Received: April 17, 2021. Revised: May 24, 2021.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Blockchain for Secure Medical Records Storage and Medical Service Framework using SHA 256 – Verifiable Key

Prashant Digambar Hakim[1]* Vinod Moreshwar Vaze[1]

[1]*Department of Computer Science,*
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India
* Corresponding author's Email: Prashanthakim03@gmail.com

Abstract: Electronic Health Record (EHR) is widely adopted by various providers for health care systems such as hospitals, medical practitioners, doctors, etc. and the medical technology involves collecting health information related to diseases, medication, medical images, etc. Personal information such as age, name, gender, billing, and weight details of an individual is highly sensitive data that need to be protected against unauthorized access, hence, the protection of medical data is a big challenge for healthcare systems. The importance of this research work to analyze the sharing of medical data securely without any leakage of patient's data when the unauthorized user accesses the data. In this current research, Chest X-ray MedPix images from the EHR are used to share medical data through encryption and uploading the data into the cloud. The proposed framework uses SHA256 cryptographic hashing technique as it can enhance the security of a patient's data. Meanwhile, the attacker is not able to reverse back the key by the process of hashing. The SHA256 has a verifiable key ability for matching and verifying the new passwords against the authentication to improve the security for sensitive data. The proposed SHA256 Verifiable Key (SHA256-VK) executed at a faster rate, as it consumed a lesser 'average block time' of 5.48612s when compared to Searchable Encryption-48.125s, Smart-Contract Ethereum Distributed Ledger-14s, Decentralized Security Architecture-Software Defined Networking (SDN)-10s and Elliptic Curve Cryptosystems (ECC) -5.88s.

Keywords: Blockchain, Chest c-ray MedPix, Electronic health record, Security, SHA256 Verifiable key.

1. Introduction

Blockchain technology allows for the creation of a public record that has the decentralized digital information across the entire network of computer systems [1]. The 'block' is referred to as the data, which are linked together in a single list, which forms a 'chain' that consists of digital information [2]. The blockchain has a wider range of applications such as healthcare, as the health data exchange in the decentralized system protects the health information [3]. An advantage of using blockchain in the medical field is that it eliminates the burden and the cost issues associated with data reconciliation, and therefore enables easy access to real-time applications using blockchain technologies [4]. The preservation and sharing of health records are necessary tasks performed in all healthcare systems. In health monitoring systems, the loss of high security negatively affects the protection of health records largely [5], and the loss of data integrity may lead to serious implications such as loss of a patient's life. So, it is necessary to provide security for electronic health records that consist of sensitive as well as private information [6]. In recent years, blockchain technology is considered more adaptive as compared to other techniques but in existing methods, when data stored in outsider servers, it might be stolen or legitimate, problems in terms of data security, personal privacy leakage, etc., [7]. The current medical data management systems that are used by medical institutions do not guarantee the integrity and reliability of patient data [8].

In the current medical data management systems, the medical data shows risk factors such as data loss, hacking of the data from unauthorized users, data security, personal privacy leakage, etc. The medical data which are obtained from medical institutions are centralized in such a manner that it becomes vulnerable to distinct cyber threats such as hacking, malicious tampering that would lead to loss of medical data and data leakage [9]. Therefore, in the present research work, the use of blockchain technology gives an advantage, since it effectively addresses the issues related to security in cloud-based systems that are immutable [10].

The main contribution of the research work is that the proposed SHA256 cryptographic hashing technique is used for enhancing the security of the data of patients, in a manner that will not allow the attacker to reverse the hashing process. The SHA256 has a verifiable key that can match dynamic passwords against the received authentication, which improves the security. The organization of the paper is as follows: Section 2 is the literature review that describes the existing methodologies involved in blockchain security in health care. Section 3 describes the proposed encryption model for blockchain technology. Section 4 describes the results and discussion of the proposed methodology. The conclusion and future work of this research given in Section 5.

2. Literature review

This section describes the existing researches involved in providing security for health care using blockchain effectively were as follows:

Chen [11] developed Blockchain-Based Medical Records Secure Storage and Medical Service Framework for cloud storage. The developed model used the hash chain that followed the factors such as decentralization, immutability, and verifiability for securing and storing personal medical data. The developed model was based on the storage scheme that managed the medical data and personal data based on the blockchain and was stored in the cloud. However, the developed model flow safely, convenient to the cost and controllable for medical blockchain network but failed to analyze improvement required in-home safety management for the medical data.

