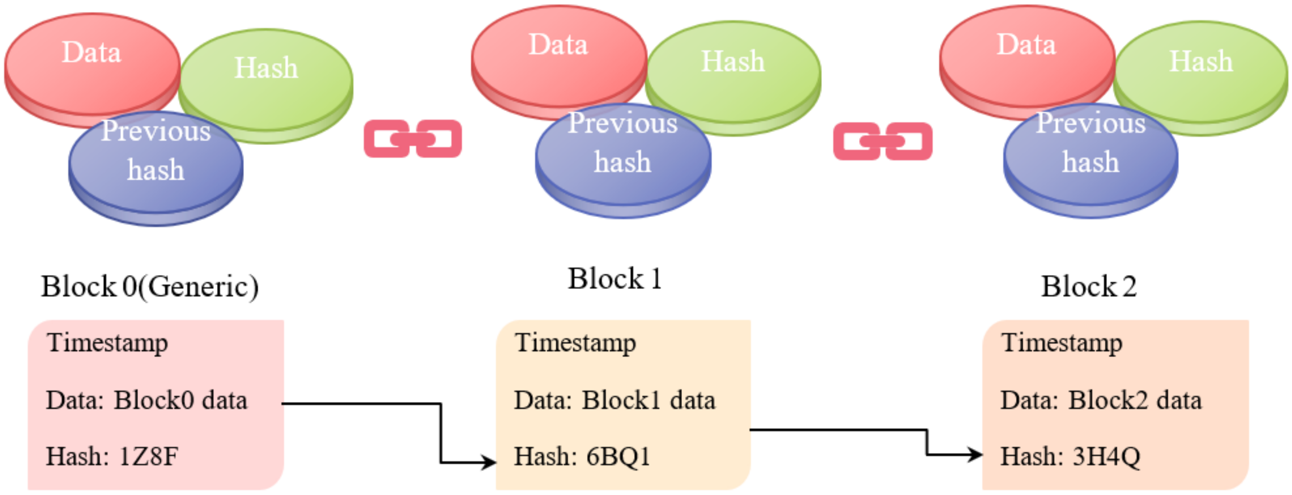

Figure 2. Blockchain arrangement

Proposed Method- SHA-256 hash function to generate a verification vector for a given message:

M and key K.

1. Initialization:

K=Input Key

M=Input Message

2. Basic SHA-256 Hashing:

$H (M)=\text{SHA-256}(M)$

3. Verification Equations:

$V1 (K, M) =\sin (K) \times\cos (M)$

$V2 (K, M) =\tan (K+M)$

$V3 (K, M) =\log (K)+\log(M)$

$V4 (K, M) =K2 -M2$

$V5 (K, M) = K + M$

$V6 (K, M) =K\oplus M$ (Bitwise XOR)

$V7 (K, M) =K\&M$ (Bitwise AND)

$V8 (K, M) =K|M$ (Bitwise OR)

$V9 (K, M) =K!\bmod M$ (Factorial of K modulo M)

$V10 (K, M) = K\times eM$

$V11 (K, M) = \arctan(K)\times\arccos(M)$

$V12 (K, M) =K\div M$ (Integer Division)

$V13 (K, M) = K\bmod M$

$V14 (K, M) =\lceil K\rceil+\lfloor M\rfloor$ (Ceil of K plus Floor of M)

$V15 (K, M) =\text{SHA-256}(K)\oplus\text{SHA-256}(M)$ (Bitwise XOR of hashes)

Final verification vector: $V (K, M) = [V1, V2,..., V15]$

Output: The final output is both the hash of the message and the verification vector: Output=Output= $[H (M), V(K,M)]$

The proposed blockchain course is detailed in Figure 3 as shown below.

