Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 3152-3167

A Framework for Secure eHealth Data Privacy Preserving on Blockchain with SHA-256 in Cloud Environment

Naveen N[1], Dr.K.Thippeswamy[2]

[1]Research Scholar, Department of Computer Science & Engineering, VTU-RRC, Belagavi, Karnataka, India
[2]Professor, Department of Computer Science & Engineering, VTU PG Centre, Mysore, Karnataka, India

Abstract

Safeguarding the eHealth information of patient's stands utmost paramount for performing web-scale analytics and reporting applications. Apparently, there has been data breaches that have become quite prominent lately. The prime target is towards resolving the issue of determining robust and trustworthy analytics in a secured way that fulfills product pre-requisites. There is proposal of an improved version of eHealth data privacy preserving system apt for the cloud space. The proposed system yields in at par integration, interoperability, availability as well as sharing of healthcare information amidst various healthcare providers, patients, and practitioners. There is distribution of patient's health details amidst the various Treatment Service Company which are combined and put away in the cloud space thus building the patient's overall eHealth information. Cloud technology benefits by providing prompt Internet access as well as feasible access to eHealth information from any location and platform at any given time. There has been a significant rise in the volume of the healthcare information produced as well as the difficulty involved in its data type. To resolve this, technique of blockchain has been recommended for determining effective measures by the practitioners at the right time. Moreover, the proposed system imbibes certain important security constraints and access control mechanism that ensures security, integrity, and protection of Ehealth information via blockchain using SHA-256. Above all, the said system encourages development of a system that is economical, highly efficient and secure.

Index Terms: Preserving privacy, Data Analytics, Cloud, e-healthcare System, Blockchain, SHA-256.

1. INTRODUCTION

The eHealth system is a major contribution in development of the overall cloud environment by outsourcing their critical data management systems. Such eHealth framework helps in building bonds among the major entities viz, patients, doctors and hospital, which also leads to generation

of voluminous amount of eHealth information. Primarily, the eHealth records comprise of diagnostic records, health monitoring data, medical histories and prescriptions as indicated by [1].

It's highly crucial that all the preserved eHealth information is kept highly confidential and protected, failing which can result in misleading and wrong treatment thus causing a negative effect on patient's life. Certain prime issue to be confronted are of authorized access, interoperability of health records, rule enforcement or data sharing policies pertaining to the shared content and securely sharing eHealth records as per [2].

Today, achieving patient's data confidentiality stands as the most critical challenge that remains of paramount importance for maintaining data integrity. With peak in digitization of healthcare system, there is significant improvement in precise analysis, patient's overall care as well as safe and secure eHealth data accessing. Caseless increase in eHealth data along with its processing and storing can definitely impact the scalability aspect of the eHealth system. Attending this concerning issue is out of reach for the old conventional approaches. Towards this, the cloud technology assures to be the most effective means in achieving the storage and processing of such massive amount of data indicates [3].

In a cloud-based eHealth system, the eHealth information is stored by the healthcare providers on the cloud servers. Transferring of eHealth information over the cloud storage space greatly helps in data sharing amidst the healthcare and research organizations in a prompt and hassle-free manner. Maintenance and storage of eHealth records must inculcate precise access control, authentication, and privacy measures in order to fulfill the integrity, confidentiality, and accessibility requirements of such information. There is proposal of a hierarchical framework that adopts blockchain for identifying the traceability of the data access policies defined by the data owner, an audit trail elaborating about the data accessed by third party requesters, agreements with the third-parties for the data sharing and much more. There must be implementation of Auditing mechanisms to enable monitoring and recording of queries and data accesses. The efficient Blockchain framework enables securing eHealth framework for building a patient oriented, permission driven data access platform as mentioned by [4].

There is recommendation of Secure Hash Algorithm using Blockchain that significantly helps in safeguarding against threats and vulnerabilities. Many national web portals offer online government services like bill payment, registration through the internet medium. The improvised secure hash algorithm comprises of 512 bits hash message and makes use of a quadratic function for choosing primitive functions and constants for every round according to [5].

There is requirement of a robust technique for message authentication and verification. Formed and standardized by the National Institute of Standards and Technology (NIST), the SHA (Secure Hash Algorithm) gives ideal performance in maintaining integrity properties. Essentially, SHA aids in compression wherein any given message size can be compressed to a fixed length hash as indicated by [4]. [6] Specifies that the SHA256 includes a ME (message

expander) and a MC (message compressor). The ME (message expander) is responsible for expanding the 512-bit input message into 64 chunks of 32-bit data which is thereafter compressed into a 256-bit hashed output by the MC (message composer). In order to maintain the Bitcoin network, the required amount of energy evolves from computing the double SHA256 values. Apparently, minimizing the hardware expense along with the energy usage of the SHA-256 circuit has become a trending research. An array of 7-3-2 compressor has been proposed for minimizing the critical path delay for SHA-256. By the means of the carry-save adder's technique, latency of additions in the SHA-256 algorithm can be minimized. the block forms the basic component of blockchain that includes a segment header having distinct information and a square body comprising of exchange information. This block information helps in interfacing the past square and listing of information from the hash estimation of reach block. Every blockchain exchange is accompanied by employing hash work collaboration that guarantees the security of blockchain process pertaining to application processing according to [7]. In addition, optimal solutions can be determined and chosen with respect to the independent program variables for gaining variable optimal solution sets with equivalent function and varying computing efficiency. And if merged with blockchain, there is enhancement in the Hash algorithm's performance, transmission efficiency, as well as the security.

