Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.023930
Article

Tech Science Press

An Effective Blockchain Based Secure Searchable Encryption System

Aitizaz Ali[1], Mehedi Masud[2], Ateeq ur Rehman[3], Can Chen[1], Mehmood[4], Mohammad A. AlZain[5] and Jehad Ali[6,*]

[1]School of IT, Monash University, Subang Jaya, Sunway, Malaysia
[2]Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia
[3]Department of Biomedical Engineering, Foundation University, Islamabad, Pakistan
[4]Department of IT, University of Haripur, Haripur, KPK, Pakistan
[5]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[6]Department of Computer Engineering and Department of AI Convergence Network, Ajou University, Suwon, 16499, Korea
*Corresponding Author: Jehad Ali. Email: jehadali@ajou.ac.kr
Received: 27 September 2021; Accepted: 01 December 2021

Abstract: Security of Patient health records (PHR) is the most important aspect of cryptography over the Internet due to its value and importance preferably in the medical Internet of Things (IoT). Search keywords access mechanism is one of the common approaches which is used to access PHR from database, but it is susceptible to various security vulnerabilities. Although Blockchain-enabled healthcare systems provide security, but it may lead to some loopholes in the existing schemes. However, these methods primarily focused on data storage, and blockchain is used as a database. In this paper, Blockchain as a distributed database is proposed with homomorphic encryption technique to ensure a secure search and keywords-based access to the database. Moreover, the proposed approach provides a secure key revocation mechanism and update various policies accordingly. A secure patient healthcare data access scheme is devised, which integrates blockchain and trust chain to fulfill the efficiency and security issues in the current schemes for sharing both types of digital healthcare data. Our proposed approach provides improved security, efficiency, and transparency with cost effectiveness. We performed our simulations based on the blockchain based tool termed as the Hyperledger fabric and Origionlab for analysis and evaluation. We have compared our proposed results with the benchmark models. Our comparative analysis justify that our proposed framework gives improvement in security and searchable mechanism for healthcare system.

Keywords: Blockchain; security; energy optimization; encryption; homomorphic encryption; secure searchable encryption

1 Introduction

Patient health record system (PHR) is the significant and vital information related to a patient history and his/her details. Digital healthcare system is considered as the platform for transferring and receiving patient

health records. The existing digital healthcare systems rely on centralized servers which are more vulnerable to security breaches. The simplest solution is to integrate digital healthcare system to blockchain technology due to its wide application and security. More importantly blockchain provides peer-to-peer (P2P) and decentralized network system. In general, blockchain can be classified into three different categories, namely, private, public and consortium blockchain. It is a permissioned and consortium managed Blockchain, which means all peers are known to each other in the network. Moreover, it provides trust and security to all the parties involved. Hyper-ledger fabric is not domain specific, and it supports Java, Go, and Node.js for creating contracts and networks applications. There exist several searchable encryption (SE) methods to provide solution to the problems as mentioned above, but they are not as efficient regarding flexibility and anonymity [1]. SE can be categorized into different types based on several parameters such as single write (SW), multiple write (MW), single read (SR) and multiple read (MR) strategies. However, all SE approaches are not efficient when deploying to the cloud or server-based architecture systems. One of the most promising and secure approaches to solve these issues is secure searchable encryption (SSE), which enables the users to encrypt the data at their own side without the involvement of a third party. SSE can be divided into two groups, i.e., Asymmetric SSE and Symmetric SSE. Our proposed extended secure search-able encryption (ESSE) is derived based on the motivation of Ali et al. [1]. Cash et al. proposed the idea of Obvious cross Tag (OXT) searchable mechanism. The idea of OXT is to distribute all master keys among the users to take more advantages of the protocol. The problem with OXT is the key loss or collusion attack which makes it more prone to vulnerabilities [2].

Our proposed approach is more resilient to active collusion attack and key lost situations. Besides, our proposed method can be applied to different platforms, such as social media, fog computing and other Internet-of-Things (IoT) based applications. In this research paper we have proposed extended multi-users extended secure searchable encryption, which supports the participants to query securely against desired keyword search in the distributed ledger. The patient encrypts the data at the beginning and upload it to the blockchain. Our research method provides facility to the data owner once the data owner completes the encryption, and it will not be necessary to be involved another process until the patient needs policy revocation or deletion.

