Blockchain-based Privacy Preservation Framework for Healthcare Data in Cloud Environment

Dr. H. Shaheen[1], Dr. P. Mohamed Shameem[2], Dr. Brumancia Easpin[3]

[1,3]Faculty of Computing and Engineering, University of West London, RAK -UAE.
[2]Deputy Dean Department of Computing and Engineering, University of West London, RAK -UAE.
Corresponding Author Email: shaheen66@gmail.com

The extensive use of electronic healthcare systems (eHealth) already has significant advantages in the management of electronic based Health Records called EHRs for both Clinicians and Clients of hospitals. It does, however, present significant security issues. After a medical institution creates and redirects it to cloud servers, patients will not be provided with physical access to EHR but, if diagnosed, will be given access by the medical institution. The integrity of the EHRs is therefore difficult to maintain, especially in the event of medical error, as the cloud platform allows the health institute to manipulate outside EHRs to cover up health misconduct.

Keywords: Electronic based Health Records (EHRs), electronic healthcare systems (eHealth), cloud servers, Integrity.

1. Introduction

The advent of electronic healthcare systems (eHealth) has revolutionized the management of health records, transitioning from traditional paper-based systems to sophisticated electronic health records (EHRs). This shift offers significant advantages for both clinicians and clients, including improved accessibility, streamlined workflows, and enhanced patient care. However, as healthcare institutions increasingly adopt cloud-based solutions to store and manage EHRs, the security and integrity of these records have become paramount concerns.

The migration of EHRs to cloud servers provides numerous benefits, such as scalability, cost-effectiveness, and remote access. Despite these advantages, it also introduces vulnerabilities that can be exploited, leading to potential breaches of sensitive patient information. One critical issue is that patients typically do not have direct access to their EHRs stored in the cloud. Access is mediated by the medical institutions, which creates a dependency on these institutions to maintain the integrity and security of the records.

The integrity of EHRs is particularly at risk in situations where medical errors occur. There is a possibility that health institutions may manipulate EHRs to obscure instances of malpractice or misconduct. Such actions not only undermine the trust between patients and healthcare providers but also pose significant ethical and legal challenges.

Significance of the Research

- To make a review on different research contributions under the e-healthcare sector in Cloud, and also to define the clear problem statement on this aspect.
- To introduce a new secure friendly platform for healthcare data in the Cloud that is integrated with block chain technology.
- To protect the personal data of sensitive healthcare data in organizations when accessing in and out of them, preservation models are introduced to make this possible.
- To intake the need of key generation in the preservation model, and also to use the optimization concept for fine-tuning of this key.
- To introduce a new enhanced or improved bio-inspired model, which ensures the convergence speed and rate for the given optimization issue.To compare the proposal concept with other traditional methods and achieve better results than others with regard to certain performance analysis.

2. Literature survey

In 2019, Mubarakali et al. [1] created a "secure and efficient health record transaction using the block chain" (SEHRTB) algorithm enabling solving patient records database transactions among clients, clinicians, network operators, and organizations by maintaining confidentiality. The project gave the healthcare industry access to block chain technologies. Patients may easily manipulate and transfer their health records into cloud storage while retaining personal security, thanks to the efforts in medical services. It also offers a good technique for safeguarding client private information in intelligent health-care systems. Finally, a comprehensive research was conducted to assess the technique's cost-effectiveness.

In 2019, Cao-et al. [3] introduced a "Secure cloud-assisted eHealth solution" that employs blockchain based technology to safeguard outsourcing Electronic Health Records from tampering (blockchain-based currencies, e.g., Ethereum). The basic idea was that only authorized users may outsource EHRs, and that each operation on outsourcing EHRs was recorded as a transaction on the public block chain. As a result, after a transaction has been recorded in the block chain, the EHRs cannot be changed. As a result, any participant can confirm the integrity of outsourced EHRs by looking at the associated transaction. A good safety guarantee and high level of efficiency were shown in the proposed security analysis and performance evaluation.

In 2019, Nguyen et al.[4] proposed a revolutionary structure for sharing EHRs with a mobile cloud system incorporating the interplanetary file system Blockchain (IPFS). In particular, intelligent contracts have been used to provide a credible mechanism of access control to

make secure EHR exchanges easier between various patients and physicians. In a realistic situation, a mobile application leveraging Amazon's Cloud Computing and the Ethereum blockchain also was demonstrated to construct prototypes. The approach provides a practical way for transferring data to mobile clouds while also offering research evidence for securing health information data from potential attacks.

Haiping et al. [5] proposed a block chain-specified privacy approach in 2020 that enables secure medical information sharing across a large number of organizations. However, the report used negligible proofs to ensure the services of the medical researchers were connected, allowing researchers to check if patient data met specific research institute needs and did not compromise the patient's privacy.

Yue et al.[6] introduced a blockchain-based application architecture, which allows patients simple and secure possession, control, and sharing of their own data without compromising privacy and which offers a new possible solution for improving the artificial intelligence in the healthcare systems by retaining patient information. Under the target-centered process paradigm, patients owned and controlled their healthcare data. Furthermore, it is practical and easy to organize all types of personal heat data with a unified indicator centered scheme (ICS).

The challenges associated with the use of the block chain with IoT devices were addressed in 2019 by Dhar et al.[7]. We present a unique framework of modified block chain models that fit IoT devices and rely on the dispersed nature of the network as well as on other aspects of privacy and security. The security and privacy features of the suggested prototype is fully used with enhanced primitive cryptography. For IoT application data and transactions, the approaches discussed in this section are safe and anonymized across a blockchain system.

In 2020, Kuo et al. proposed an integrated level model learning framework, block chain model distribution, also a unique accord at a higher level approach to the Model Ensemble. In addition, a Hierarchical Chain (Hierarchical privacy conserving blockchain modelling) implementation example was built and corrective predictions and a state-of-the-art flattened network topical technique was used to evaluate learning iteration, and execution time.