Mehedi [12] developed blockchain-based security management for the IoT infrastructure with Ethereum transactions. The developed model used the terminal devices in the network technology that integrated IoT infrastructure with Ethereum transactions for the blockchain platform. An advantage of the model was that it ensured high availability, privacy, and high security that replaced the traditional back end system. However, the developed model required additional technologies for the exchange of data among the nodes, which was a major challenge.

Rathore [13] developed Blockchain-based decentralized security architecture (BlockSecIoTNet) for IoT networks. The decentralized approach was constructed for providing security using Software Defined Networking (SDN) architecture in IoT-based blockchain technology. An advantage of the developed model was that the IoT network was relied on for detecting the attacks in the network more effectively. However, the developed model used a slightly longer time of about 8 and 14 seconds for system recovery from the normal state.

Chen [14] developed Blockchain-based Searchable Encryption for sharing of Electronic Health Record. The developed model used an index for EHRs that constructed complex logic expressions for data searching. The index was migrated in the blockchain for network propagation and the data owners had control over the EHRs data. The developed model included proof-of-concept for the scheme to improve security. The model was not applicable for real-world settings as it would be high energy-dependent and was difficult for processing integration.

Kim [15] designed a Secure Protocol for Cloud-Assisted Electronic Health Record System using Blockchain. In the developed blockchain technology, data integrity was provided for controlling access during log transactions. The cloud servers that stored the patient's EHRs, provided security for the resources managed the transactions. However, in the developed model, a realistic simulation for protocol testing was needed for providing secure protocol to the cloud in the blockchain.

3. Proposed methodology

The section explains the workflow of the proposed method along with implementation steps. The proposed research will add individual features such as empowering, data integrity, data sharing, towards record authenticity and audibility. Thus, the proposed work considers an innovative technology for providing a solution to secure the health record in blockchain technology. The explanation for the proposed method is shown in Fig. 1.

3.1 Database chest X-rays (MedPix)

The health data includes information on each patient who has undergone medical services in the hospital. The patient's health data are recorded in the EHR that provides healthcare services in the medical center.

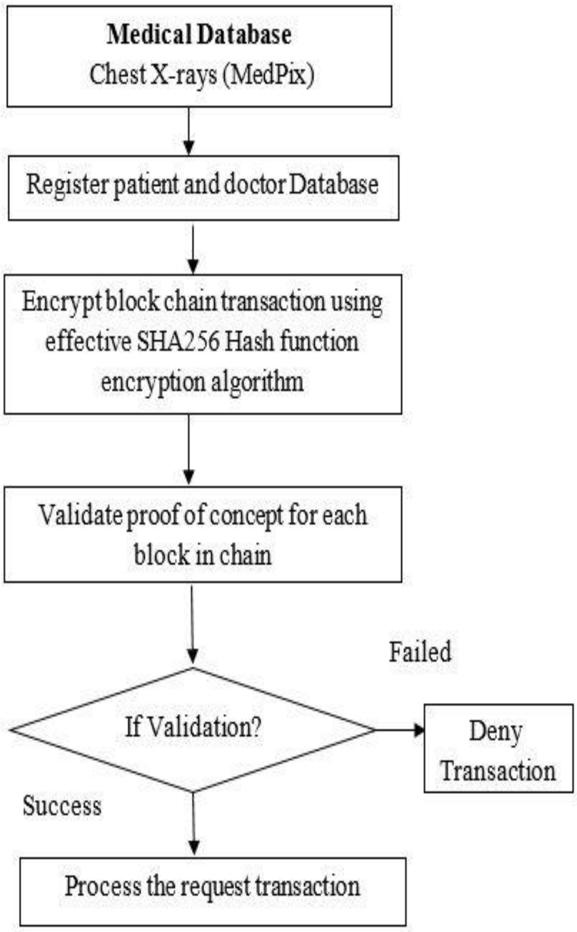
Medical Database
Chest X-rays (MedPix)
Register patient and doctor Database
Encrypt block chain transaction using effective SHA256 Hash function encryption algorithm
Validate proof of concept for each block in chain
Failed
If Validation?
Deny Transaction
Success
Process the request transaction

Figure. 1 Block diagram of the proposed method

These medical centers are well registered in detail about the patients, which describes their data as well. The network administrators are registered by medical centers that participate in the private blockchain. The medical centers will be registered by the network administrator will participate in the blockchain privately. The EHR will generate an identity for each data to store in the medical centers. The medical centers view EHRs that belong to the medical centers of each patient and uploads the medical data through the server. The medical centers are viewed in the EHRs that will store in the cloud serves for sharing the transaction information and store in the cloud servers.

