Electronic Health Records System Using Blockchain Technology

Q.H. Hasan
Information Technology Department, Altinbas University, Istanbul, Turkey.
E-mail: Hasanqasim86@gmail.com

Ali A. Yassin
Computer Science Department, College of Education for Pure Sciences, Basrah University, Iraq.
E-mail: aliadel79yassin@gmail.com

Oğuz ATA
Information Technology Department, Altinbas University, Istanbul, Turkey.
E-mail: oguz.ata@altinbas.edu.tr

Received May 17, 2021; Accepted August 18, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI05/WEB18248

Abstract

Blockchain technology is one of the most important and disruptive technologies in the world. Nowadays the healthcare center needs to share patient databases over all departments of the healthcare centers. Although, electronic healthcare records overcome several problems compared with manual records, but still suffer from many issues such as security, the privacy of patient data overall as we should transfer over a database from a central database to a decentralized database. In this paper, we proposed a good security system to manage the data of patients based on blockchain technology and a decentralized database. Depending on decentralized database and blockchain. Our proposed system provides the secure exchange of patient data, reliability, and high efficiency in sharing data during transaction data network equivalence checking to perform this validation of patient information in the blockchain and healthcare centers.

Keywords

Electronic Healthcare Record, Blockchain, Privacy, Security, Decentralized Database.

Introduction

Medical services and health care have become a focus of attention in the modern era of human care through some of the healthcare technologies available on the internet, mobile

application and others (A. Celesti, A. Ruggeri, M. Fazio, A. Galletta, M. Villari, A. Romano, 2020). Healthcare centers adopt centralized servers to access data, ease of designing the network, facilitating communication with the patient and another department (S.M. Alkhushyni, D.M. Alzaleq, and N.L.G. Kengne, 2019). The revolution in health care depends on the ability of the patient to interact with the new technology (T. Benil and J. Jasper, 2020). Healthcare origination suffers from how data is shared on their platforms under Health Insurance Portability and Accountability (HIPAA) that is increasingly a trust for everyone in the digital healthcare world using a special key within Blockchain and decentralized database between main components like (P. Mukherjee and D. Singh, 2020), (D.C. Nguyen, P.N. Pathirana, M. Ding, A. Seneviratne, 2019). Blockchain technology can access also share data at the best level from service with the principle of storing electronic health care records. (G. Capece and F. Lorenzi, 2020) E-health supports perfect diagnostic through patient health data participation through via communication with doctor healthcare centers (Q. Feng, D. He, H. Wang, L. Zhou, and K.K.R. Coo, 2019). Modern Technology offers the shortest path to obtain deep diagnostic to analyze patient's data and can predicate of the regular and chronic disease such as debates (A. Sardi, A. Rizzi, E. Sorano, A. Guerrieri, 2020). The security of patients' is one of the most challenges faced by the healthcare system (K. Renuka, S. Kumari, and X. Li, 2019). The blockchain can provide exchange data between healthcare centers securely (V.M. Harshini, S. Danai, H.R. Ush, M.R. Kounte, 2019). Decentralized database and reliable system (without relying on any third party) (K. Renuka, S. Kumari, and X. Li, 2019). Trust relation among healthcare centers is established by mathematical methods and cryptography technologies instead of semi-trusted central institutions based on the blockchain can mitigate the limitation of the single point of failure (see figure 1) (V. Patel, 2019). Blockchain technology contains mainly elements: decentralization, transparency, constant, independence, open-source, and anonymity depending on the advantage blockchain can trustworthy of the transactions processed in the system (Y.S. Jeong, D.R. Kim, and S.S. Shin, 2019). Blockchain technology could be supported in healthcare by integrating the entire real-time clinical data of a patient's health (S. Wang, Y. Zhang, and Y. Zhang, 2019). The main work principle of our proposed system is to exchange data between environment components (blockchain, database, patients, doctors, healthcare centers) based on a secure decentralized database (X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, 2020). A centralized database has many features like protected patient data, preserve the privacy of patient (G. Yang and C. Li, 2018), the contribution of the proposed system as follows: -

1. On the healthcare side:-

- The doctor and patient can use the system in easy ways.
- Each patient can register in one healthcare center to obtain e-healthcare records and then he uses them in other healthcare centers based on blockchain and decentralized database.
- The patient can use the proposed system anytime/anywhere to gain medical information over-communicates with the doctor.
- Decentralization when compared database centralized model with blockchain no longer needs to rely on the semi-trusted third party.
- Autonomy each patient holds all rights to e-health record data when sharing with the doctor's securely (N. Rifi, E. Rachkidi, N. Agoulmine, and N.C. Taher, 2017), (Blockchain in health, 17).

2. On the information security side:-

- Our proposed system can protect the patients' data save in a secure decentralized database.
- The transferring data between healthcare centers perform securely.
- We are building our system based on blockchain, decentralized database (DDB), Advanced Encryption Standard (AES), hash function, hash MAC and key management (F. Tang, S. Ma, Y. Xiang, and C. Lin, 2019), (S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C.M. 2019).