Khuat et al., [8] refers to the working of the hash function in the blockchain network. The existing status of-the-workmanship hash work in blockchain is considered as protected due to the associated examination. For breaking a private key of 256-bit length, the programmer must exhaust 2256 conceivable key instances. Execution of the mill prevailing mill super-PCs is able to execute 1018 key tests per second. This makes the hacking framework consume around 3x1051 year for debilitating the looking space of the key. Even in case of undesirable condition where the programmer is provided with highly sophisticated computer that can tackle the above mentioned issue in a single day instead of 3x1051 extended duration, the blockchain technique is robust enough to combat any threats by linking the blocks together through a cryptographic hash work.The research merges blockchains with Hashing algorithm and emphasizes towards enhancement of computation execution of hashing capacity by upgrading the competency of correspondence offices and organization's information transmission. The investigation structure is divided as follows: section 2 elaborates overall related work, Section 3 lays down the proposed structure, Section 4 covers entire results along with various discussions and lastly the conclusion and future related work is presented in section 5.

2. RELATED WORK

The process of Digitization offers the benefits of easy computation, better storage and improvised accessibility of medical records thus uplifting which enables better treatment experiences for patients. Applying privacy preserving mechanisms is essential to the protection of digital assets, whether they be personal, industrial or commercial. Current mechanisms

measures include the collection of data from several points to detect, and potentially foresee, anomalies that can be attributed to malicious behavior [10].

Fengweiwang et al. has recommended the approach of privacy-preserving collaborative model learning using skyline computation, referred to as PCML which relies upon paillier cryptosystem involving threshold decryption and distributed skyline computation. The owner encrypts the local diagnosis models which are computed without decryption with PCML during the collaborative model learning process. The healthcare system comprehends a global diagnosis model in association with their local diagnosis models with the cloud's support in order to safeguard the critical eHealth information and provide overall protection as indicated by [11].

Mingwuzhang et al., has put forth the scheme of a PPO-CPQ (Privacy- Preserving Optimization of Clinical Pathway Query scheme) to enable safe clinical pathway query under e-Healthcare cloud servers by protecting the patient's confidential details like age, gender, and physical index. Initially, there is formation of various secure and privacy-preserving sub-protocols namely, privacy-preserving comparison, privacy-preserving clinical comparison, privacy-preserving stage selection and privacy preserving stage update protocol that makes the entire e- Healthcare protected. With the help of a secured greedy algorithm, query and the Min-Heap technology is executed for uplifting the efficiency as mentioned by [12].

The distributed ledger technique of Blockchain offers a protected, immutable, tamper-proof and dispersed data store. This technique allows the alliance of non-trusting partners for carrying out their business activities without the need of third-party authorization thus providing a transparent infrastructure network. In a nutshell, through the blockchain technique, multiple stakeholders can reveal their agreement consistently regarding the actual state of shared data. Usually, the data owner is responsible and controls the permissions related to the release of medical data which is quiet a challenging task. Patient-driving interoperability has become much trending in the medical sector points out [9]. And the technique of Blockchain can further simplify the flow of data sharing from institution-centric to patient-centric thus providing the patients with effective ownership on their data as well as uplifting patient-driven interoperability using digital access rules effectively. There is a brief description pertaining to the major characteristics of blockchain technology in [13-14].

H.S. Jennath et al., discovers the possibility of forming trusted blockchain based Artificial Intelligence models in e-Health sector which can provide a transparent platform for consent-based data sharing. Training and testing of AI or machine learning models is not performed on similar datasets. For training, authorized data sets are employed which further helps in prediction. For acknowledging the individual's consent and data traceability of data sources that are imbibed to build and train the AI model is taken into account in an immutable distributed data store. The audit trail of the data access seized through Blockchain helps the data owner in comprehending the data exposure. In addition, the user gets to know which all revenue models

can be formed over this framework to construct authentic AI models that aids in commercial data sharing, as stated by [15].

Tharukarupasinghe et al., has recommended a dynamic consent management architecture based upon the technique of blockchain technology and smart contracts that complies six prime design targets. Also, there is no need of the patients for the data verification process. There are three smart contracts involves namely: 1) registration, 2) request policy and 3) response policy. At the time of registration, there is generation of a smart asset also referred to as "consent profile". Rest of the smart contracts includes access policies that are specified for addressing the prime key design goals according to [16].

RenpengZou et al., has suggested the framework of medical data sharing and privacy preserving eHealth system that employs the blockchain technique and integrates Repucoin with the SNARKs based chameleon hash function for preventing against potential blockchain threats. This framework helps in building a new chain model that forms micro-blocks contribution to the chain's weight as claimed by [17].