The rest of our paper is organized as follows. In Sections 1.1 and 1.2 we discuss the motivation of our proposed works and contributions. Section 2 provides literature review of the state-of-the-art schemes related to our proposed method. In Section 2.1, we discuss the Preliminaries Data, and Section 2.2 provides details of the Proposed Secure Search Algorithm. Moreover, in Section 2.3 Algorithm for Homomorphic Encryption is discussed. In Sections 2.4 and 2.5 the Proposed Access Control System Framework and the revocation policy for access control is illustrated. In Section 3, the experimental environment, parameters, and results are discussed. Finally, Section 4 concludes the paper and gives directions for future works.

1.1 Motivation

Cloud computing is a distributed and flexible storage platform that can be accessed anytime and anywhere on demand. However, data outsourced to the Cloud can be considered insecure as the data owner has no control over data which potentially leads to more security threats. Similarly, security is the primary concern when dealing with medical records in the Cloud. Digital health record is one of the most valuable records potentially stored in the Cloud, which makes it more attractive for threat actors to find vulnerabilities and expose digital health records into high risks due to their value and price in the market. Regardless of currently advancement in access control models and frameworks, there still exist lots of issues. These issues include absence of measuring granularity in authorizing [2], reliance on identity and role or purpose-based access control schemes [3]. The existing access control systems only relies on identity-based, role-based, or attribute-based methods. Through analysis and comparison, it is observed

that ABE (Attribute Based Encryption) is the optimal access control model among existing access models [4]. The Public-Key encryption does not fulfill the security requirements for attribute-based encryption.

In our proposed framework, we will use Attribute Based Signature (ABS) because it offers unforgeability and anonymity of the signer [1]. The significant difference in our proposed scheme and in the traditional one is the application of the computational trust value. The advantages of trust evaluation include:

1) Developing a novel lightweight consensus mechanism by combining with the BFT (Benzyntine Tolerance Protocol).
2) Measuring the trustworthiness of the user and prosumers before creating smart contracts and before initiating interactions among multi-parties.
3) It also helps in the accountability of the privacy and consent violation.
4) Moreover, it also helps to check the integrity before adding them to the genesis. Existing ABAC (Attribute Based Access Control) and RBAC (Role Based Access Control) system has low efficiency, and these are not machine intelligent [5].
5) To achieve more efficiency and security, we proposed an improved Access Control System with the combination of ABE, trust value and anonymity.

Our proposed approach will examine the parameters chosen, including user behavior, attributes, trust, unauthorized request, forbidden request, and range of specification. Users will be divided into different categories based upon the trust value such as very low, low, unknown, moderate, high, very, and high trusted users. A threshold value will be set if a user meets the threshold and satisfy the policy, then an access will be granted and vice versa.

1.2 Contributions

The contribution of our proposed approach is summarized as following:

A detailed literature review of the state-of-art of patient and participants detection based on encryption and security algorithm.

- A novel cross-domain and access control policies are proposed using homomorphic encryption.
- We proposed the idea and implementation of policies revocation, updates, delete and add using homomorphic encryption.
- We have achieved an optimum security and anonymous keyword search in the hyperledger fabric framework. Our proposed research method provide alternative private key in case of key is lost.
- We have achieved the efficiency as compared to the existing method as this method exhibit more communication and encryption cost as these method needs to encrypt the data.
- Our proposed methods provide more efficient solution to the users. In this section we have discussed the study and the loophole found in the previous research.

We have divided our literature review into two sections. First, we present a literature review of the current and previous methods used for PHR. The second part describes a review of access control model with their pros and cons.

2 Literature Review

Applications of blockchain in digital healthcare systems play an important role in healthcare industry. Self-generated data collection and verification processes in the correction and gathering of data from different sources, which are immutable, and tamper resistant against security breaches [6,7]. However,

one of the applications of blockchain is to provide distributed data, with redundancy and fault tolerance of the system. In this research, we have proposed a new access control method to achieve trust with secure access control using blockchain [8]. We have proposed a framework based on novel smart contracts using access control policy for participants to achieve privacy and security for patient data in the PHR system. Based on the literature, we have identified some specific research issues related to blockchain and PHR during access [9]. Our proposed research omits dependencies on the central authority and a single point of failure in the system. System security is achieved through immutable ledger technology which is also called blockchain [10]. For performance evaluation, we have used caliper for the proposed system. Moreover, we have used different scenarios through configuring block size, block type, endorsement policy and proposed optimization as evaluation metrics [11,12].

The performance measurement consists some of the parameters such as latency, throughput, and network security to achieve high throughput. In addition, in this research, we will prove the blockchain capability and importance in various aspects, which proves that it can be the subsequent technology for substituting current healthcare systems [13]. Honar et al. [14] proposed a system based on a patient monitoring system, relying on a patient centric agent in the major module of the system; they achieved better the security and privacy of the system through their simulations. They also developed a P2P-based records sharing protocol that support algorithms. Poslad and Poslad [15] highlighted recent issues and developed an access control policy for digital medical records through fine grained access control system.