Table I: Features & Challenges: Traditional techniques using block chain for preserving the privacy cloud in the healthcare system

Authors and [citation]	Methods	Features	Challenges
Mubarakali-et al. [1]	SEHRTB	Increased throughput Late latency reduction	No assessment of system feasibility
Omar-et al. [2]	MediBchain protocol	Satisfies all requirements Improved time consumption	There is a need to investigate interoperability between various healthcare process elements.
Cao-et al. [3]	TP-EHR	Ensuring security from various current attacks Demonstrated a communication and	More research is needed to look at the use of block chain methods to enhance the system

		computation overhead that is both practical and efficient.	of eHealth.
Nguyen-et al. [4]	IPFS	Reliable and fast medical data sharing	Efficient e-health record management is imperative on mobile clouds.
Haiping-et al. [5]	Proxy re-encryption based model	Minimal execution time Ensures confidentiality	No optimization on implementation process
Yue-et al. [6]	HGD architecture	Patients know who accesses their information Simple regulatory decisions regarding patient data collection and sharing	For good data management, further optimization concepts are required.
Dhar-et al. [7]	Secure Hash Algorithm	Very much secure Offers better privacy	Need consideration on DDOS attacks
Kuo-et al. [8]	Consensus algorithm	Minimal execution time Reduced over head	It must be evaluated in a real-world setting.

Problem statement

Table I describes the characteristics and problems of traditional techniques for preserving privacy in the healthcare system using the cloud. More study works on this subject are being utilised, and the approaches associated with their works are being presented, along with their benefits and drawbacks: With higher capacity, SEHRTB [1] has reduced latency. The system's feasibility will be estimated in future studies. The MediBchain protocol [2] reduces time consumption while meeting all requirements. However, there is a need to investigate interoperability between various healthcare process elements.TP-EHR [3] is resistant to a variety of existing attacks and has a low connection and processing overhead. Further research should be done on Blockchain technology for healthcare data. IPFS[4] uses medical data sharing securely and timely, although it will need to be considered in future mobile cloud management of e-health records. The proxy-based re-encryption architecture[5] guarantees confidentiality with little execution time, but during implementation, no refinement is made. The architecture of HGD is a mechanism that notifies patients who have access to their data and is able to make decisions straightforwardly on the storage, collection and sharing of data. More optimization principles are required, however, for good data management. In [7] the Secure Hash algorithm is absolutely secure and privacy-enhanced. However, DDOS attacks should be regarded. There is a low run-time and little overhead consensus algorithm used in[8], but it needs to be evaluated in the real world.

3. Research methodology

Through the development of the big data cloud and the medical information monitoring

systems, the sharing of electronic medical records across companies for improved medical treatment and progress has attracted great attention in the fields of academia and industry. The source of massive information, concerns about personal privacy, challenges to trust inherent in companies and complex regulation, mean the rapid progress of stymie health intelligence. In the process of sharing electronic medical records, blockchain has been widely used to address issues of privacy and sécurité. The objective of this paper is to provide a new decentralised block chain model for cloud applications. The major intention of this research is to preserve confidential health information on the block chain in order to make sure about the protection, integrity and transparency. Nevertheless, this is not sufficient under the scenario of the medical sector, since the local accessing of sensitive data is possible to encourage the attackers to carry out anomaly activities. Therefore to overcome these crises, a privacy preservation model will be deployed in healthcare data that ensures the security of healthcare organisations. In this work, the sensitive data will be subjected to below given methods:

- Information sanitization
- Information restoration

During sanitization, the original information gets transferred to sanitised data and during the restoration process, the original data will be recovered. Nevertheless in both cases, key generation remains a key aspect, as it is known only by an authorised person for accessing the data. Since the key generation is a complex process, it is planned to employ the optimization concept that tunes the key in an optimal manner, such that the security becomes much stronger to conserve the sensitive data. This work uses a hybrid optimization strategy that incorporates both the Elephant Herding Optimization (EHO) and Particle Swarm Optimization (PSO) algorithms for optimization. In reality, EHO [26] is a novel type of swarm-based metaheuristic search method that is based on elephant herding behaviour. PSO[27] is a computing method for solving problems by trying to improve the potential solution to a series of Quality criteria. The PSO is a computational method for resolving problems.

The original data is transferred to sanitised data during sanitization, and the original data is retrieved during the restoration phase. Nonetheless, key creation remains a critical component in both circumstances, as it is only known by an authorised person for accessing the data after the sanitization process, and the data will be stored in an encrypted state with a cloud data custodian.

An encrypted database could be part of a distributed storage system, such as a storage area network, that saves their records over numerous health storage devices. To properly maintain an encrypted database, access control policies that limit access to its contents in a form prescribed might be employed. Patients can submit encrypted PHRs to each PHR partition by encrypting them separately, such as personal information on I, (ii) medical data, (iii) health insurance data, and (iv) prescription details. The PHR client application also generates re-encryption settings, which are submitted to the SRS-Setup and Re-encryption Server (SRS). In case a user wishes to process some PHR, he must authenticate it first and then download it from the cloud. It should be observed that the user does not currently decode the PHRs, since the user must first receive the corresponding decryption parameter. The SRS

verifies whether the user was able to access the sector whereby the decoding settings were requested from the PHR owner's desired "access control list" called ACL. The SRS will produce and transmit the required parameters to the applicant user based on access rights granted in the ACL.