A blockchain oriented incentive technique has been recommended by Ranamubashar et al., for patient driven data collection system that enables training of Machine Learning and Deep Learning pertaining to medical researches. The system works by fetching abnormal or unique data information from the patients by offering them certain incentives in return. Thereafter the doctor validates the abnormality of data and annotates the data for training the neural network model. This procedure significantly enables the medical sector, doctors as well as the researchers in determining innovative and effective treatments for diseases that remain still incurable. The above system make sue of secure Blockchain technique for storing the patient's information and imply the payment rules, indicates [18].

Bhavyesharma et al., has proposed the a national blockchain framework that help in maintaining the access controls pertaining to patient's EHR (Electronic Health Records) and aid in funding of India's National healthcare approach. This particular approach offers the healthcare provides a clear-cut and transparent insurance claim along with auditable trail of EHR access through smart contracts. It employs a zero-knowledge proofs for validating the authenticity of the beneficiaries' identity and provide access to the service the providers through proxy re-encryption as stated by [19].

RaifaAkkaoui et al., suggests the MedChain architecture that enforces edge computing and blockchain for enhancing and fulfilling the essential pre-requisites that helps in safeguarding the data management healthcare ecosystem with respect to efficiency, security and scalability as pointed out by [20].

For storing and assessment of health information, Rajashekhar M Patil et al., has built a general framework that is based upon the blockchain network that adopts an analytical engine for

effective storage that can process voluminous data on a real time basis. Accessing the health information of any patient is allowed to the relevant authorized patient only. That is by using the private key the patient can access their information which is generated when the patient's record is stored in a blockchain. There is just triggering of Smart contracts upon storing the data on the blockchain. There is no provision of overall information to the others as mentioned by [21].

Jigna et al., highlights the concerns regarding security and confidentiality in Healthcare 4.0 that's sectioned into following four parts. 1.) Brief discussion regarding the background and history of healthcare. 2.) Depiction of standard and advance architecture using the conventional security approaches and blockchain technique. 3.) Taxonomy description pertaining to security and privacy concerns of Healthcare. 4.) Presenting the concerns and research challenges regarding the Healthcare's 4.0 security and confidentiality as per [22].

A comprehensive study has been proposed by Shekachenthakara et al. that covers the prevailing e-health cloud preserving cryptographic and non-cryptographic techniques responsible for maintaining the confidentiality in cloud and any sort of threats confronted in the digitalization process says [23].

The research emphasizes towards the formation of Parameterizable Implementation of SHA-256 calculation in FPGA referring the approach of Blockchain. SHA-256 forms the basis of Blockchain design that ensures security and privacy of a network. Significant results are generated with the single direction hash work and available information that ensures authorization of information and non-disavowal. [24] Presents that the technique of Blockchain innovation is gaining significant popularity Online as it works on decentralization. [25] Acclaims that the Bitcoin employs SHA-256 calculation. Though, mining of pools and illustrations cards makes the issue of centralization quiet obvious. [26] Presents that the present research revolves around the prime technique of blockchain which being the SHA-256 hash work. An equipment quickening agent has been recommended that varies according to the application's requirements. This allows the enabling of *hardware acceleration* of highly computational intensive part of the protocol that comprises of huge computation of SHA-256 hash function. Apart from the blockchain's deployment, hardware acceleration of SHA-256 benefits the efficiency of IoT applications immensely as the SHA-256 is utilized in different security approaches like the Hash-Based Message Authentication Code and the Digital Signature Algorithm. Apparently, SHA-256 is highly implemented cryptographic hash functions which is popularly adopted in security-critical regions apart from the IoT, like finance or cloud computing. The SHA-256 Hash algorithms can be split in $O(\sqrt{N})$ evaluations, with N resembling the size of the function domain. This yields in 2128 evaluations rather than 2256 that tends to be computationally tough. Though the birthday attack is enforced, still the SHA-256 collision resistance can be split into 285 operations. Determining such nonce is tedious but once determined, the validity check becomes easier. The cryptographic hash function employed in Bitcoin is twice SHA-256 according to [27].

3. PROPOSED WORK

This research has put forth a technique for safeguarding the privacy of the E-healthcare records through the Blockchain approach. The distributed ledger technique of Blockchain helps in effectively recording transactions amidst two parties. The transactions are stored on a record called blocks which are interlinked via cryptography in order to build a chain called Blockchain.

The concept of interoperability in medical sector refers to the electronic exchange of the medical records among various hospitals or between the hospital and the labs practitioners. The patient's on the other side have no clue regarding the placement of their health records or its sharing. Entities such as the data management, data exchange and privacy protection play a pivot role here. Herein lies the utmost implementation of a efficient framework and approach which emphasizes on patient centered interoperability by making the patient control their own data. The Blockchain technique in association with SHA-256 enables and accelerates privacy preserving patient centric interoperability. Cryptographic hash algorithms like SHA assures trustworthy transactions cryptographic hash algorithms. The present research assumes a brief study pertaining to instruction-set customization that leverages Blockchain with SHA algorithms for protecting the confidentiality in cloud as depicted in.