Chen et al. [16] explored two methods for performance evaluation of the system of blockchain framework, optimizing performance with aggressive caching and configuration endorsement policy. The drawbacks of the existing methods and prototypes are their dependency on the centralized system. The dependency on a centralized system makes PHR and EHR systems more vulnerable to security breaches. Another issue related to cross domain authorization access approach [17,18]. The existing systems provides cross domain authorization access, but it lacks in providing security to collusion attacks and social engineering attacks. In the traditional symmetric key model encryption is carried out using symmetric key. Data owner divide data into some groups and then encrypts these groups using the symmetric key [19]. Users who have the private key can decode the encrypted data [20]. In this scheme, authorized users are listed in the ACL. The major drawback of this scheme is that the number of keys grows linearly as the number of data groups increased [21]. Also, if there is a change in the user and data owner relationship, then it will lead to affect other users in the ACL. In a nutshell, this scheme is not in practical use when dealing with different scenarios [9]. Different platforms and types of blockchain are used in healthcare industries [22]. In our proposed research we will be using Hyperledger fabric platform and permissioned blockchain technology. To win user trust, blockchain-enabled medical record sharing has been extensively discussed within the last two years [23].

2.1 Preliminaries Data

This section also describes the fundamental of the preliminary data, research findings and the importance of methodology.

Blockchain technology Uses of blockchain in digital healthcare systems which has an important role in the present digital health industry. Data distribution, redundancy and fault tolerance are such features which are supported by blockchain. Through this research, we have proposed a new access control method to achieve trust with secure access control using blockchain. Our proposed framework bypasses the dependencies on the CA and a SOP in the framework [24]. In our proposed framework immutable technology is used to achieve system security, and for performance evaluation we will use caliper. We will use different scenarios for our experiment through the variation of size of a block, creation time of a block, designed policy and proposed method for the evaluation of such metrics. These evaluation metrics contains delay, throughput, and PHR security to achieve optimize results [25]. Through performance

optimization the proposed system will ultimately improve the latency, security, and more trust. In alternate our proposed research will prove that the blockchain application and importance in digital healthcare system offers various aspects and justify that it can be the succeeding technology for substituting traditional health model [26]. The procedure for number of rounds and transaction of PHR is represented as below.

Where n is the number of neurons in previous layer. In the case of activation function, the most common one is hyperbolic tangent, but the selection is made in relation to expected output. For instance, one of such a function is hyperbolic tangent, which range is in $\langle 1, 1\rangle$ and the mathematical formulation of this is: General idea of neural network is based on the construction the grid of neurons composed as layers. There are three types of layers. The first one is called input, and it takes data and process them further. The next type is called hidden and combine intermediate layers. Their number may be different, in contrast to other types. The last one is known as output one, which return the results of classification. Highlight the cost of each method against quality of data [27,28].

2.2 Proposed Secure Search Algorithm

We have designed a novel secure searchable algorithm that offer the facility to the users to encrypt at their own side and upload it to the distributed ledger. Through our proposed extended secure searchable algorithm, a user can anonymously search the keywords using blockchain users API. In case a user lost the key he or she can revoke the policy and can request for the new key. It provides protection against active collusion attacks. The list of parameters used in our proposed framework are listed in Tab. 1 as following:

Table 1: List of notations and their explanation

S. No	Parameters	Details
1	BN	Blockchain network
2	CID	Clinician ID
3	LID	Lab ID
4	PHR	Patient health record
5	R^S	Ring signature
6	U^{name}	Username
7	P^K	Private key
8	R	Integer
9	N	Number of nodes
10	G	Bi-linear order group
11	P^1	Generator of addictive group 1
12	P^2	Generator of addictive group 2
13	iD	Bi-linear identifier
14	H	Homomorphic encryption
15	K	Degree of signature

Our proposed framework consists of four main participants' i.e., Admin, doctor, patient, and Lab technician. We have proposed delegation policies and algorithms for each node.

2.3 Algorithm for Homomorphic Encryption

We have designed a novel algorithm based on homomorphic encryption used for searching keywords in blockchain directory securely. The complete structure of this algorithm is described in algorithm 1.