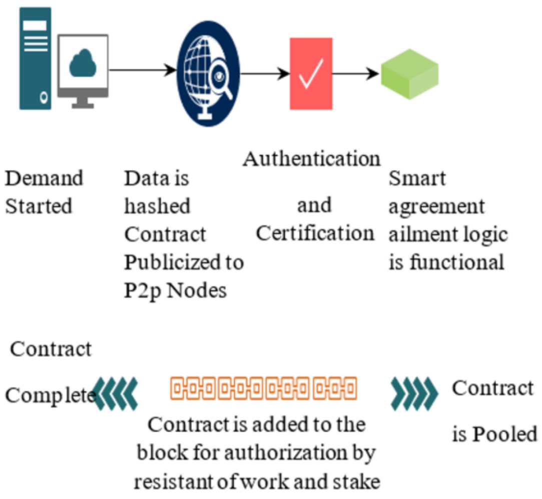
Demand Started
Data is hashed Contract Publicized to P2p Nodes
Authentication and Certification
Smart agreement ailment logic is functional
Contract Complete
Contract is added to the block for authorization by resistant of work and stake
Contract is Pooled

Figure 3. Blockchain course

4.1 Exploring a novel combination of mathematical equations and SHA-256 hashing for verification

Cryptography, in its essence, is a blend of art and science, aiming to ensure data privacy and integrity. The core idea is to make data understandable only to someone who possesses the right key, thereby preventing unauthorized access. Within this vast domain lies the concept of hashing, which involves converting input data into a fixed-size string of bytes, typically a digest that looks random. One such popular hash function is SHA-256.

The algorithm outlined here intends to harness the prowess of SHA-256 and marry it with a series of mathematical equations to generate a verification vector. This proposed system would ensure an extra layer of verification for any given message, *M*, and key, *K*.

4.2 Initialization

Every algorithm begins with initialization. Here, we have two main entities:

•*K*, the Input Key, which is presumably private and aids in the secure computation of our results.

•*M*, the Input Message, which is the data or information we wish to process and verify.

4.3 Basic SHA-256 hashing

SHA-256 stands for Secure Hash Algorithm with a 256-bit digest. When you input a message into the SHA-256 function, it generates an almost unique 256-bit (32-byte) signature. The process involves multiple rounds of processing and bitwise operations, ensuring that even a tiny change in the input message results in a vastly different hash.

$H (M)$ denotes the hash of message M when processed using SHA-256.

4.4 Verification equations

Beyond traditional hashing, this method introduces a set of 15 mathematical equations, aiming to generate a unique verification vector.

•$V1$ (K, M): It multiplies the sine of key K with the cosine of message M. Trigonometric functions introduce periodicity, ensuring diverse results for different inputs.

•$V2$ (K, M): Here, the tangent of the summation of key and message is taken.

•$V3$ (K, M): This is the summation of the logarithms of K and M, promoting exponential diversity.

•$V4$ (K, M): A straightforward squared difference between the key and the message.

•$V5$ (K, M): This represents the summation of K and M.

•$V6$ (K, M) to $V8$ (K, M): These are bitwise operations on K and M. They handle the binary representations of the inputs, adding another layer of complexity.

•$V9$ (K, M): This involves the factorial of K, which then undergoes modulo operation with M. Factorials can grow large rapidly, making this equation computationally intensive.

•$V10$ (K, M): Now, K is multiplied through the exponential of M, foremost to fast evolution for huge M.

•$V11$ (K, M): A mixture of the arctangent of K and the arccosine of M.

•$V12$ (K, M) and $V13$ (K, M): These are integer division and modulo processes, correspondingly.

•$V14$ (K, M): Syndicates the ceiling of K and the floor of M.

•$V15$ (K, M): A prominent equation that calculates the SHA-256 hashes of together K and M, then takings their bitwise XOR.

Final verification vector and output:

In the end, we get the verification vector V (K, M) as an array of the solutions to all fifteen equations. This vector adds another layer of verification by functioning as an extra "signature" for the original message.

A combination of M's SHA-256 hash and the verification vector is the algorithm's ultimate result. Together, [H (M), V (K, M)] provides a powerful way to verify the validity and authenticity of a communication.

In conclusion, this method's power is in the wide variety of mathematical operations it employs, which include hashing, bitwise operations, exponential growth, and trigonometry. Within the realm of cryptography, it exemplifies how several branches of mathematics have come together. Even while it's intriguing in theory, we won't know if it works or is secure until it's tested and assessed by experts in the field.

Competing computers use hashing to try to solve a difficult mathematical issue; the SHA-256 hash function is the building block of this Proof of Work structure. When one computer in the distributed system finds a solution, it notifies the others, demonstrating their combined effort. A decentralized validation method is demonstrated by each computer independently verifying the solution's accuracy. Once confirmed, the discoverer receives a financial reward.