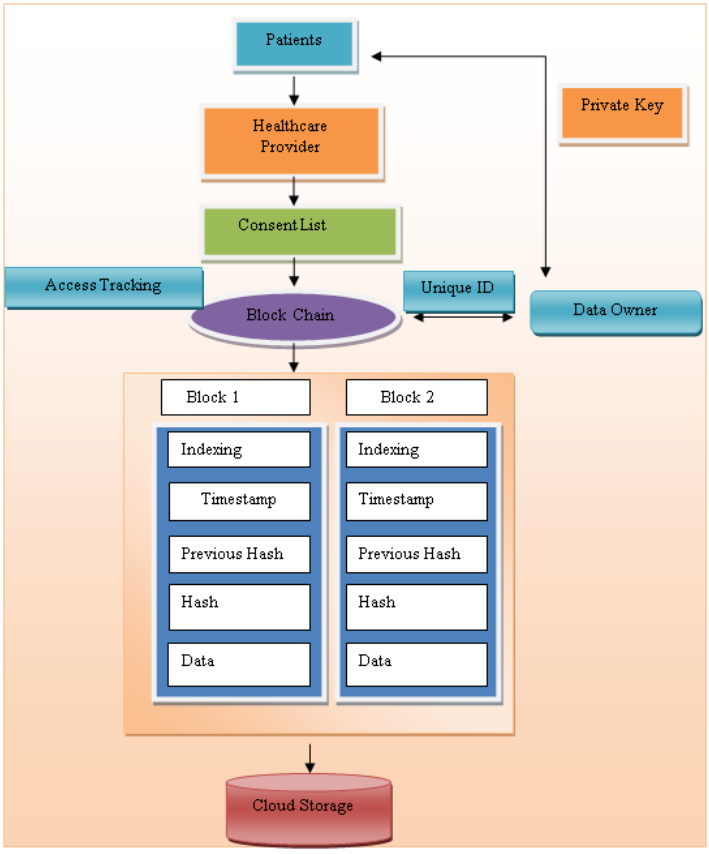


Figure 1: Architecture of the proposed work

The main components of the Blockchain network are

Participants - Patients and Data owner resemble the primary participants of a Blockchain network.

Assets - The E-healthcare records forms the major assets.

Transactions – Represents processing of assets such as appending the participants to the network, generating medical records, updating and fetching the participants' details, granting or revoking access to the data users.

Healthcare Provider – There are diverse implementation of Blockchain in medical sector. The ledger technique enables transferring of patient's medical records securely and managing the medicine supply chain.

Consent List –This list manages the users' private data disposal policies along with the corresponding consents such as generation, updates, and withdrawals. The consent tend to be significant as it legitimizes any sort of collection and use of personalized data. Moreover, the data subjects can generate domain-specific, generic or privacy policies that includes a set of rules pertaining to the data subjects' consents.

Hash Algorithm – It generates value of fixed length output. This algorithm is implemented on online interfaces as it ensures enhanced security against possible threats**.** It also guarantees safe and secure message transaction.

Indexing – There is continuous generation of hashing addresses using hash work on the key value. This is because the input is split by the SHA-256 into fixed size blocks. It may happen that the last block is smaller, hence it is padded till it matches the desired block size.

Time Stamp – Using the timestamp, the exchange data remains fixed or consistent on the square which further helps in depicting the exchange. The timestamp remains closely linked to the square so the timestamp of the parent block is recollected for the hash to determine the hash esteem. The default timestamp comprising the overall essential timestamp info is then returned. There exist a timestamp data array for every active currency since the Origin Stamp submits the hash to various blockchain.

Figure 1 illustrates the framework which enables the patients' in sharing their health records via Blockchain. The framework maintains the confidentiality and security of health records on Cloud space while doing so. Upon forwarding the sensitive data to the healthcare provider, the ledger provides the data into ownership and the key shared among the patients and data owners for security purposes. Once the key distribution is over, the record is obtained by the consent list. This list helps in managing the private info pertaining to the user's data disposals and updations as well as offers a set of rules for privacy policies. In addition, there is interaction between the Data owner and patient through blockchain without letting any third party or an attacker to

intrude. Block chain significantly helps in protecting and confining the patient's information by allocating unique ID to the patients through transaction and also securely sharing the data amidst the participants. The Secured Hash Algorithm in collaboration with blockchain elevates the security level. Information handling of SHA-256 is performed through pre-processing and hash calculation. At first there is padding of message in pre-processing wherein the padding message is parsed into N x 512-bit blocks that further results in the final information of fixed length for better transaction. Secure hash algorithm has been imbibed on web portals for tightening the security against potential threats.

3.1 Structure of the Blockchain

A block usually includes the hash of the prior block, timestamp, nonce and transaction data which helps in generating the hash for that particular block through the cryptographic algorithms. These hash pointers associates each block to its predecessor, at the same time holding a hash of the preceding block too as depicted in Figure.2.