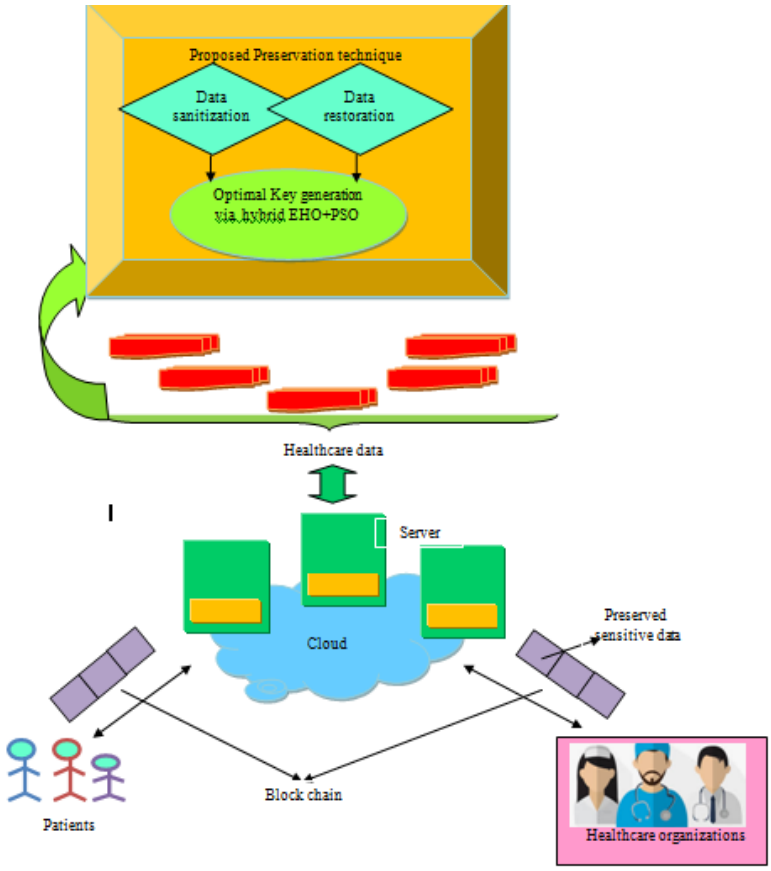

Figure 1: Block diagram of proposed privacy-preservation model in Healthcare using blockchain technology

DATA SANITIZATION:

The sensitive data is disguised during the sanitization procedure, thus avoiding leaking sensitive data on the cloud side. In a cloud environment, both routine and sensitive data are stored. For the sanitation process, a new meta-heuristic algorithm inspired by the distinctive social behaviour of the lion should be developed, which is based on the improved-lion crossover (CI-LA).

DATA RESTORATION:

Using the same key, the original data should be revived during the restore process. In this case, the ideal key generation is made to include change level, hiding rate and data conservation rate in the objective model. All contribute to the enhancement of cyber safety in the cloud.

BLOCKCHAIN IN HEALTHCARE:

The confidential material is destroyed during the sanitization procedure. A blockchain provides a secure platform for both storing and transmitting data to its transparency. Each block in the chain serves as both an independent unit with its own information and a dependent link in the collective chain, resulting in a connection regulated by users rather than a related party that stores and transmits the information. Blockchain can help with mobile health apps, monitoring devices, sharing and storing electronic medical records, clinical trial data, and insurance data management, along with other things. Despite the fact that there is currently minimal study on blockchain with healthcare, it is on the verge of revolutionising the industry; because of its decentralisation principles, blockchain can increase the availability and privacy of patient information, thus modernising the business.

A distributed ledger digital directory, or blockchain, is a growing chain of immutable, encrypted blocks that keeps record. The blockchain system operation is shown in Figure 2.Through Elephant Herding Optimization (EHO)/Particle Swarm Optimization (PSO), the pairs in a Health Care Networks are programmed to handle healthcare transactions in the way of historic blockchain in 130 healthcare programmes. There are one or more healthcare transactions per block inside the chain and validation data confirming the legitimacy of each and every transaction, as determined by peer to peer verification 120 (example: pairs 120A via 120N), also mentioned as pairs 120. People 120 function on the network peer-to-peer.

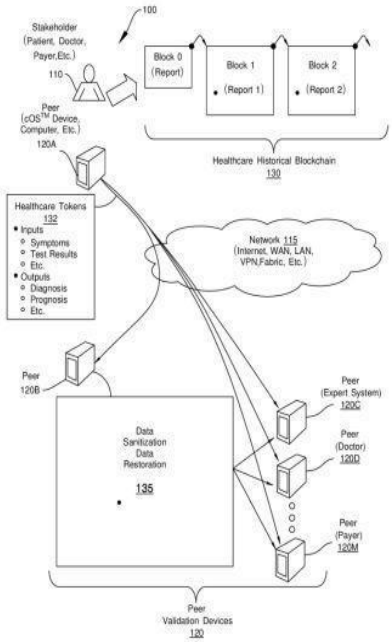

Figure 2: BlockChain System Overview [29]

This programme is modern and decentralised with a block chain of healthcare. Stakeholder 110 might be a patient and is an organisation that is involved in the life cycle of healthcare. On the other hand, Observer 110 can represent various entities. Observer 110 may be a

nurse, a physician, a care provider, a technician,a parent, a guardian, a broker or any other individual, each of 110 observers may have associated blockchain (HHBC) 130. For observer 110, HHBC 130 is a chronicle or header of health transactions (for example, public leader, private ledger, safe ledger, etc).

When a client experiences with the therapist, the doctor strives to comprehend the situation of the patient. Such information could be used to support a current health deal. The doctor takes one or more measures on the basis of information such as treatment, diagnosis, prognosis or other work. The actions of the doctor can be taken into account the results or results of the health transaction. The HHBC 130 may begin with an initial birth block or a birth block which contains information on the birth of the patient, based on information provided by the doctor (e.gClient data, Apgar score, attending physician etc.).It should be pointed out that every entity in the ecosystem disclosed has a separate block chain, as is the case with Optimization assisting a block chain-based privacy to secure health information. The ecosystem has a single chain covering all transactions. This ensures the sanitization of sensitive data in blocks with the best key.

The HHBC 130 Healthcare Historical BlockChain could be made up of any number of blocks. Note that each entity in the disclosed ecosystem has a separate block chain, just like Optimization, which helps to secure information about health in the block chain-based privacy. The ecosystem has a single transaction chain. This ensures that sensitive data are sanitised with the best key in blocks.