Algorithm 1: Homomorphic Encryption

1. Initialize T←indexed by keywords W.
2. Choose key KS for PRF
3. Choose keys KX, KI, KZ for PRFFp
4. Zp and parse DB as (idi, Widi)di = 1
5. Init t←N
6. Ke←F (KS, w)
7. for id DB(w) do
8. Adjust counter c←1
9. Compute xid Fp(KI, id), z Fp(KZ, w||c)
10. y←xidz1e Enc(Ke, id)
11. Set xtag gFp(KX, w) xid and XSet XSet xtag
12. Append (y, e) to t and c←c + 1
13. end for
14. T[w]←t
15. end for
16. Set (TSet,KT) TSet.Setup(T)
17. let EDB = (TSet, XSet)
18. return EDB, K= (KS, KX, KI, KZ, KT)
19. Token Generation (q(w), K)
20. Client's input is K and query q(w = (w1,…, wn))
21. Computes stag←TSet.GetTag(KT, w1)
22. Client sends stag to the server
23. for c = 1, 2, … until the server stops do
24. for i = 2, …, n do
25. xtoken[c, i] gFp(KZ, w1||c)Fp(KX, wi)
26. end for
27. xtoken[c] (xtoken[c, 2],…, xtoken[c, n])
28. end for
29. T okq←(stag, xtoken)
30. return T okq
31. Searching Technique
32. ERes
33. t←TSet(Retrieve)(TSet, stag)

2.4 Proposed Access Control System for Framework

We have proposed a novel secure access control system which is based on attribute based for our proposed framework.

The PHR access control system has four types of users, including admin, patients, clinicians, and laboratory staff. The precise execution of admin in a blockchain network is shown in Algorithm 1. The enrolment certificate of an admin is requested from the certification authority. The admin has full access to the system, including write, read, update, and removal of participants. Patient can revoke and update the policy against each PHR [29]. A user whose attributes matches the access control policy is allowed to access the PHR otherwise no access is allowed to a PHR.

2.5 Proposed Revocation Policy

Due to the collusion attack our system will monitor the user behavior and interaction with the system. To remove the colluded node or user we have proposed the revocation policy. The shared key in the blockchain access control policies is revoked and new share key among the shareholder will be created. Update policy and proposed algorithm to implement the update policy we have proposed our novel algorithm called as update policy. In case of the data owner lost the private key so the update algorithm can be used to request for new private key.

3 Proposed Methodology

However, to provide solution to the challenges and issues highlighted in the literature in multi-site clinical systems, we have proposed a blockchain-based access control and secure searchable encryption system for keyword searching, storing, retrieving, and sharing of personal healthcare data using homomorphic encryption. We model our system on Hyperledger Fabric and used homomorphic encryption for security and secure search. Our proposed algorithm is embedded in smart contracts for blockchain technology, and we have described all our novel algorithms function in detail. The parameters and the notations that contain in the blockchain are described in the tabular form as described in Tab. 1. In this section, we describe the design of our proposed system: setting up the network, installing private channels, and writing channel-specific smart contracts. In Fig. 1 we have provided the simulations results for the comparative analysis of keyword search using homomorphic encryption and the confirmation time in seconds. From the results and comparative analysis, it is clear that our proposed framework performs better than the benchmark models [30]. As, the confirmation time is considerably very less in case of our proposed framework so ultimately the throughput of our proposed framework is more as compared to the benchmark models [31].

3.1 Experimental Results and Discussion

In our proposed research Hyperledger caliper will be used as a tool for the blockchain network. It can support different hyperledger frameworks, e.g., fabric, composer, saw tooth, iroha, etc. We have implemented the homomorphic encryption for our encryption and decryption to provide secure searchable encryption mechanism. In this proposed research, caliper tool play an important role in the verification and execution of the system as well as various parameters. The parameters include latency, throughput, encryption and decryption time, computational cost. In our experimental setup the configuration parameters are modified as per assessment, such as block size, block time, endorsement policy, channel, keyword search, update policy, add policy, delete policy, and revoke policy. Our simulation setup configurations consist of the following specifications: Dataset size: 100 number of blocks + PHR Hardware: GPU Enabled System Software: Ethereum, Hyperledger Fabric Parameters: Block Height, Number of blockcs, No. Transac, No. PHR, Delay, signature creation, security (Execution time of

Policies) and Cost (Execution Time of Blocks), Number of simulations : Number of Test performed on single data set. Number of rounds or transactions: 5000.