3.2 Registration phase

The medical information of the patients includes details such as gender, age, general health, family history, and the sensor readings are stored securely in a separate database. The medical staff and the authorized doctors are allowed to access the patients' medical information. The main purpose is to provide authentication between the patient and the healthcare provider using a strong framework policy. The patient effectively communicates with the provider through a security protocol and automatically provides control access, authentication.

3.3 Login phase

The login phase is followed by many calculations such that the doctor or patient will choose an identity to set a private password. The doctor or patients for calculating the dynamic passwords for every patient choose arbitrary random numbers. The dynamic password is sent to the doctor along with the patient's data to the cloud's health care server through a secured channel. The cloud server will generate a query and the registered patients' health data will be updated in the BC. The server calculates One-Time Password (OTP) every time it receives a request from the registered patients and doctors. The server will choose a random number that will compute a session key using an algorithm known as private encryption. Finally, the server stores all the patient/doctor information on a BC, and sends the session key via a secure channel to the patient.

3.4 Encryption phase

To secure the healthcare blockchain process, a fully homomorphic encryption algorithm is used in the proposed method. There are two keys required for communication, one is a public key and the other is a private key. Furthermore, the cryptosystem is a one-way process i.e., the public key is used only for encryption, and the private key is used only for decryption. The medical center will receive the information from a smart contract of patients using a session key and the medical center will generate a patient's smart contract and EHR. The smart contract generated in the medical center uploads the data to the blockchain. The medical center will encrypt the EHRs of their registered patients by using a verifiable secured secret key that sends the key to another medical center. The key generation is processed with data security is as shown below:

Key Generation ($\boldsymbol{\beta}$):

To process the generation of the private key and public key, the following equation should be calculated using Eq. (1).

$$\beta = r\, w_i \, mod\; q \tag{1}$$

where, r is a random integer, such that $gcd\ (r, q)$ = 1 (i.e. r and q are co-prime), w_i is the word to encrypt n-bit messages, $w = (\, w_1, w_2, \dots . w_n\,)$ of n non-zero natural numbers and a random integer q, $q \; is \; greater \; than \; \sum_{i=1}^{n} w_i$.

Encryption:

The proposed SHA-256 with a verifiable secure secret key is a cryptographic hash function that obtains an output value of 256 long bits. The process of hashing is performed to enable the data to be transformed into a secure format, which will be in an unreadable state until the recipient knows the secret key. When the data is in encrypted form, the data used will be or can be of an unlimited size or will be a long size. An advantage of using hashing function when compared with the existing encryption techniques is that the attacker cannot reverse the process of hashing. The algorithm used in the proposed method considers an input message of length 2^{64} and the outputs will be of 256 bits' hash. This is the specialty of SHA 256, which is a unilateral function that can find the plain text not only using a single hash function but also improves the security for the medical data. The main features of SHA256 are:

1. It is difficult or impossible for data reconstruction using the hash value.
2. If two messages are having the same hash value then the collision occurs then the possible number of hash values present is 2^{25}. This has more number of atoms and therefore two hash values with the same value are unimaginable. However, it is an extremely unlikely condition.
3. If the original data is altered with the minor change in the hash value, then the newly generated hashed value will be not derived from the same data.

The researcher tends to use SHA256 with a verifiable secret key which lessens the weight during the computation to maintain strong security.

In the blockchain, each block uses a $SHA256$ hash algorithm that customizes the token in the new block, which is composed, based on the Previous Block (PB), hash values, and Nonce (N). The verifiable secret key (ver) has the key resolver that is used for carrying the Time Stamp (TS) for the authentication and verification of the password. The elements used for the research is computed using the following elements is represented as $SHA256\ (NB//PB//verTS\ //N)$.

$SHA256$ is computed by concatenating elements which are shown in Table 1.