The token number 132 can be used to represent the numerous inputs and output activities of a specific patient. The health token number 132 shows the data on the nature of the healthcare transaction linked to statehood 110. The healthcare token number 132 will be followed by a defined, possibly standardised space. For example, the health care namespace should include standardised codes that categorise inputs and outputs (such as CPT, DSM ICD 10, ICD 9,and so on).

When 120 peers conduct or validate health transactions, they can provide a common reference framework or terminology using a shared healthcare namespace. This technique ensures that all 120 pairs or 110 stakeholders represent information as a result of consistent, repeatable, and verifiable completion of transactions.

Healthcare Tokens 132 can be packaged with a pair of 120A, which could be the medical EMR system, into one or more validating devices, such as 120B up to 120M. For example, the 132 tokens can be packed in JSON , XML or in other network 115 for user-friendly formats.

In the illustrated example, peer 120B acquires token 132 and seeks to build block 135 of validity, which comprises, amongst others, the transactions of healthcare represented by tokens 132. For instance, the transaction can have transaction-ID, digital signature validator, timestamp and so on.. The validity block-135 can have a validity token indicating the legitimacy of the patient/doctor interaction from the evaluator's perspective. The validity tokens might include "agree" else "disagree." Alternative information could also be included in a complicated token of validity, such as comments or recommendations for improving transactions; for example an alternative diagnosis.

Validity block-135 is generated by Peer 120B in accordance with the validity requirement. It's important to remember that other peers can handle the identical transaction at the same time. The validity criterion can be regarded as evidence of work for health transactions. In addition, additional criteria that must be satisfied before transactions are declared complete may be covered in the validity criterion.

As shown, Peer 120B constructs block-135 of validity for one or more transactions. A single patient visiting a doctor's clinic will be expected to have only one transaction in block-135. Block-135 of validity could include many transactions for a very active observer 110. (e.g., a hospital).

Validity block-135 is created through the combination of earlier block information from the HHBC 130 with extra data, which results in a link between validity block 135 and the blockchain. Time stamp, medical token-132, validator digital signature, and, most significantly, authenticity token all seem to be instances of additional transaction information. Until the convergent validity is passed, Peer-120B can compute a validity block-135, which is normally a combination of the validity block header plus transaction hash. In embodiments where a hash function examines block-135 validity, peer-120B, for example, can increase a value for nonces until a hash is created with the requisite proof of work characteristics, such as a number of leading null bits (e.g., Secure Hash Algorithm-256 and Scrypt, etc.).

Peer-120C is for data sanitization; during sanitization, the original data is transferred to sanitised data, and the original data is retrieved during the restoration phase.

Validity block 135 can be forwarded to additional peers 120 in ecosystem 100 once it has been appropriately calculated and/or approved by the peers. The HHBC 130 is then added to the Validity Block 135. As a result, Block-135 forms part of stakeholder 110's documented medical history. When additional peers 120 pick up and integrate Validity Block 135 into their own versions of the HHBC 130, it will be regarded as part of the HHBC 130.

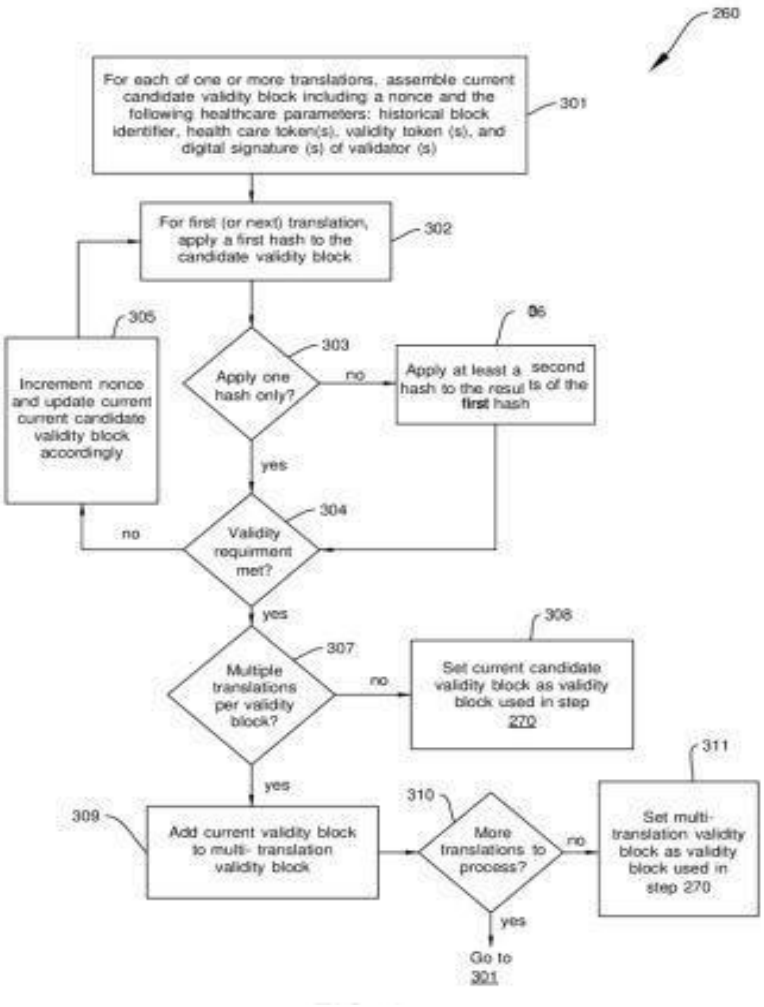

Figure 3 : Flow Diagram of Block Chain Processing[29]

A flow diagram depicting the processing phases is shown in Figure 3.

As will be discussed later, the disclosed approach allows simply one transaction per block or several operations per block to yield validity blocks. This flexibility acknowledges that processing multiple transactions for a single validity block may be useful and efficient in some instances, whereas completing a transaction may be more valuable in others. A client appointment, for instance, can result in many transactions for the patient or only a single transaction. In the first example, the treatment of all transactions simultaneously can help to reduce time and give a basis for combining several transactions in the HHBC data structure so that patient information can be provided without the requirement for a separate "visit" field.