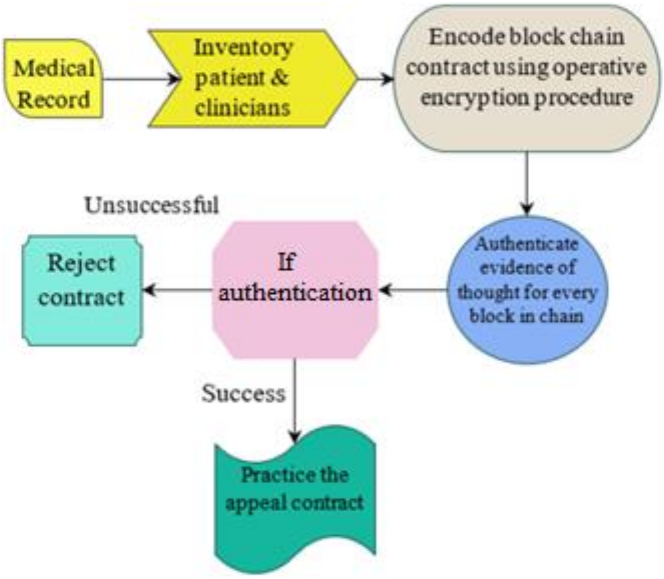
Medical Record
Inventory patient & clinicians
Encode block chain contract using operative encryption procedure
Authenticate evidence of thought for every block in chain
If authentication
Unsuccessful
Reject contract
Success
Practice the appeal contract

Figure 4. The proposed methodology flow diagram

As depicted in Figure 4, the proposed healthcare framework's system architecture comprises a web-based application with two ends: a front end for patient interaction and a back end facilitating internal communication using blockchain technology. The precise request acts as the pivotal link connecting these two endpoints. The proposed healthcare architecture is simplified for all audiences by providing examples of web-based interactions between patients and providers. In the background, where block chain communication occurs, there are entities that are linked as a network of nodes.

The clinical data set was compiled using a standard data set maintained by the University of California, Irvine (UCI) and referred to as the AI storehouse. Next, a robust lightweight authentication and key understanding system is populated with patient and doctor data to ensure their safety. The three steps depicted in this proposed standard are the registration process, the login procedure, and the authentication procedure.

Secure and reliable method to confirm the patient is by checking the hash value, encrypted with the patient's private key and created with SHA256. We add this hash value to the request to ensure that the first request gets to the clinic fully and on time. This is required to decrypt the patient's public key and is maintained separate from the requests being created. After the SHA256 algorithm is done with its processing, the hash value is stored in a database for further analysis.

Due to the fact that patient data that is used in this method is obtained from medical records, it is crucial to develop a procedure that would decrypt the code and assess the current relevance of the data. In the course of decrypting a patient request encrypted by the SHA256 method, the sender's hash value is disclosed to the receiver. To ensure the safe isolation of the sensitive information from the patient solicitation, a hash code will be created, and its equivalent will be decrypted in a way that is different from the process of collecting patient solicitation information.

In terms of the advancement of health data, the two most important objectives should be the integration of multiple systems and the refinement of the electronic health records (EHRs). The proper use of EHRs guarantees the correctness of the data, and, therefore, the quality of the decisions made in the course of patient treatment. The combination of the separate systems that used to operate in isolation allows the healthcare providers to exchange the patient's information, which contributes to the improvement of the treatment process and excludes the possibility of the mistakes. If we provide the highest priority to these projects, it will be possible to create a more harmonic ecology in the healthcare industry and, therefore, increase the rates of productivity, cooperation, and care for patients.

There are several limitations such as security issues in IoT devices, integration of blockchain with the existing healthcare information systems, and handling of big data. Another issue that we need to consider is the protection of users' personal data and compliance with rules. More studies are needed to achieve the objectives of eradicating these limitations and proving that the proposed paradigm is beneficial in real-life healthcare environments.