Table 1. $SHA256$ algorithm and their elements used in the present research work

Acronyms	Description
H	Hospital
P	Patient
BC	Block Chain
R	Request
TS	Time Stamp
KR	Private Key
KU	Public Key
N	Nonce
ID	Patient's identification
H	Hash value
AT	Authentication Token

Confidentiality:

The generated data will ensure whether any information has been theft during the transaction. If the patient requests for an authentication token, then the block chain of health data from the hospital regarding the patient details will be confidentially transferred. The patient will request an authentication token to BC can be represented as $ATKU(BC)[IDP, RP, KUC, TS, N00]$

The generated authentication token belonging to the patient will be used by the BC and is used for decrypting the requests together with the private key of the patient encrypts the data by using the BC's private key shown in Eq. (2).

$$ATC = TKR(BC)\ [IDP, RP, H, KUC, TS, N00] \quad (2)$$

Authentication:

The processes of key agreement and the login phases are completed and the doctor or server setups an authentication system for communications. The doctor and patient change the dynamic passwords at any point of time with the time stamp, only when the session keys are bundled with the request. The new passwords will be verified with the healthcare server that has the ability for verifying the passwords by matching the verification key against the authentication key. If the passwords are not matched, then the connection will be denied. If the intruders happen to impersonate the patient's and the doctor's legal data, by copying the transaction messages, then these messages are resent to the doctor and the patient at another time from the server. The applied timestamp with the random number will prevent them from exploiting the data. Using the private key, the patient will send their signed ID, nonce, and time. This whole package will be encrypted by the third person (or other hospitals) using its public key. By then, the package is decrypted with its private key to grant access to the Patient's ID and should be signed by the patient's private key to prove its authenticity. Using the patient's private key, the key is used for encrypting elements such as ID, TS, $N00$ and issue an encrypted new nonce $N0$ spawned by the patient's based on the hospital's public key and forward it back to the Hospital is represented as $TKU(M)[N0, TKR(P), [IDPP, TS, N00]]$.

Data integrity:

Data integrity is ensured by SHA256 and the patient's hash value is generated using SHA256, which is encrypted using the private key of the patient. The encrypted hash value is concatenated with the original request and directs towards Hospital. These hash values are separated from the requests from decryption of the patient's KU undergoes computation using the SHA256 algorithm. The confidential information of the patient from the hospital data needs to be established better thereby computes the code, decrypts the code and checks whether the data are the same. The hash value from the receiver (H) will be revealed from the patient request using the SHA256 algorithm for the process of decryption. The confidential information of the patient request will be properly established by computing the code and decrypting the hash code from the request. The confidential information is decrypted by using the patient's public key which computes the hash value for the transaction received based on the requests from SHA256 – VK. Revealing confidential information of the patient request establishes properly the hash code and the hash codes are decrypted by generating the same hash code. The patient will respond as nonce $N1$ from the H and send the hash code from the previous step for encryption using KU of H is represented as $TKU(H)[TKR(P), [N1]]$.

The security attributes include replays, requests, hash values, public keys, identification of the public key. These attributes are secured during online transactions and checks for the tokens received by the process of authentication from BC to P and P to H .The patient's key verification and hospital vitrification will be used to perform the token authentication and also communication is performed in the secure domain. These two stages will be simultaneously performed using two-way authentication and recording the data into the BC system. The patients and the hospital data are protected with the security are responsible for integrity check and the authentication check is performed through verifiable validation. The validation of each blockchain is carried out by Proof Of Concept (POC) or Proof of Work.

The steps of POC (Proof Of Concept) include:

- Check whether the patient is valid or not.
- Check whether the doctor is valid to retrieve the patient data or not.
- Check whether the lab technician's data is related to the patient's lab report.
- If the request transaction is successful, then those transactions are enabled for further processes, otherwise, the transactions are denied.

4. Results and discussion

The simulations of the proposed research work are performed on a computing system with an Intel Core i9- 3GHz processor, 128 GB memory, and Windows 10 (64 bit) operation system, and coding is implemented in Python 3.7.

4.1 Performance measures

The parametric measures that are used to validate the performance results of the proposed blockchain technology with verifiable secure hash technique, (i) Block time, and (ii) total execution time. Block time defines the time each block takes to mine data. The total execution time, also known as the CPU time, is the total amount of time taken to execute the process, and this measure is generally independent of the initiation time but is often dependent on the input data.