In the second scenario, it could be helpful to access verification of each and every

transaction and create an HHBC validity-block for that patient rather than to wait for subsequent transactions, especially in case the in or out patient is unlikely to generate new operations for a long time to come. For example, a medical practitioner can take part in many of the transactions each day to help create a validity block every day that contains numerous transactions to be uploaded to HHBC.

In reference to FIG. 4, stage 301, the candidate's validity block with nonce and the following parameters is created. The following are the one or more healthcare tokens, one or more tokens (produced following a validator check the medical tokens) and historical block identifier. Step 302 hashed for the first time the applicant validity-block. Step-303 determines whether in the procedure for single hash should be utilised. If no, go to step-304 once the initial hash results are achieved with at least a second hash. Step 306 permits the approach to increase the processing quantity needed to provide evidence, if desired. The technique goes straight to step-304 if the outcome of step-304 is positive. The validity criteria are met by step-304 checks if the result of the step-302 or step-306 (if only one hash is utilised) fulfils the validity criteria. A typical test of work validity is, in this scenario, that a certain amount of leading zeros is included in the Hash result. However, many changes are practicable.If no, step-305 increases the numpty in the candidate's current validity block, and step-302 recalculates the accessing using a new nonce value.

The HHBC basically depicts the patient's lifetime care path. In order to establish the travel of the patient, each link in a chain might also be viewed, possibly using the browser. For longitudinal investigations, each subject might be examined individually or collectively. Patients who have been administered similar, if not identical, medicines might benefit greatly from such techniques. After the prescription is filled, the healthcare transactions can be reviewed to see whether there are any links between patient outcomes.

In the sense that secret information can be coded within many keys, the method presented might be deemed semi-secure. Explicit security, on the other hand, could be used to encrypt the HHBC and further protect it. Once the peer's identity has been established, the HHBC data can be decrypted as needed.

In response to interaction with healthcare the HHBCs are vivid, dynamic things that vary over time as validity blocks. In various embodiments one or more tendencies can examine the nature of the HHBC progression. HHBC, for instance, could be a leading symptom of health concerns with a change rate (e.g. monthly transactions). In addition, it is possible, throughout stakehood, to tie external elements (e.g. environmental circumstances etc.) to this data.

Another fascinating component of the concept divulged is that each and every validity-block in blockchain has data indicating every health transaction, that can be accessed via browser, as has already been indicated. In addition to the above specified time stamps and tokens, a wide range of health information may also be provided. In addition, linkages to EMRs or genetic data used in transactions could also be included in each transaction. Human readable pointers may include its name, handles of files, URIs, URLs or any kind of text addresses. In certain settings, documents can be identified by document object identifier.

In terms of the inventive subject matter, the validity token might also take on intriguing

elements. A couple function as validators in earlier circumstances for one or more medical transactions. As a transaction processor, tokens of validity can be collected from other validators. The FIG.1 may be referred by peer 120A to 120B, although a peer 120D validity token has been obtained. After the tokens or references have been received for the support of clinical data, Peer 120D produces the token to confirm its authenticity. In the processing of health care operations many organisations, probably non-affiliated companies, are involved in further minimising the risk of fraud.

The methods released focused on the HHBC also lead to exciting Internet-of-Things capabilities (IOT). Selected medical data guardians who may give access to the information with necessary authorised authorization can get clinical evidence produced by devices or services. Clinical data can then be referenced via transactions with in the HHBC blocks via appropriate signage for the designated medical data custodian site(s). The HHBCs could use this approach to obtain data for the entire health care cycle, adding information from the Internet of Things (personal area networks, sensors,ambient information, etc.), from the stakeholders in primary care(e.g., PCPs, etc).), stakeholders in secondary care (e.g. experts, etc.). This enables the care models (e.g., self-care, retail, remote care, etc.) to provide medical data guardians with evidence-based data while simultaneously providing HHBC with access to analysis data.

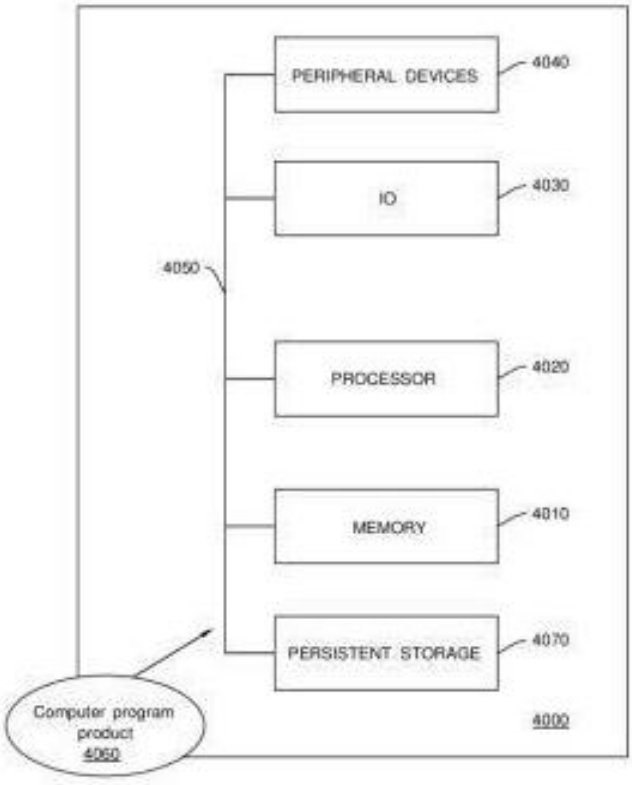

Figure 4: Computer system example 4000[29]

In accordance with the current project,FIGURE.4 showed an example of a 4000 computers (one or more components as shown in FIG. 3) which can be utilised to implement the instruction codes of a 4060 computer programme. Computer programme product 4060 consists of the executability of the code that is stored on an electrically readable medium that can be utilised to control one or more computers, for instance Computing Device 4000. An electrically readable medium is any of the non-transitory media that holds data and may be retrieved locally, sometimes globally, for instance, through a network connection.There may be a number of geographically scattered media, each of which is configured to store discrete stages of the programming language at multiple places and/or times. The computer system 4000 shown above performs several illustrative activities described through an executable instruction code, saved in a readable electronic medium. Typically, the executable code for controlling the execution of the actions specified herein would be implemented in software.