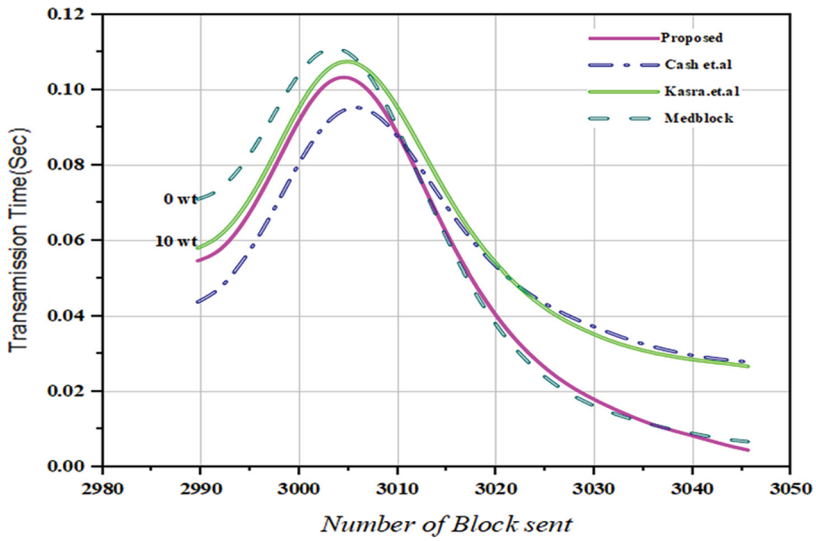

Figure 1: Comparative analysis of the proposed framework versus benchmark models based on the number of blocks sent versus transaction time per seconds

Experiment 1: We run our first experiment up-to 5000 rounds, and we evaluated our results based on the number of the personal health records sent *vs.* number of rounds. Experiment 2: We run our experiment 2 for 9000 number of rounds we evaluated the efficiency of the proposed system according to the number of PHR sent versus number of rounds or transactions.

In Fig. 1, we have explained the number of blocks sent from one domain to another domain and number of transactions. It is shown in the figure that the number of transactions which mean the number of patient health record (PHR) or electronic health record (EHR) sent per round. We run our simulations for 3050 rounds and evaluated the number of patient health record sent. We did comparative analysis with the benchmark models such as Medrec and Med block. In Fig. 1, we have described the simulations results based on our proposed policies. We have proposed access control policies for our proposed framework using homomorphic encryption and pseudo random algorithms. We have evaluated our proposed access control policies against number of execution time and number of access policies.

Tab. 2 provides the predictive valued based on the proposed techniques i.e., homomorphic encryption. We have predicted the number of false positive and false negative. We can see from Tab. 2 that our proposed method provides more accuracy as compared to the previous benchmark models. In Tab. 2 FPR stands for false positive rate, FNR stands for false negative rate, ACC for accuracy and FDR stands for false detective rate.

Table 2: Performance analysis of the number of people and accuracy

Number of people	FPR	FNR	FDR	ACC
100	0	0	0	1
200	0	0.022	0.025	0.96
300	0.002	0.029	0.035	0.87

The number of transactions sent per second. From the simulations we can see that our proposed framework is much better than the benchmark models. We have achieved more efficiency as compared to the benchmark models.

In Fig. 2, we have explained the simulations results based on two parameters i.e., number of attributes and search times in seconds. We have compared our proposed framework with the benchmark models.

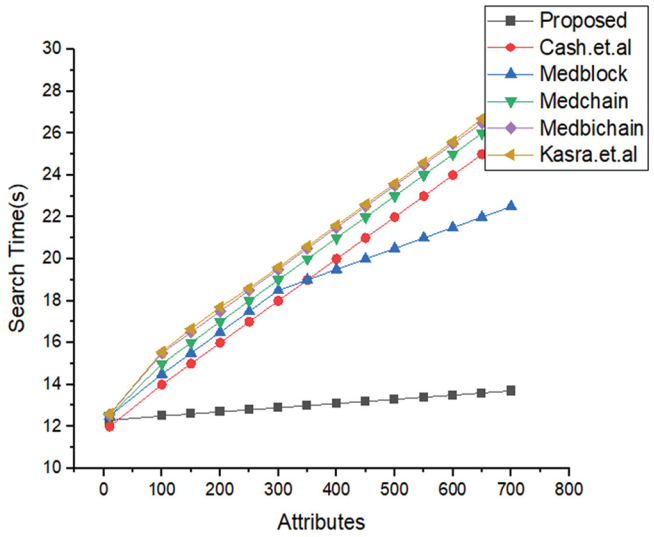

Figure 2: Comparative analysis of the proposed framework versus benchmark model based on the number of attributes versus search time

We did experiments on the policy revocation, policy creation and add policy. It can be easily seen that the authorization policy took less time as compared to the authentication policy and delegation policy. These simulations in Fig. 3 justify that our proposed access control policy provide more security and less computational cost respectively. Fig. 4 describes the simulations results of number of users classified based on their interaction and behavior with the proposed framework. In Fig. 4, we have explained the comparative analysis based on the number of attributes and the time complexity. For the same dataset we run our experiments on our proposed framework and we compared the efficiency and number of packets sent to the nodes. It can be easily observed that the number of PHR sent to the base station are more in number in case of our proposed framework.