4.2 Quantitative analysis

Table 2 shows the performance result of the proposed SHA 256 with a verifiable secret key algorithm, obtained in terms of blockchain memory, block generation and total execution. The number of blocks ranges from 50 to 500 and as the number of blocks keeps changing; the blockchain memory will increase due to the embedding of more data information. The graphical representation of the block generation time varies linearly from 50 to 500 blocks.

When the blockchain memory is increased to 0.2850Mb, the block generation time also increases to 9.9747s, which shows that the block generation time will be increased if the number of blocks also increases. The graphical representation of the proposed SHA256-VK concerning blockchain memory is shown in Fig. 2 and the proposed SHA256-VK with respect to block generation is shown in Fig. 3.

Received: April 17, 2021. Revised: May 24, 2021.

Table 2. Quantitative analysis for the proposed SHA 256 with verifiable secret key Algorithm in terms of block generation time with respect to the memory acquired

Number Of Blocks	Block Chain Memory Size(Mb)	Block Generation Time(secs)
50	0.28331	0.9973
100	0.28353	1.9946
150	0.28365	2.9919
200	0.28386	3.9913
250	0.28393	4.9867
300	0.28423	5.9852
350	0.28426	6.9825
400	0.28442	7.9796
450	0.28481	8.9774
500	0.2850	9.9747

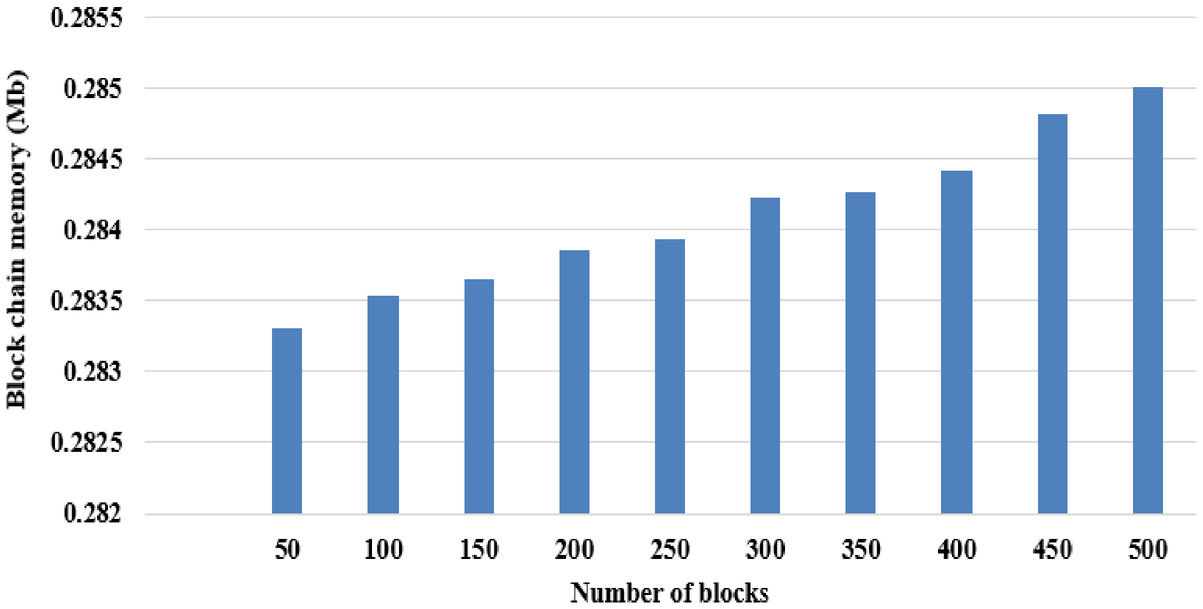

Figure. 2 The graphical representation for the proposed SHA256-VK with respect to blockchain memory