Performance Evaluation

We created a test environment for our protocol by creating applications in JAVA 1.8 and Solidity 0.4.11 on a machine with a CPU-3.30 GHz, Intel(R) Core(TM) i5, Windows 8 64-bit OS and 8 GB of RAM.

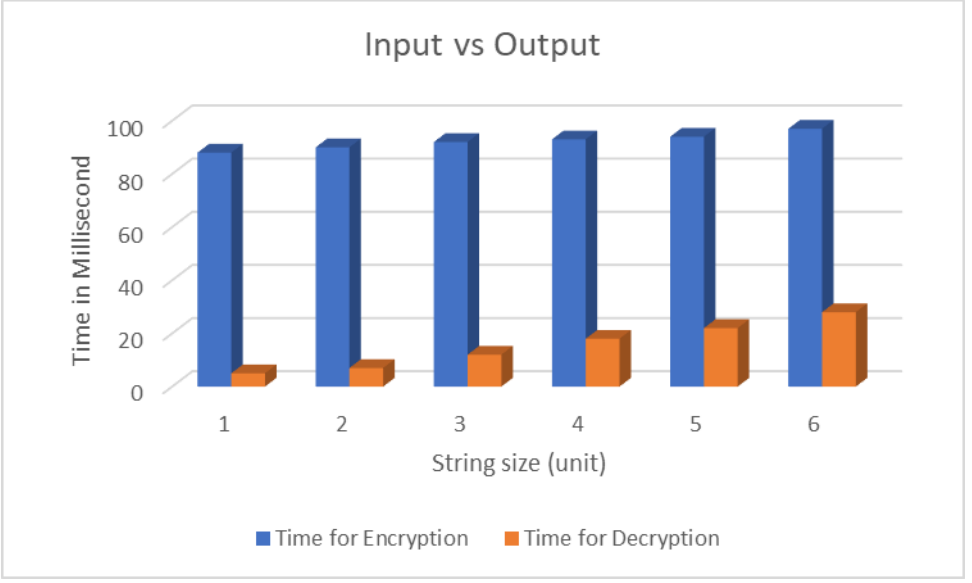

Figure 5: Generation of Input vs Output

EHO - PSO was used to create and retrieve the input and output, respectively.Input and output generation are separate processes. Encryption will occur during the input process and decryption will occur during the output process. FIG 6 shows how two processing procedures take vastly different amounts of time. Both the time and the length of the string rise as the length of the string grows longer, although encryption takes longer than decryption. It takes 80-90 milliseconds to encrypt and decrypt data.

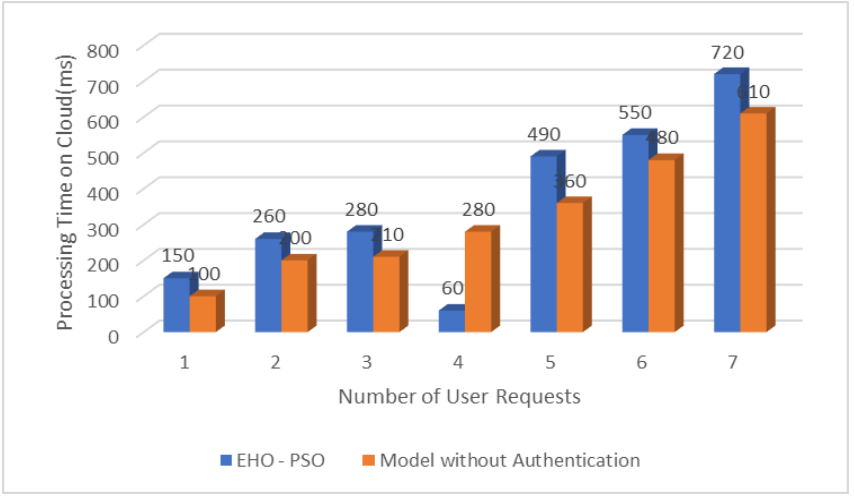

Figure6(a) : Cloud Time Consumption

We calculated the average cloud process time for multiple user access (FIG.6(a)). The user authentication strategy based on a smart agreement takes longer to perform user requests than the unauthenticated alternative. This is due to the amount of time you spend on user identification and access authentication. In the worst-case situation, however, the additional cost is only about 100 milliseconds, which is still small and acceptable in real-world scenarios.

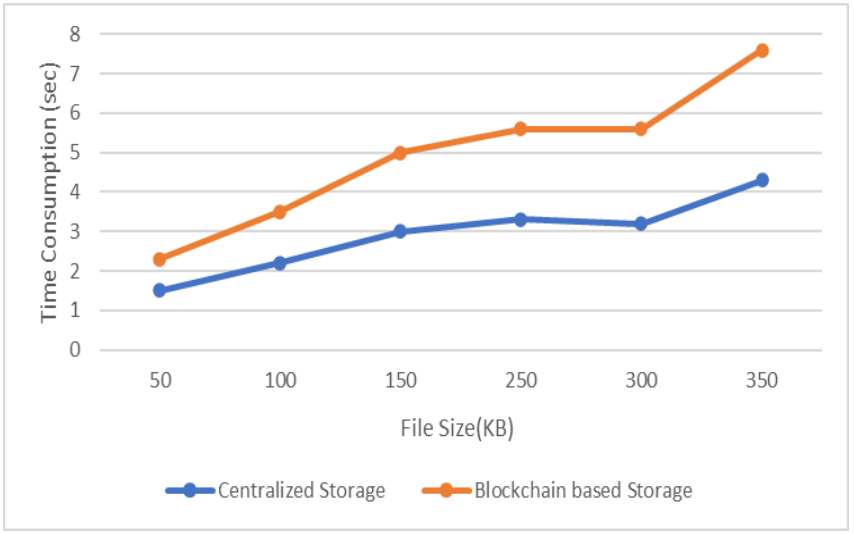

Figure6(b) : Cloud Storage using Blockchain

In our Electronic Medical Record, we look at our performance in terms of overhead communication for access to EHRs on cloud blockchain storage (FIG.6(b)).We examined the time required for the EHR to access data from the access request to data on a mobile phone.