5. RESULT ANALYSIS AND DISCUSSION

We might think of the blockchain as an immutable digital ledger that records all monetary transactions and, in principle, anything of value. This ledger is known as the blockchain. A blockchain is an ever-expanding digital ledger of all of the blocks (units of data representing financial transactions) that are cryptographically connected to one another. Each block also includes a timestamp, the cryptographic hash of the preceding block, and the transaction data, which is represented as a tree-like structure called the Merkle tree root hash. A blockchain is a distributed, immutable, and continually updated ledger of all past and present economic transactions. It's important to remember that a public record can be verified by anyone associated with the company, because blockchain records are not maintained in a central location. Due to the lack of a standardized framework, developers cannot exploit any given framework with confidence that they have caused it to fail.

The effectiveness of the proposed blockchain technique undergoes scrutiny through a verified secure hash computation utilizing the provided elements and factors. Validation of the findings is conducted via an exhibition metric termed Square Time, measuring the duration required to mine a single square as shown in Table 1 and Figure 5. The cumulative time spent executing a cycle typically remains unaffected by its initiation time but may vary based on data intricacies, thus aligning closely with a proportion of interaction execution time, commonly referred to as central processor time. This process ensures the robustness of the blockchain system, as it evaluates the cryptographic integrity of the hash computation and assesses the efficiency of mining operations which is presented in Figure 6. By employing Square Time as a benchmark, the technique's performance can be quantitatively evaluated, shedding light on its scalability, security, and operational viability within diverse computational environments. Since the efficacy of safety in cloud-supported EHR should be enhanced, realistic simulations for constructing a safe convention obstruction were developed using the approach for acceptable simulation for convention testing used in the prior work. When compared to the previous standard SHA256, the proposed SHA256-VK showed significant improvements in both security and square execution time. The block chain memory size evaluation of the proposed method is compared with existing approach in Table 2 and Figure 7.

Table 1. Parameter evaluation of the proposed method with the state of the art methods

S. No.	Algorithms	Evaluation Parameters	
		Average Block Time	Blocks Generation Time (200 Blocks)
1	SE [12]	48.63	9.71
2	SDN [14]	11.24	5.27
3	ECC [15]	5.93	4.52
4	Proposed algorithm	5.16	3.83

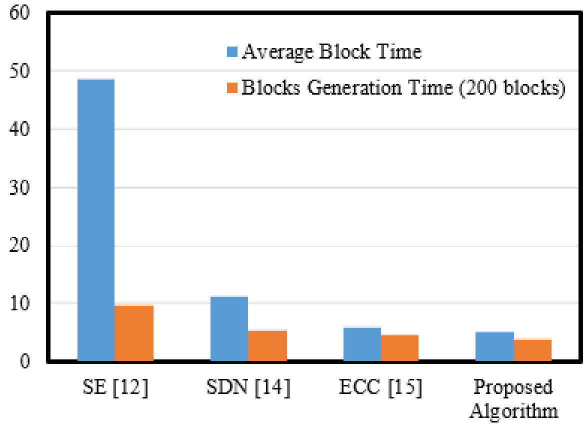

Figure 5. Parameter evaluation of the proposed method with the state of the art methods

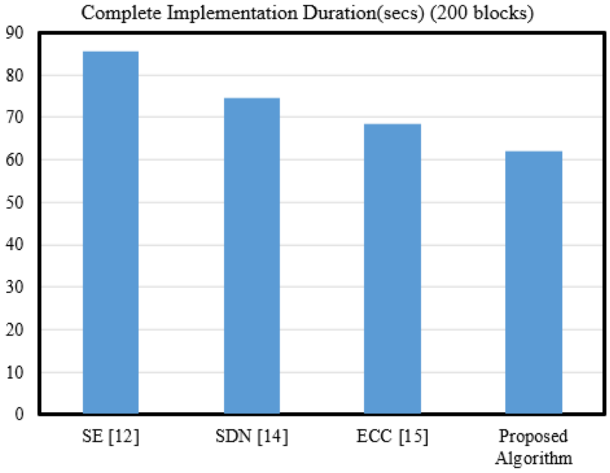

Figure 6. Whole implementation time assessment of the projected technique with the state of the art techniques