In Fig. 4, we have shown the simulation results for the number of attributes taken and time complexity. Fig. 4 represent the number of attributes and the time-complexity in micro-seconds. The number of attributes ranges from 1 to 8. The value of time complexity starts from 0 to 1200. In case of benchmark-based models it is very less comparatively to our proposed scheme. Hence, we have improved the efficiency 1.9 times as compared to the benchmark models. In Fig. 5, we have achieved the throughput and efficiency using hyperledger fabric tool. Through our proposed framework, we have used the optimum block height to achieve the maximum throughput. The Gas is the space or the unit during the transactions used. We have evaluated these experiments with the number of rounds as the input and the number of packets sent to the cluster as the output. From these simulations it is clear that we have achieved the maximum efficiency and throughput for the same dataset used in the literature. i.e., Medrec and Medblock, which we call as the benchmark models.

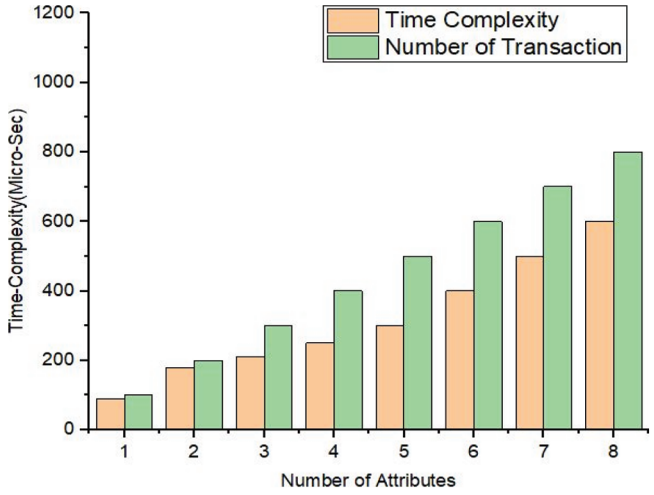

Figure 3: Performance analysis of encrypted number of attributes *vs.* time complexity

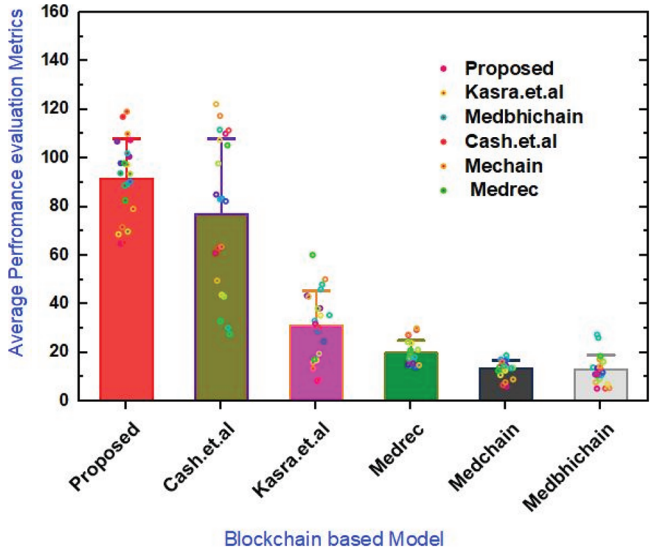

Figure 4: Average performance analysis of the proposed framework and benchmark models

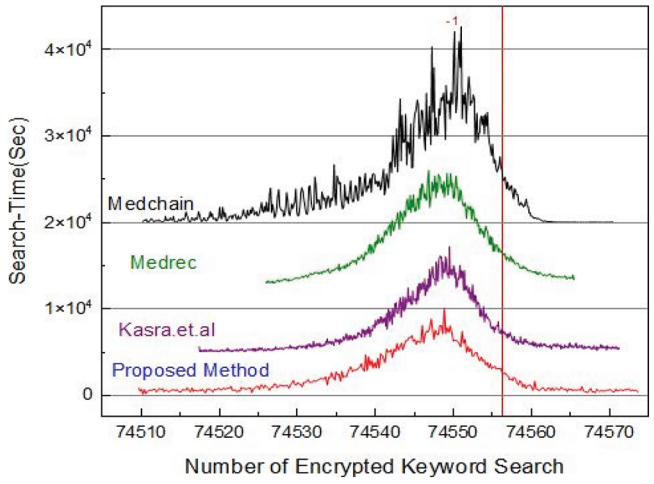

Figure 5: Average performance analysis of the proposed framework and benchmark models