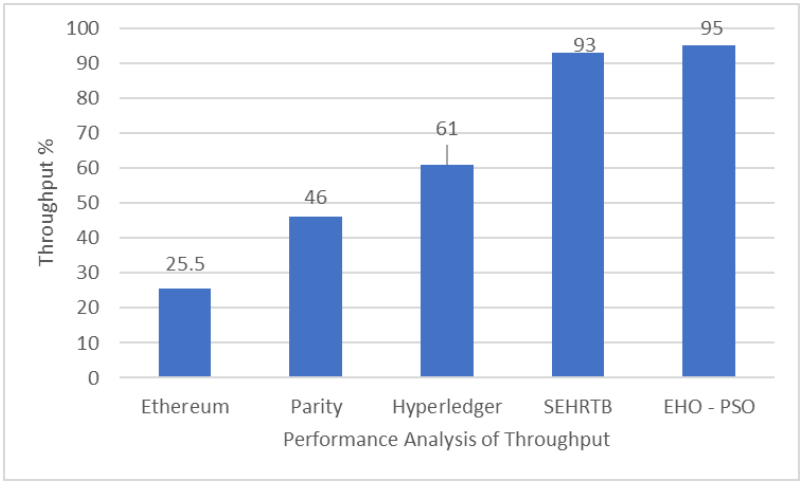

Figure: 7 Performance Analysis of Throughput

The proposed EHO - PSO is compared to existing Ethereum, Parity, and Hyperledger [30] approaches in terms of bandwidth, execution time and latency. Hyperledger outperforms Ethereum and Parity in the benchmarks[30]. It cannot, however, scale to more than 16 hubs. Hub errors are more forgivable with Ethereum and Parity. However, these systems are vulnerable to security attacks that split the block chain. The primary bottlenecks in Hyperledger and Ethereum are consensus procedures. Exchange marking using Parity, on the other hand, creates a bottleneck. Ethereum and Parity have considerable overhead cost in terms of memory and disc usage.

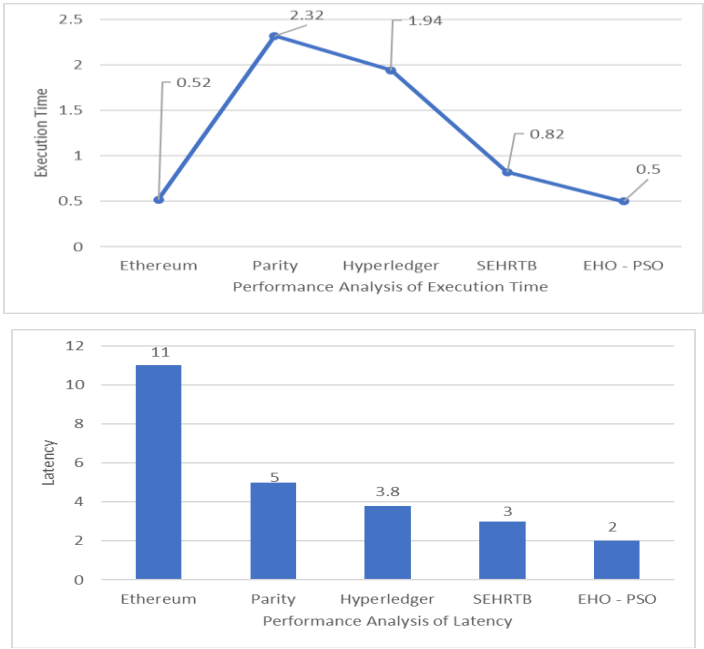

Figure : 8 Performance Analysis of Latency

In terms of execution time, Hyperledger is the closest technique [30]. However, it takes longer to share and retrieve data in the storage server. Efficient time is preserved for the execution of EHO-PSO algorithms. The EHO - PSO ensures the transaction of medical records and governs access to records that are kept and processed in the storage environment. The EHO - PSO reduces latency by 2.05 seconds, ET by 1.08 seconds and increases performance by 30.5 percent. Finally, it states that the suggested EHO - PSO method performs all other algorithms on all input and evaluation matrices.

Figure: 9 Performance Analysis of Execution Time

4. Conclusion

The technology of Blockchain enhances safety and accessibility and it may be used for a number of applications within the healthcare system, including storage and exchange of medical records and health care insurance and mobile apps as well as remote monitoring and clinical studies. There are presently limited studies on the use of blockchain in healthcare, but more study is being conducted on a regular basis.Blockchain is among the most active domains of computer research right now, and it has the potential to transform the health care hierarchy by allowing people to own their medical records and data. The performance of the Cloud-based solution to privacy protection in the health system based on the block chain will be simulated and an experiment carried out. In terms of costs (execution expenses, processing costs) and time for performance studies, the model suggested will be compared with various advanced models (computation time).