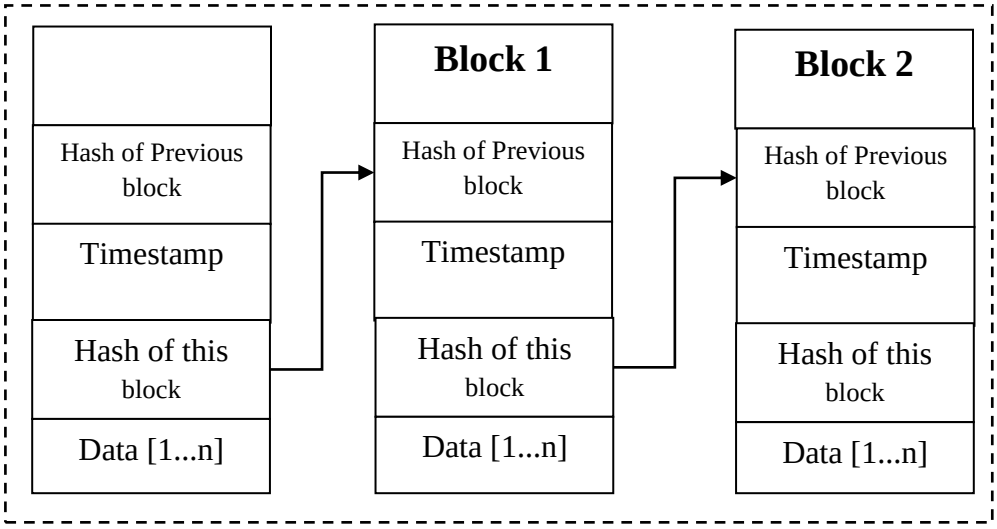


Figure 2: Blockchain Structure

Every block comprises of the hash of the previous block timestamp, hash for the preceding block and data set. These, along with the cryptographic algorithms helps in generating the hash for that particular block. Hashes resemble unique identifiers of the blocks present in the Blockchain. Private keys which depicts the digital signatures are allocated to the participants for carrying out data transaction activities within the network.

Following are the benefits made of Blockchain based architecture

1. Blockchain aids in effective data storage and its access from anywhere.
2. Blockchain employs the cryptography technique for safeguarding the storage and accessibility of inforamtion

3. Entire health information gets stored in a universal set of blockchain nodes which can be accessed securely.
4. The healthcare records can be accessed using the smart contracts, but with pre-set criteria**.**

3.2 Blockchain for E-healthcare Record

Blockchain depicts a peer-to-peer model for involving interaction between the Data owner and patient without letting any third party or an attacker to intrude. Entire collection of user information resides securely on the Blockchain. The personalized health information of patients' and info of the health care providers are put away on the Blockchain by the data owner which is secured and encrypted through a private key. Only authenticated users are allowed to access these health records thus maintaining the confidentiality and integrity of the data.

3.3 Features of the Blockchain

i. **Decentralization –** Unlike centralization, the block chain is based upon decentralization wherein the clinical info and other healthcare data is made securely accessible among various hospitals and medical practitioners.
ii. **Immutability –** Since there is safe and secure sharing of information pertaining to the patient, treatment and miscellaneous healthcare records, there are bleak chances of any threats and vulnerabilities. And hence audit-ability and variability can be avoided.
iii. **Identity management -** Each patient is allocated with a unique digital identifier that is stored on Identity Management Blockchain. Any Electronic health record or any other treatment info can be mapped against this unique digital identifier without altering it.
iv. **Access rule –** Using the self-executing codes on blockchain known as the "smart contracts", patients can grant permission to access their Access Rules medical records. It also helps in maintaining the audit trail of data access transactions.

3.4 Structure of SHA-256 Algorithm

SHA-256 Algorithms:

Input: Block of Message

Output: Fixed Size bits

Step 1: Pre-Processing

i). Indexing and Padding with 0's until data is a multiple of 512, less 64 bits.

Step 2: Initialize Hash Values

ii). Now create hash values

Step 3: Initialize Round Constants

iii). Similar to step 2, we are creating some constants. This time, there are 64 of them.

Step 4: Chunk Loop

IV). The following steps will happen for each 512-bit "chunk" of data from our input.

Step 5: Create Message Schedule

V). Copy the input data from step 1 into a new array where each entry is a 32-bit word

Step 6: Compression

vi). Initialize variables and set them equal to the current hash values respectively

Step 7: Modify Final Values

vii). after the compression loop, but still, within the chunk loop, we modify the hash values by adding their respective variables to them.

Step 8: Concatenate Final Hash

Viii). Combine them all together to get fixed length bit size.