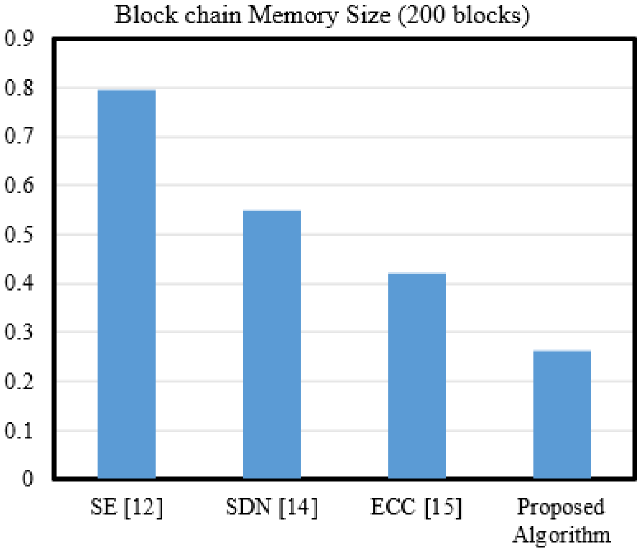

Figure 7. Block chain memory size evaluation of the proposed method with the state of the art methods

Table 2. Parameter assessment of the projected technique with the state of the art methods

S. No.	Algorithms	Evaluation Parameters	
		Total Execution Time (secs) (200 Blocks)	Block Chain Memory Size (200 Blocks)
1	SE [12]	85.69	0.795
2	SDN [14]	74.58	0.549
3	ECC [15]	68.34	0.421
4	Proposed algorithm	61.92	0.263

Interoperability extends beyond mere technical integration to include user accessibility across various blockchain implementations. Currently, widespread adoption is hindered by the need for users to possess a deep understanding of technical details to effectively engage with multiple blockchains. However, for blockchain and cryptocurrencies to achieve ubiquity, simplifying user interaction is essential. This means protecting users from the complexities and providing intuitive interfaces. The central argument of this thesis is the creation of a secure, intuitive interface capable of communicating with multiple blockchains. This approach aims to democratize access to blockchain technologies, empowering users regardless of their technical skills. By simplifying interfaces, more people can navigate between different blockchain platforms effortlessly, fostering participation in the decentralized ecosystem. Ultimately, prioritizing user-centric design principles lays the groundwork for widespread acceptance, thereby building trust and accelerating the mainstream integration of blockchain technologies.

The overall system execution time increases in direct proportion to the number of blockchains utilized. A quantitative study noted a decrease in efficiency as the number of blocks grew from 50 to 500, leading to an increase in overall execution time. Table 1 presents the results of this study, detailing the time (in seconds) required to implement the proposed SHA-256 VK cryptographic technique based on varying block counts. The graphical representations in Figures 5 and 6 visually illustrate the relationship between the number of blocks and the corresponding execution times.

In Figure 6, the proposed method is compared with existing approaches to evaluate the blockchain memory size, and it can be concluded that the memory size is comparatively reduced with the proposed method.

6. CONCLUSION

Prescriptions and previous medical records are now crucial pieces of information in a patient's diagnosis and treatment plan, reflecting the growing importance of medical care in modern society. Medical charts historically, medical records were kept on paper, which made them vulnerable to loss or tampering. Therefore, it was essential that the data be kept electronically. Data security is bolstered by the SHA256 cryptographic hashing algorithm, which renders information hashed with it unrecoverable by an adversary. SHA256 uses a trusted key, so it can compare the newly entered password to the authentication it has on file and, if they match, accept the new password as legitimate. With regards to typical block generation time, total execution time, and block chain memory size, the proposed solutions perform better than the state-of-the-art.

Improved results are seen across the board for several metrics when using the suggested methodology. The underlying fusion process can't handle the more frequent occurrence of the noisy add-on. This new and improved method has numerous advantages, one of which is its resistance to the selected plaintext attack and its ability to unravel into the original picture even as noise from the transmission channel increases. If the code phrase is correct, just the transaction recovery will be completed; otherwise, the request will be ignored.

ACKNOWLEDGMENT

The authors extend their appreciation to Taif University، Saudi Arabia, for supporting this work through project number (TU-DSPP-2024-68).

FUNDING

This research was funded by Taif University, Saudi Arabia, Project No. (TU-DSPP-2024-68).