References

1. Azath Mubarakali, Subash Chandra Bose, Karthick Srinivasan, Amria Elsir & Omer Elsier," Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain", Journal of Ambient Intelligence and Humanized Computing, 2019.
2. Abdullah Al Omar, Md Zakirul Alam Bhuiyan, Anirban Basu, Shinsaku Kiyomoto, Mohammad Shahriar Rahman," Privacy-friendly platform for healthcare data in cloud based on blockchain environment", Future Generation Computer Systems, vol. 95, pp. 511-521, June 2019
3. Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, Ferrante Neri," Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain", Information Sciences, vol. 485, pp. 427-440, June 2019
4. D. C. Nguyen, P. N. Pathirana, M. Ding and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," in IEEE Access, vol. 7, pp. 66792-66806, 2019.
5. Haiping HuangPeng ZhuQinglong Huang, "A blockchain-based scheme for privacy-preserving and secure sharing of medical data", Computers & Security, vol. 99, Article 102010, First available on 1 September 2020, December 2020.
6. Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li & Wei Jiang," Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control", Journal of Medical Systems, vol.40, Article number: 218, 2016
7. Ashutosh Dhar Dwivedi, Gautam Srivastava, Shalini Dhar and Rajani Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT",Sensors, 15 January 2019, vol.19, 326; doi:10.3390/s19020326.
8. Tsung-Ting Kuo , Jihoon Kim, and Rodney A. Gabriel, "Privacy-preserving model learning on a blockchain network-of-networks", Journal of the American Medical Informatics Association, 27(3), 2020, 343–354 doi: 10.1093/jamia/ocz214.
9. Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, Douglas C. Schmidt," Analyzing the performance of a blockchain-based personal health record implementation", Journal of Biomedical Informatics, vol. 92, April 2019, Article 103140
10. Gautami Tripathi, Mohd Abdul Ahad, Sara Paiva," S2HS- A blockchain based approach for smart healthcare system", HealthcareIn press, corrected proof, Available online 19 November 2019, Article 100391
11. Ado Adamou Abba Ari, Olga Kengni Ngangmo, Chafiq Titouna, Ousmane Thiare, Abdelhak Mourad Gueroui," Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges", Applied Computing and Informatics, In press, corrected proof, Available online 22 November 2019
12. Tiago C. S. Xavier, Igor L. Santos, Flavia C. Delicato, Paulo F. Pires, Claudio L. Amorim," Collaborative resource allocation for Cloud of Things systems", Journal of Network and Computer Applications, vol. 1591 June 2020, Article 102592
13. Antonio Celesti, Davide Mulfari, Antonino Galletta, Maria Fazio, Massimo Villari," A study on container virtualization for guarantee quality of service in Cloud-of-Things", Future Generation Computer Systems, vol. 99, pp. 356-364, October 2019
14. G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarné," Using trust and local reputation for group formation in the Cloud of Things", Future Generation Computer Systems, vol. 89, pp. 804-815, December 2018
15. Yuan Tian, Mariya M. Kaleemullah, Mznah A. Rodhaan, Biao Song, Tinghuai Ma," A privacy preserving location service for cloud-of-things system", Journal of Parallel and Distributed Computing, vol. 123, pp. 215-222, January 2019

16. Xiaolong Xu, Shucun Fu, Lianyong Qi, Xuyun Zhang, Shancang Li," An IoT-Oriented data placement method with privacy preservation in cloud environment", Journal of Network and Computer Applications, vol. 124, pp. 148-157, 15 December 2018
17. Abdu Gumaei, Rachid Sammouda, Abdul Malik S. Al-Salman, Ahmed Alsanad," Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation", Journal of Parallel and Distributed Computing, vol. 124, pp. 27-40, February 2019
18. Pan Jun Sun," Security and privacy protection in cloud computing: Discussions and challenges", Journal of Network and Computer Applications, In press, journal pre-proof, Available online 4 April 2020, Article 102642
19. Hui Tian, Fulin Nan, Chin-Chen Chang, Yongfeng Huang, Yongqian Du," Privacy-preserving public auditing for secure data storage in fog-to-cloud computing", Journal of Network and Computer Applications, vol. 127, pp. 59-69, 1 February 2019
20. Nureni Ayofe Azeez, Charles Van der Vyver," Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", Egyptian Informatics Journal, vol. 20, no. 2, pp. 97-108, July 2019
21. Muneeb Ul Hassan, Mubashir Husain Rehmani, Jinjun Chen," Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions", Future Generation Computer Systems, vol. 97, pp. 512-529, August 2019
22. Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H. Deng," A blockchain-based location privacy-preserving crowdsensing system", Future Generation Computer Systems, vol. 94, pp. 408-418, May 2019
23. Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, Neeraj Kumar," A survey on privacy protection in blockchain system", Journal of Network and Computer Applications vol. 126, pp. 45-58, 15 January 2019
24. Hao Wang, Shenglan Ma, Hong-Ning Dai, Muhammad Imran, Tongsen Wang," Blockchain-based data privacy management with Nudge theory in open banking", Future Generation Computer Systems, In press, corrected proof, Available online 4 October 2019
25. Yun Chen, Hui Xie, Kun Lv, Shengjun Wei, Changzhen Hu," DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks", Information Sciences, vol. 501, pp. 100-117, October 2019
26. Wang, Gai-Ge & Deb, Suash & Coelho, Leandro, "Elephant Herding Optimization", DOI:10.1109/ISCBI.2015.8, 2015.
27. Junhao Zhang, Pinqi Xia, "An improved PSO algorithm for parameter identification of nonlinear dynamic hysteretic models", Journal of Sound and Vibration, vol. 389, pp. 153-167, 17 February 2017.
28. M. Marsaline Beno, Valarmathi I. R, Swamy S. M and B. R. Rajakumar, "Threshold prediction for segmenting tumour from brain MRI scans", International Journal of Imaging Systems and Technology, Vol. 24, No. 2, pages 129-137, 2014, DOI: https://doi.org/10.1002/ima.22087
29. https://patentimages.storage.googleapis.com/72/da/6f/95585e5e8709c3/US20150332283A1.pdf
30. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J (2018) Untan gling block chain: a data processing view of block chain systems. IEEE Trans Knowl Data Eng 30(7):1366–1385