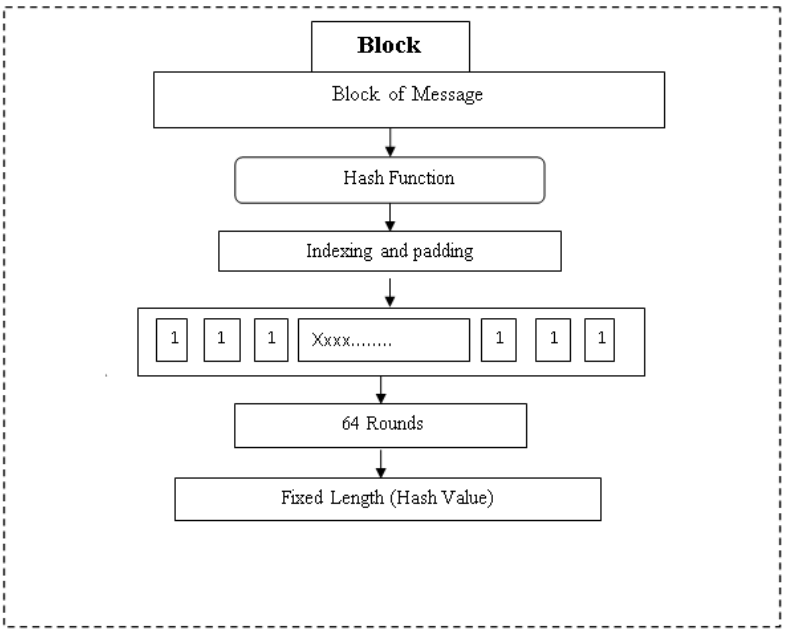


Figure 3: Hash Structure

This capacity of SHA-256 hash is discussed in this section. SHA-256 hashing calculation is briefly elaborated the official NIST standard. There are main two steps in the SHA-256 calculation. 1.) Pre-measure of the first messages by message cushioning and extending the directive for the round calculation. In cushioning, the bits are appended as per a few standards to achieve the length as a whole number of 512-cycle. The message block is divided into 512 bits. Thereafter, every 512 bits is extended to 64*32 piece for SHA-256 round calculation. The proposed system generates the hash for any N-bit message input once the message is split into blocks of 512-bits each. It then carries out the compression in order to produce a fixed length hash value as depicted in Figure. 3. A reconfigurable message module is created for generating such fixed bit blocks of messages.

4.RESULTS AND DISCUSSION

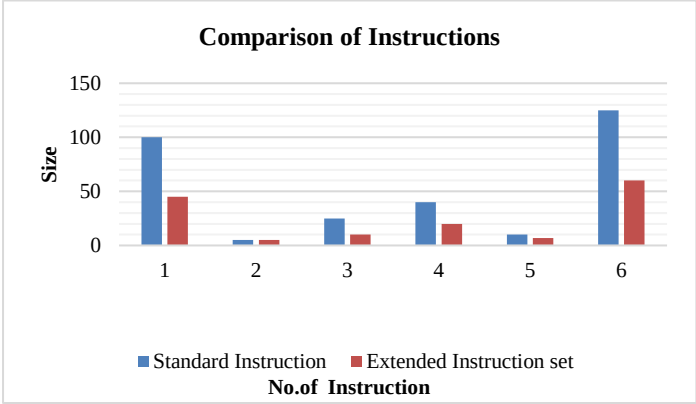


Figure 4: Performance of SHA-256

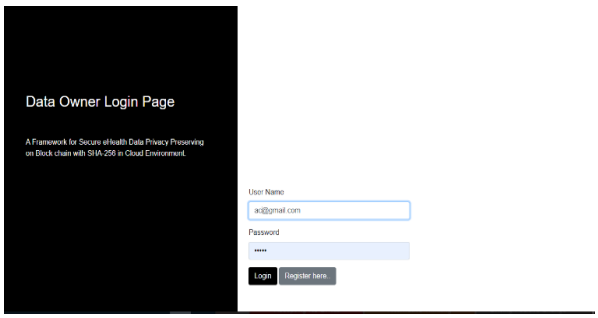
The research work proposes, a blockchain-based privacy-preserving architecture to elevate dynamic consent-based access control that can collect data for clinical data privacy. Table 1 presents the improvement in the processing size of SHA-256 through extra instructions. Apart from the hashing functions for SHA-256, additional instructions comparison are employed too. Important health info such as the name, address, age resemble the standard instructions to be transmitted from a clinical point of patients. Whereas the extended instructions comprises of a set of proposed health information that includes medications list, allergies, diagnoses, a clinical outlook to be exchanged amidst the data owners.The user can update both the standard as well as the extended instructions. Fig 4 illustrates that the proposed system is capable enough in handling both size of the data's privacy.

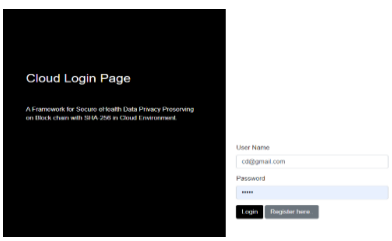
Numberof Instruction	**1**	**2**	**3**	**4**	**5**	**6**
Standard Instruction	100	6	25	40	10	125
Extended Instruction set	45	5	10	20	7	60