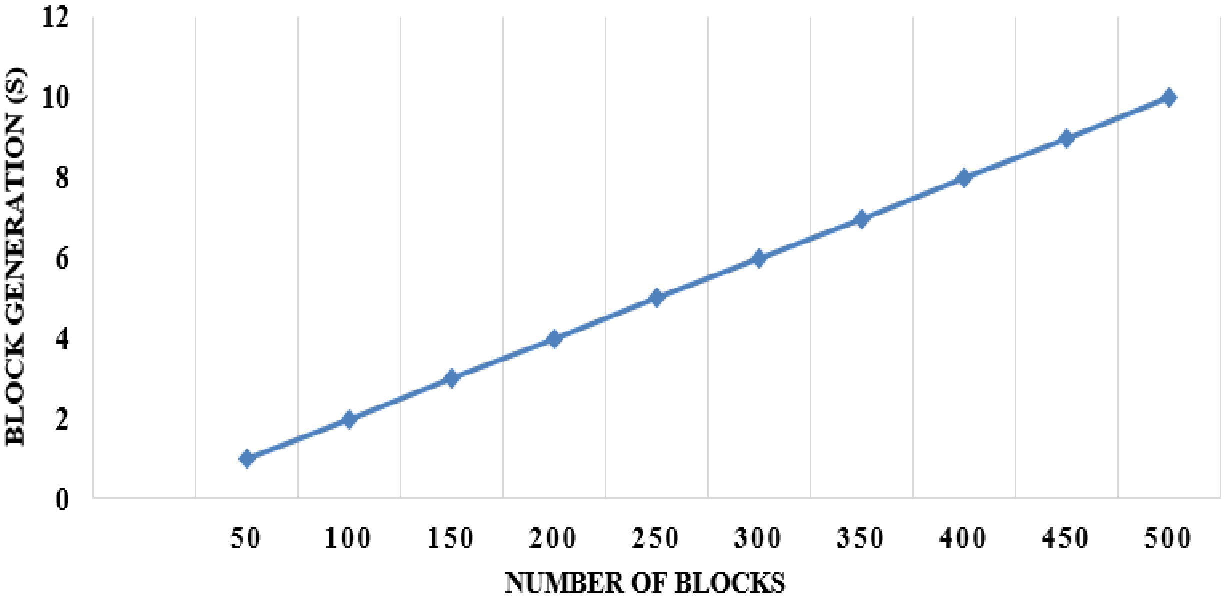

Figure. 3 The graphical representation for the proposed SHA256-VK with respect to block generation

Table 3. Quantitative analysis for the proposed SHA 256-VK cryptographic scheme in terms of number of blocks with respect to the time execution (secs)

Number Of Blocks	Total Execution Time(secs)
50	58.897
100	60.835
150	61.835
200	61.888
250	63.829
300	63.839
350	64.839
400	69.844
450	70.867
500	78.791

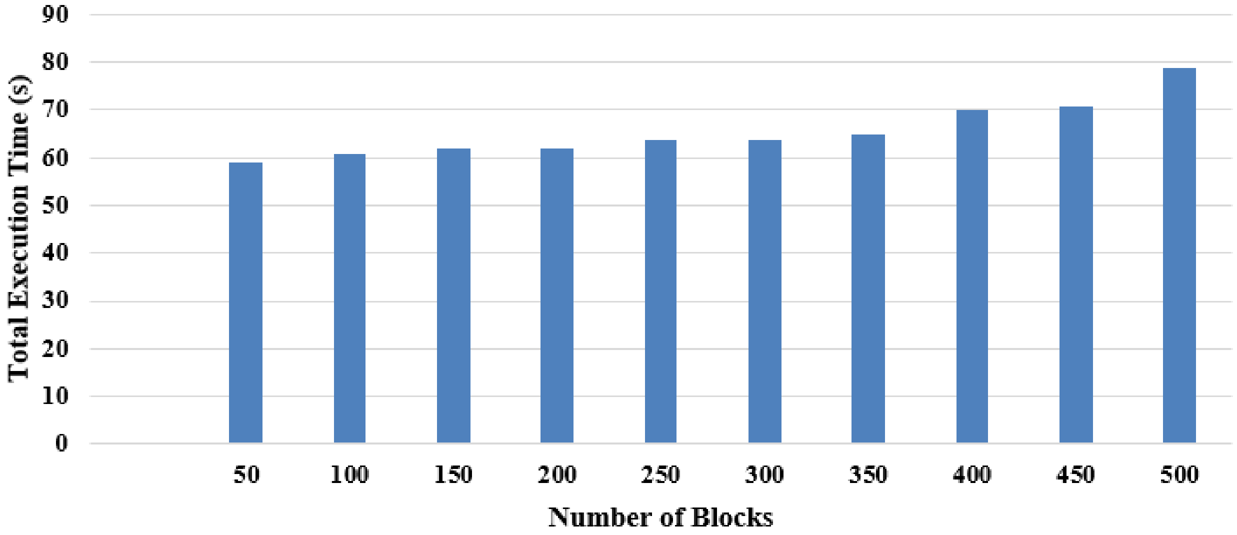

Figure. 4 The graphical representation for the proposed SHA256-VK with respect to total execution time (s)