Fig. 5 provides the comparative analysis based on the number of keyword search and the time for searching the keywords. We have designed a novel algorithm for the transaction of personal health record using blockchain technology. Through PHR proposed algorithm the user can encrypt the clinical and patient data and upload it to the distributed ledger. Our proposed algorithm eliminates the involvement of blockchain manager. In Fig. 6, we have carried out the comparative analysis of our proposed framework and benchmark models. The performance is carried out based on search time of keywords and number of attributes. From Fig. 6, we can see that with an increase in the number of attributes the will it takes time to search a keyword. It is obvious from Fig. 6 that our proposed framework performs better than the benchmark models. The efficiency of our proposed framework is more as compared to the benchmark models.

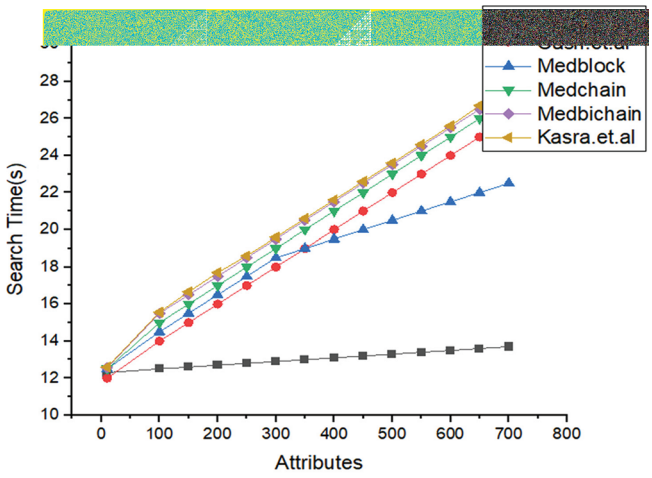

Figure 6: Comparative analysis of our proposed framework versus benchmark models

4 Conclusion

We have implemented a novel extended approach of homomorphic encryption in digital healthcare system leveraging blockchain technology which provides secure keyword search facility at the users end. Our research supports immutable, tamper resistant, and deliver secured data, which results in reduction of security breaches to the healthcare data. Furthermore, our novel mechanism allows blockchain users to encrypt data at their own premises and upload to the distributed ledger for record purpose. Users can securely search the desired health related data without decryption based on homomorphic SSE. Our technique provides resistance to active collusion and replay attacks due to the flexible policy revocation. In addition, Blockchain technology also supports distributed data, redundancy, and fault tolerance features for digital system. Hence, In this paper, current challenges and problems in the literature faced by the digital healthcare industry were solved. We proposed a framework and algorithm that enables access control policy for users to achieve privacy and security for patient health data in the PHR system. The proposed method provides more Independence to the users, and it support flexibility and fine-grained keyword search. We have justified our scheme and research algorithms as well aspolices through simulations on hyperledger fabric tool. We have used Pycharm tool for data analysis. With our proposed method, we have improved the security and anonymity as compared to the benchmark models such as Medrec, Medchain and Medbichain respectively.

Acknowledgement: Authors would like to thank for the support of Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Ali, M. Naveed, M. Mehboob, H. Irshad and P. Anwar, "An interference aware multi-channel mac protocol for wasn," in *Proc. of the 2017 Int. Conf. on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*, Karachi, Pakistan, pp. 1–9, 2017.

[2] A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud *et al.,* "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, no. 16, pp. 2034, 2021.

[3] Y. Arfat and R. A. Shaikh, "A survey on secure routing protocols in wireless sensor networks," *International Journal of Microwave and Wireless Technologies. Technol*, vol. 6, pp. 9–19, 2016.

[4] S. Idrees, M. Nowostawski, R. Jameel and A. Mourya, "Security aspects of blockchain technology intended for industrial applications," *Electronics*, vol. 10, pp. 9–51, 2021.

[5] A. Sharma, R. Sarishma, N. Tomar, Chilamkurti and B. G. Kim, "Blockchain based smart contracts for internet of medical things in e-healthcare," *Electronics*, vol. 9, pp. 1609, 2020.

[6] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, pp. 943–961, 2019.

[7] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, pp. 13951–13976, 2016.