REFERENCES

[1] Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D., Sun, L. (2020). An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems. Sensors, 20(5): 1521. https://doi.org/10.3390/s20051521

[2] Li, C.T., Shih, D H., Wang, C.C., Chen, C.L., Lee, C.C. (2020). A blockchain based data aggregation and group authentication scheme for electronic medical system. IEEE Access, 8: 173904-173917. https://doi.org/10.1109/ACCESS.2020.3025898

[3] Xia, Q., Sifah, E.B., Smahi, A., Amofa, S., Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2): 44. https://doi.org/10.3390/info8020044

[4] Roy, V., Shukla, S. (2017). Effective EEG motion artifacts elimination based on comparative interpolation analysis. Wireless Personal Communications, 97(4): 6441-6451. https://doi.org/10.1007/s11277-017-4846-3

[5] Kim, S.K., Huh, J.H. (2020). Artificial neural network blockchain techniques for healthcare system: Focusing on the personal health records. Electronics, 9(5): 763. https://doi.org/10.3390/electronics9050763

[6] Rajput, A.R., Li, Q., Ahvanooey, M.T. (2021). A blockchain-based secret-data sharing framework for personal health records in emergency condition. Healthcare, 9(2): 206. https://doi.org/10.3390/healthcare9020206

[7] Chen, L., Lee, W.K., Chang, C.C., Choo, K.K.R., Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future generation Computer Systems, 95: 420-429. https://doi.org/10.1016/j.future.2019.01.018

[8] Kim, M., Yu, S., Lee, J., Park, Y., Park, Y. (2020). Design of secure protocol for cloud-assisted electronic health record system using blockchain. Sensors, 20(10): 2913. https://doi.org/10.3390/s20102913

[9] McGhin, T., Choo, K.K.R., Liu, C.Z., He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135: 62-75. https://doi.org/10.1016/j.jnca.2019.02.027

[10] Clohessy, T., Acton, T., Rogers, N. (2019). Blockchain adoption: Technological, organisational and environmental considerations. Business Transformation through Blockchain, 1: 47-76. https://doi.org/10.1007/978-3-319-98911-2_2

[11] Roy, V. (2020). Network physical address based encryption technique using digital logic. International Journal of Scientific & Technology Research, 9(4): 3119-3122.

[12] Mehedi, S.T., Shamim, A.A.M., Miah, M.B.A. (2019). Blockchain-based security management of IoT infrastructure with Ethereum transactions. Iran Journal of Computer Science, 2(3): 189-195. https://doi.org/10.1007/s42044-019-00044-z

[13] Nuryyev, G., Wang, Y.P., Achyldurdyyeva, J., Jaw, B.S., Yeh, Y.S., Lin, H.T., Wu, L.F. (2020). Blockchain technology adoption behavior and sustainability of the business in tourism and hospitality SMEs: An empirical study. Sustainability, 12(3): 1256. https://doi.org/10.3390/su12031256

[14] Agi, M.A., Jha, A.K. (2022). Blockchain technology in the supply chain: An integrated theoretical perspective of organizational adoption. International Journal of Production Economics, 247: 108458. https://doi.org/10.1016/j.ijpe.2022.108458

[15] Jung, D.H. (2022). Enhancing competitive capabilities of healthcare SCM through the blockchain: Big data business model's viewpoint. Sustainability, 14(8): 4815. https://doi.org/10.3390/su14084815

[16] Chittipaka, V., Kumar, S., Sivarajah, U., Bowden, J.L.H., Baral, M.M. (2023). Blockchain technology for supply chains operating in emerging markets: An empirical examination of technology-organization-environment (TOE) framework. Annals of Operations Research, 327(1): 465-492. https://doi.org/10.1007/s10479-022-04801-5

[17] Cai, C., Hao, X., Wang, K., Dong, X. (2023). The impact of perceived benefits on blockchain adoption in supply chain management. Sustainability, 15(8): 6634. https://doi.org/10.3390/su15086634

[18] Alazab, M., Alhyari, S., Awajan, A., Abdallah, A.B. (2021). Blockchain technology in supply chain management: An empirical study of the factors affecting user adoption/acceptance. Cluster Computing, 24(1): 83-101. https://doi.org/10.1007/s10586-020-03200-4