The total time of execution of the system increases when the number of blocks increases. As the number of blocks increased from 50 to 500, the total execution time, in terms of seconds, also varies from 58.897s to 78.71s. Table 3 shows the Quantitative analysis for the proposed SHA 256-VK cryptography scheme in terms of a number of blocks with respect to the total execution time (secs). The graphical representation for the total execution time is shown in Fig. 4.

4.3 Comparative analysis

The comparative analysis of the proposed model with the existing models in terms of average block time (s) is shown in Table 4. The average block time of the proposed SHA256-VK model is 5.48s faster when compared to the average block time of existing models used for storing confidential information in the blockchain. In Mehedi [12], the developed Smart-Contract Ethereum Distributed Ledger model failed in the data exchange process among the nodes that led to an increase in the average block time. Similarly, Rathore [13] developed a Decentralized Security – SDN model which consumed a slightly longer time of about 10 to 14 seconds for system recovery from the normal state. Whereas Chen [14] and Kim [15] developed Searchable Encryption and ECC model for realistic simulation required improvement in terms of practical simulations. The secured protocol resistance required improvement in the efficiency of the security for EHR in the cloud. The proposed SHA256-VK showed improvement in terms of security as well as block execution time. The proposed SHA256-VK cryptographic hashing technique enhances the security of the patient's data in such a way that the attacker cannot reverse the process of hashing.

This is because, the SHA256 uses a verifiable key that can verify or match the new password by matching it against the authentication received, thereby resulting in improvement of the security and execution time.

Table 4. Comparative Analysis for the existing and the proposed research work

Authors	Methodology	Number of blocks	Average block time (s)	Computational cost (s)
Mehedi [12]	Smart-Contract Ethereum Distributed Ledger	500	14	-
Rathore [13]	Decentralized Security -Software Defined Networking (SDN)	500	10	69
Chen [14]	Searchable Encryption	-	48.125	-
Kim [15]	Elliptic Curve Cryptosystems (ECC)	500	5.88	74.02
Proposed method	**SHA256 with verification secret key**	**500**	**5.48612**	**65.54**

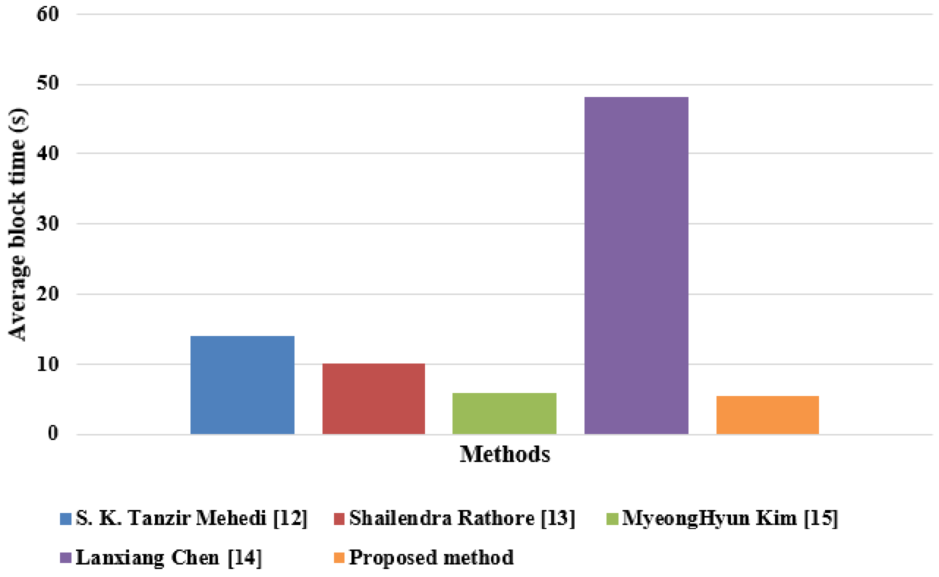

Figure. 5 Graphical representation of the comparison among existing methods and the proposed SHA-256 VK scheme