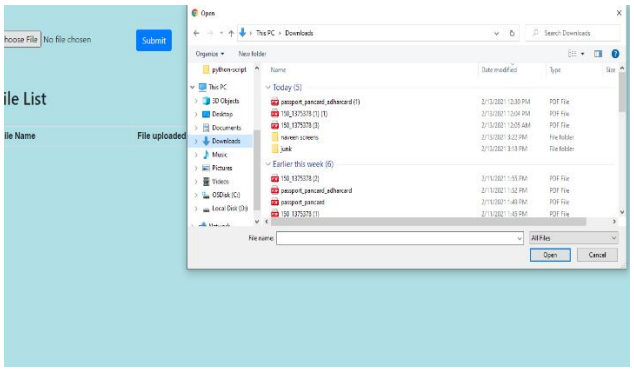
Table 1: Improvement in the processing size of SHA-256

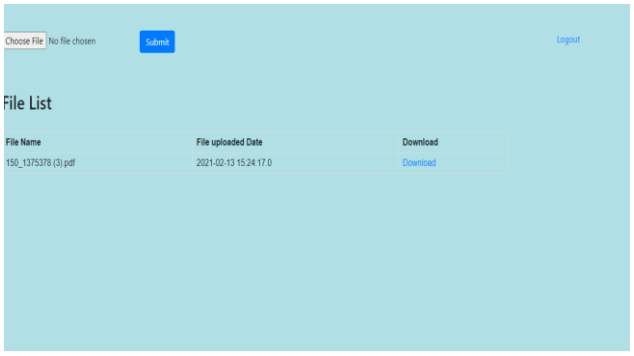
The output size of instruction has been minimized to a fixed length with the recommended system. The Blockchain offers a dynamic control of data access with SHA-256. The patient's record are reserved in a confidential manner which prohibits any other user to access it until the accessibility permission is granted by the patient. Also the patients can access their own records only with the help of the private key given by the blockchain and not without it. Patient's data that was collected and stored in blockchain was assessed in accord with the pattern of health records output over a certain duration. Comparing the performance parameters of the design to the prior implemented hash algorithm designs reveals that the former exhibits greater performance with respect to frequency of operation.

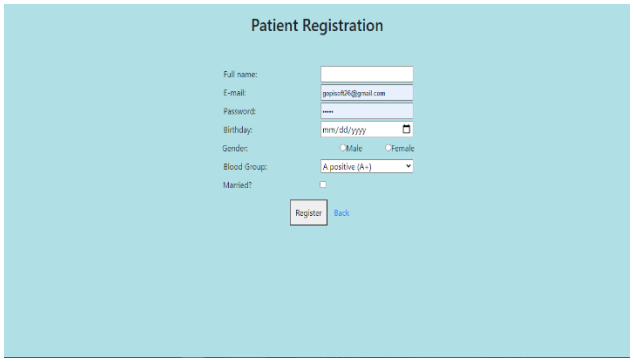
Simulation Results

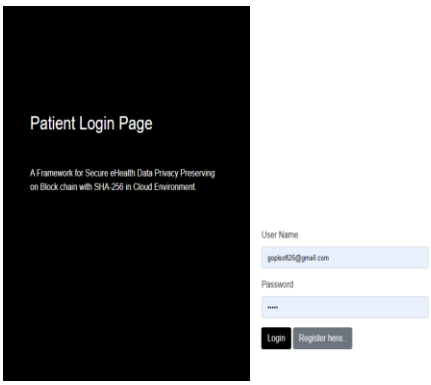












5. CONCLUSION

The blockchain technique has potential and visible significance in confronting the arduous issues prevailing in the medical sector. It emphasizes and ensures towards effectively achieving the

following parameters of security, integrity, decentralization, availability, and authenticity as it employs a general ledger and block-based framework. The research put forth a blockchain in accordance with SHA-256 engineering for generating fixed 256-bit message hash for an M-block message input (having any N-digit length) that preserves privacy. Towards this, a reconfigurable message module is created that generates fixed piece squares of messages. The ultimate target is to provide entire control and ownership to the patient so that they can further grant permission of who all can access their medical records thus building a controlled and confidential cloud environment. The research acclaims and achieves the aim of securing the EHRs (Electronics Health Record) by safeguarding and securing the patient's information through the means of blockchain and its significant features of interoperability and decentralization. This helps in concluding that the pioneering and elevating blockchain technique is ideal most for EHR and can offer momentous contribution in the future research and upliftment of healthcare domain.

REFERENCES

[1] Xiaoliang Wang, Liang Bai, Qing Yang, Liu Wang, Frank Jiang (2019), "A dual privacy-preservation scheme for cloud-based eHealth systems",Journal of Information Security and Applications, vol.47, pp. 132–138.

[2] H.S. Jennath1, V.S. Anoop, S. Asharaf (2020), "Blockchain for Healthcare: Securing Patient Data andEnabling Trusted Artificial Intelligence", International Journal of Interactive Multimedia and Artificial Intelligence, Special Issue on Artificial Intelligence and Blockchain, vol. 6, pp. 15-23.

[3] Froilan E. De Guzman, Bobby D. Gerardo(2019)," Implementation of Enhanced Secure Hash Algorithm Towards a Secured Web Portal", 2019 IEEE 4th International Conference on Computer and Communication Systems,IEEE.