[19] Nazim, N.F., Razis, N.M., Hatta, M.F.M. (2021). Behavioural intention to adopt blockchain technology among bankers in Islamic financial system: Perspectives in Malaysia. Romanian Journal of Information Technology & Automatic Control, 31(1): 11-28. https://doi.org/10.33436/v31i1y202101

[20] Cho, S., Lee, Z., Hwang, S., Kim, J. (2023). Determinants of bank closures: What ensures sustainable profitability in mobile banking? Electronics, 12(5): 1196. https://doi.org/10.3390/electronics12051196

[21] Jena, R.K. (2022). Examining the factors affecting the adoption of blockchain technology in the banking sector: An extended UTAUT model. International Journal of Financial Studies, 10(4): 90. https://doi.org/10.3390/ijfs10040090

[22] Hashimy, L., Jain, G., Grifell-Tatjé, E. (2023). Determinants of blockchain adoption as decentralized business model by Spanish firms–an innovation theory perspective. Industrial Management & Data Systems, 123(1): 204-228. https://doi.org/10.1108/IMDS-01-2022-0030

[23] Palos-Sanchez, P., Saura, J.R., Ayestaran, R. (2021). An exploratory approach to the adoption process of bitcoin by business executives. Mathematics, 9(4): 355. https://doi.org/10.3390/math9040355

[24] Fülöp, M.T., Topor, D.I., Ionescu, C.A., Căpușneanu, S., Breaz, T.O., Stanescu, S.G. (2022). Fintech accounting and Industry 4.0: Future-proofing or threats to the accounting profession? Journal of Business Economics and Management, 23(5): 997-1015. https://doi.org/10.3846/jbem.2022.17695

[25] Ferri, L., Spanò, R., Ginesti, G., Theodosopoulos, G. (2021). Ascertaining auditors' intentions to use blockchain technology: Evidence from the Big 4 accountancy firms in Italy. Meditari Accountancy Research, 29(5): 1063-1087. https://doi.org/10.1108/MEDAR-03-2020-0829

[26] Tran, L.T.T., Nguyen, P.T. (2021). Co-creating blockchain adoption: Theory, practice and impact on usage behavior. Asia Pacific Journal of Marketing and Logistics, 33(7): 1667-1684. https://doi.org/10.1108/APJML-08-2020-0609

[27] Roy, V., Khaparkar, S., Tripathi, P. (2023). An effective identification of flavor complaint by adaptive analysis of electroencephalogram (EEG) signal. In 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP), BHOPAL, India, pp. 25-28. https://doi.org/10.1109/IHCSP56702.2023.10127108

[28] Orji, I.J., Kusi-Sarpong, S., Huang, S., Vazquez-Brust, D. (2020). Evaluating the factors that influence blockchain adoption in the freight logistics industry. Transportation Research Part E: Logistics and Transportation Review, 141: 102025. https://doi.org/10.1016/j.tre.2020.102025

[29] Roy, V. (2021). An improved image encryption consuming fusion transmutation and edge operator. Journal of Cybersecurity and Information Management, 8(1): 42-52. https://doi.org/10.54216/JCIM.080105

[30] Khazaei, H. (2020). Integrating cognitive antecedents to UTAUT model to explain adoption of blockchain technology among Malaysian SMEs. JOIV: International Journal on Informatics Visualization, 4(2): 85-90. https://doi.org/10.30630/joiv.4.2.362

[31] Dehghani, M., Kennedy, R.W., Mashatan, A., Rese, A., Karavidas, D. (2022). High interest, low adoption. A mixed-method investigation into the factors influencing organisational adoption of blockchain technology. Journal of Business Research, 149: 393-411. https://doi.org/10.1016/j.jbusres.2022.05.015

[32] Malik, S., Chadhar, M., Chetty, M., Vatanasakdakul, S. (2022). Adoption of blockchain technology: Exploring the factors affecting organizational decision. Human Behavior and Emerging Technologies, 2022(1): 7320526. https://doi.org/10.1155/2022/7320526

[33] Bakri, M.H., Aziz, N.A.A., Razak, M.I.M., Hamid, M.H.A., Nor, M.Z.M., Mirza, A.A.I. (2023). Acceptance of Ddkoin blockchain using UTAUT model: A customer perspective approach. Calitatea, 24(192): 103-121. https://doi.org/10.47750/QAS/24.192.13