The comparative analysis also showed that the proposed SHA256 with verification secret key estimates the time that it takes for model to execute on real-time hardware of 65.54s given input size, requires a relatively large number of steps up-to 500 number of blocks to complete. Thus, the computational cost was lowered in the proposed research when compared to the existing ECC and SDN systems. Table 4 shows the Comparative Analysis for the existing and the proposed research work and Fig. 5 shows the graphical representation of the comparison between the existing methods and proposed method.

5. Conclusion

The present research work uses BC as a storage supply chain and each operation will be counted, verified and the data stored in the chain are also immutable. The notable features of the proposed method offer potential solutions for healthcare systems to protect the patient's data privacy and data sharing. The present research uses the BC as a storage scheme or a service framework that stores, shares and utilizes the medical data of hospitals. The proposed Blockchain-based solution is a viable approach that allows one to build upon SHA256 cryptographic algorithms to ensure data integrity, standardized auditing, and some formalized contracts for data access. The proposed SHA 256-VK was suitable for healthcare systems that implement EHRs because it provides more security and efficient protection than other related schemes such as ECC, Smart-Contract Ethereum Distributed Ledger, and Searchable Encryption. An advantage of using the proposed SHA 256 is that it is difficult for the hackers to reconstruct the data from the hash value due to the usage of a verifiable key in the algorithm. If the intruder tries to reconstruct the data, the verifiable key will check for the dynamic new password by matching it with the authenticated password. If the password matches, only then the retrieval of the transaction is done, or else, it will be denied. The proposed SHA 256 showed 0.4 to 48 seconds of improvement for average block time and 4 to 9 seconds of improvement in terms of computational time when compared to the existing ECC and SDN systems methods. For future works, realistic simulations need to be set up for testing the security protocol. If the practical simulations are present, then a secured protocol for cloud assessment for the EHR system was required using BC.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions (Mandatory)

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS", *IEEE Access*, Vol. 8, pp. 59389-59401, 2020.

[2] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications", *Journal of Information Security and Applications*, Vol. 50, pp. 102407, 2020.

[3] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, "An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems", *Sensors*, Vol. 20, No. 5, pp. 1521, 2020.

[4] R. Haque, H. Sarwar, S. R. Kabir, R. Forhat, M. J. Sadeq, M. Akhtaruzzaman, and N. Haque, "Blockchain-Based Information Security of Electronic Medical Records (EMR) in a Healthcare Communication System", *Intelligent Computing and Innovation on Data Science*, pp. 641-650, 2020.

[5] C. T. Li, D. H. Shih, C. C. Wang, C. L. Chen, and C. C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System", *IEEE Access*, Vol. 8, pp. 173904-173917, 2020.

[6] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments", *Information*, Vol. 8, No. 2, pp. 44, 2017.

[7] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform", *Cognitive Systems Research*, Vol. 52, pp. 1-11, 2018.

[8] S. K. Kim and J. H. Huh, "Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records", *Electronics*, Vol. 9, No. 5, pp. 763, 2020.

[9] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition", *Healthcare*, Vol. 9, No. 2, pp. 206, 2021.

[10] B. Arunkumar and G. Kousalya, "Blockchain-Based Decentralized and Secure Lightweight E-Health System for Electronic Health Records", Intelligent Systems, Technologies and Applications, pp. 273-289, 2020.

[11] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework", *Journal of medical systems*, Vol. 43, No. 1, pp. 1-9, 2019.

[12] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of IoT infrastructure with Ethereum transactions", *Iran Journal of Computer Science*, Vol. 2, No. 3, pp. 189-195, 2019.

[13] S. Rathore, B. W. Kwon, and J. H. Park, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network", *Journal of Network and Computer Applications*, Vol. 143, pp. 167-177, 2019.

[14] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing", *Future Generation Computer Systems*, Vol. 95, pp. 420-429, 2019.

[15] M. Kim, S. Yu, J. Lee, Y. Park, and Y. Park, "Design of secure protocol for cloud-assisted electronic health record system using blockchain", *Sensors*, Vol. 20, No. 10, pp. 2913, 2020.