[4] Al-Odat, Z., Abbas, A., & Khan, S. U. (2019). Randomness Analyses of the Secure Hash Algorithms, SHA-1, SHA-2 and Modified SHA. 2019 International Conference on Frontiers of Information Technology (FIT). doi:10.1109/fit47737.2019.00066

[5] Pham, H. L., Tran, T. H., Phan, T. D., Duong Le, V. T., Lam, D. K., & Nakashima, Y. (2020). *Double SHA-256* Hardware Architecture With Compact Message Expander for Bitcoin Mining. IEEE Access, *8, 139634–139646*. doi:10.1109/access.2020.3012581, IEEE.

[6] Jinhua Fu,[1,2] Sihai Qiao,[2] YongzhongHuang(2020)," A Study on the Optimization of Blockchain Hashing Algorithm Based on PRCA", Security and Communication *Networks* is an international journal publishing original research and review paper.

[7] Khuat Thanh Son, Nguyen Truong Thang, Le Phe Do, and Tran ManhDong(2018),"Application of Blockchain Technology to Guarantee the Integrity and Transparency of Documents", IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.12.

[8] AparnaKumari, SudeepTanwar, SudhanshuTyagi, Neeraj Kumar (2018), "Fog computing for Healthcare 4.0 environment: Opportunities and challenges", Computers and Electrical Engineering, vol., 72, pp. 1–13, Elsevier

[9] William J. Gordon, Christian Catalini (2018), "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability", Computational and Structural Biotechnology Journal, , vol. 16, pp. 224–230, Elsevier

[10] Maecus Christen, Bert Gordijn, Michele Loi, "The Ethics of Cybersecurity", The International Library of Ethics, Springer open, http://www.springer.com/series/7761

[11] Fengwei Wang1, Hui Zhu (2019),"Privacy-preserving Collaborative ModelLearning Scheme for E-healthcare", 2017 vol. 4, pp. 13. DOI 10.1109/ACCESS.2953495, IEEE Access.

[12] Mingwu Zhang, Yu Chen, Willy Susilo, (2020), "PPO-CPQ: A Privacy-Preserving Optimization ofClinical Pathway Query for E-Healthcare Systems", Transactions on Internet of Things, DOI 10.1109/JIOT.2020.3007518, IEEE.

[13] Christian Catalini, Joshua S. Gans, (2019), "Some Simple Economics of The Blockchain", National Bureau of Economic Research, NBER Working Paper No. 22952.

[14] "Blockchain in health care: hype, trust, and digital health", Analysis and Inter-pretationvol. 393, June 22, 2019.

[15] [15] H.S. Jennath1 *, V.S. Anoop2 , S. Asharaf, (2020), " Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence", Artificial Intelligence and Blockchain, International Journal of Interactive Multimedia and Artificial Intelligence, Vol. 6, Nº 3.

[16] TharukaRupasingae, Fradaburstein (2019),"Blockchain based Dynamic Patient Consent: A Privacy-Preserving Data Acquisition Architecture for Clinical Data Analytics", Fortieth International Conference on Information Systems, Munich.

[17] RenpengZoua, XixiangLv, (2020) "SPChain: Blockchain-based Medical Data Sharing and Privacy-preserving eHealth System", Journal of LATEX Templates.

[18] Bhavye Sharma, RajuHalder (2020.), "Blockchain-based Interoperable Healthcare UsingZero-knowledge Proofs and Proxy Re-Encryption",12th International Conference on Communication Systems & Networks (COMSNETS), IEEE.

[19] RaifaAkkaoui,Xiaojun He (2020), "EdgeMediChain: A Hybrid Edge Blockchain-BasedFramework for Health Data Exchange,Vol. 8, DOI: 10.1109/ACCESS.2020.3003575, IEEE.

[20] Dr. Rajashekhar M. Patil, RaghavendraKulkarni (2020), "Universal Storage and Analytical Frameworkof Health Records using Blockchain Datafrom Wearable Data Devices", Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020), Part Number: CFP20K58-ART; ISBN: 978-1-7281-4167-1,IEEE.

[21] Jigna J. Hathaliya, SudeepTanwar (2020), "An exhaustive survey on security and privacy issues in Healthcare 4.0", Computer Communications, vol. 153, pp. 311–335, Elsevier.

[22] ShekhaChenthara, Khandakar Ahmed (2019), "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing", vol. 7, pp. 74361-82,IEEE.

[23] Devika K.N.; Ramesh Bhakthavatchalu,(2019)" Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept", 2019 International Conference on Communication and Signal Processing (ICCSP), IEEE.

[24] Yang Lu (2018)," Blockchain: A Survey on Functions, Applications and Open Issues", Journal of Industrial Integration and Management, Vol. 03, No. 04, 1850015.

[25] RaffaeleMartino, AlessandroCilardo(2020),"Designing a SHA-256 processor for blockchain-based IoT applications",Internet of Things, Volume 11,Elsevier.

[26] Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019), "A survey of blockchain from security perspective", Journal of Banking and Financial Technology. Doi: 10.1007/s42786-018-00002-6, Springer.

[27] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018), "BlocHIE: A Blockchain-Based Platform for Healthcare Information Exchange", 2018 IEEE International Conference on Smart Computing (SMARTCOMP),IEEE.