[8] J. Liu, X. Li, L. Ye, H. Zhang, X. Du *et al.,* "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *Proc. of the 2018 IEEE Global Communications Conf. (GLOBECOM)*, Abu Dhabi, United Arab Emirates, pp. 9–13, 2018.

[9] F. A. Khan, M. Asif, A. Ahmad, M. Alharbi and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustainable Cities & Society*, vol. 55, pp. 102018, 2020.

[10] Z. Mushtaq, S. S. Sani, K. Hamed, A. Ali, S. M. Belal *et al.,* "Automatic agricultural land irrigation system by fuzzy logic," in *Proc. of the 2016 3rd Int. Conf. on Information Science and Control Engineering (ICISCE)*, Beijing, China, pp. 871–875, 2016.

[11] H. Kim, S. H. Kim, J. Y. Hwang and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *Ieee Access*, no. 7, pp. 136481–136495, 2019.

[12] S. Chakraborty, S. Aich, and H. C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. of the 2019 21st Int. Conf. on Advanced Communication Technology (ICACT)*, PyeongChang, Korea, pp. 260–264, 2019.

[13] A. D. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, pp. 326, 2019.

[14] H. P. Honar, M. Rashid, F. Alam and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, no. 3, pp. 772, 2021.

[15] T. T. Kuo and L. Ohno-Machado, "Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," Preprint Arxiv:1802.01746, 2018.

[16] X. Chen, J. Ji, C. Luo, W. Liao and P. Li, "When machine learning meets blockchain: A decentralized, privacy-preserving and secure design," in *Proc. of the 2018 IEEE Int. Conf. on Big Data (Big Data)*, Seattle, WA, USA, pp. 1178–1187, 2018.

[17] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. K. R. Choo *et al.,* "Decentralized authentication of distributed patients in hospital networks using blockchain," *Ieee Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.

[18] A. Yazdinejad, R. M. Parizi, A. Dehghantanha and K. K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks," *Ieee Transactions on Network, Science and Engineering*, vol. 8, no. 2, pp. 1120–1132, 2019.

[19] J. Ali, G. M. Lee, B. H. Roh, D. K. Ryu and G. Park, "Software-defined networking approaches for link failure recovery: A survey," *Sustainability*, vol. 12, no. 10, pp. 42–55, 2020.

[20] J. Ali and B. H. Roh, "An effective hierarchical control plane for software-defined networks leveraging topsis for end-to-end qos class-mapping," *Ieee Access*, vol. 8, pp. 88990–89006, 2020.

[21] G. Tripathi, M. A. Ahad and S. Paiva, "S2HS-A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, pp. 100–391, 2020.

[22] M. Pourvahab and G. Ekbatanifard, "An efficient forensics architecture in software-defined networking-iot using blockchain technology," *Ieee Access*, vol. 7, pp. 99573–99588, 2019.

[23] C. Lazaroiu and M. Roscia, "Smart district through iot and blockchain," in *Proc. of the 2017 IEEE 6th Int. Conf. on Renewable Energy Research and Applications (ICRERA)*, San Diego, CA, USA, pp. 454–461, 2017.

[24] M. C. Lacity, "Addressing key challenges to making enterprise blockchain applications a reality," *Mis Quarterly Executive*, vol. 17, pp. 201–222, 2018.

[25] A. Devibala, "A survey on security issues in iot for blockchain healthcare," in *Proc. of the 2019 IEEE Int. Conf. on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, pp. 1–7, 2019.

[26] K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *Proc. of the 2016 IEEE 18th Int. Conf. on High Performance Computing and Communications; IEEE 14th Int. Conf. on Smart City; IEEE 2nd Int. Conf. on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, NSW, Australia, pp. 1392–1393, 2016.

[27] J. Sengupta, S. Ruj and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, pp. 102–481, 2020.

[28] M. Dabbaghjamanesh, B. Wang, S. Mehraeen, J. Zhang and A. F. Kavousi, "Networked microgrid security and privacy enhancement by the blockchain-enabled internet of things approach," in *Proc. of the 2019 IEEE Green Technologies Conf. (GreenTech)*, Lafayette, LA, USA, pp. 3–5, 2019.

[29] P. Singh, M. Masud, M. S. Hossain and A. Kaur, "Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid," *Computers and Electrical Engineering*, vol. 93, pp. 107–209, 2021.

[30] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Sensing as a service model for smart cities supported by internet of things," *Transactions on Emerging Telecommunication Technologies*, vol. 25, pp. 81–93, 2014.

[31] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, pp. 25, 2010.