The organization of the paper, in the second section, highlights the electronic health records related work using blockchain technology. The third section will explain the modus operandi and architecture of our proposal system submitted to healthcare records using blockchain. The fourth section will show the results and explains the Performance Comparisons with the related schemes while in the final section we provide the conclusion and references.

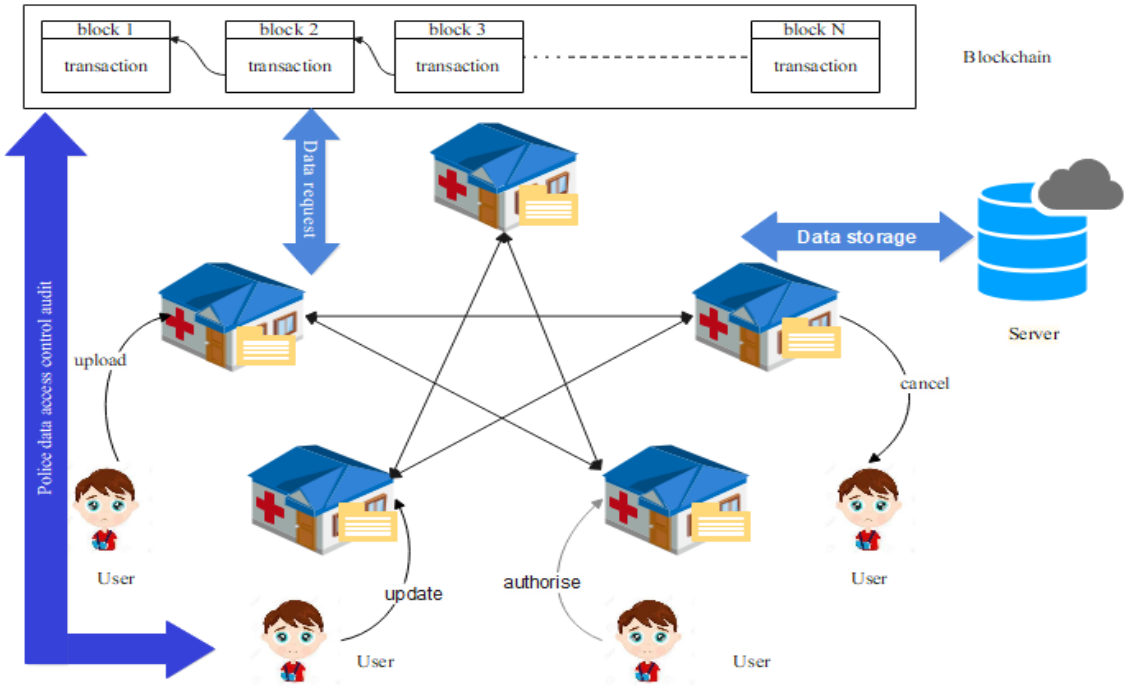

Figure 1 The healthcare system based: blockchain

Related Work

Table 1 The base contributions and constraints dependent on blockchain EHRs

Paper	Main contributions	Constraints
Peterson et al. (2016)[20]	1. A new consensus of the algorithm is designed to manifest interoperability to support interoperability of data. 2. It requires designing of the networks for the objective of altogether effective data sharing with syntax, data, phrases and security.	1. This consensus cannot be submitted on account of communication programmatically.
Dan et al. (2016)[17]	1. By using a smart contract to automatically verify access compatibility to reduce manual operation. 2. The strength to effectively publish smart contracts during any registered process.	1. Potential actual identity and personal information inflation.
Sun et al. (2018)[21]	1. It shares data of securely to several sublimation organizations. 2. Easier it makes users locate data of EHR. 3. Sharing EHR through securely on-chain and off-chain distributed storage model. 4. It shuns the storage determines the blocks	1. It is very hard build fully-trustworthy third parties to store data of EHR. 2. The patient cannot control right on data.
Patel (2018)[11]	1. Only the list of entities applying in the block can provide best protection and privacy. 2. Access of data is validated with approval patients.	1. Depend on the existence imaging centers while likely obtrusive together the hazard of sly offensive.
Zheng et al. (2018)[22]	1. It reduces the burden in blockchain storage from GB for continuous dynamic high-frequency data.	1. It is highly hard to provide trustworthy with third part to cloud storage platform. 2. It cannot protect data privacy in order to the data buyer should obtain sensitive data from plain texts.
Liu et al. (2018)[23]	1. Significant reduction in data leakage and a way to reduce the treasury burden inside the blockchain. 2. Access of data is limited on the cloud. 3. Cloud storages perform data access procedures only if the request prediction is identical.	1. It is not easy to build completely reliable third parties. 2. It may not be able to resist the huddly attack by cloud servers and users.
Juneja and Marefat (2018)[24]	1. Patients have the right to control their own data. 2. Data stored securely can be retrieved with accuracy in increasing the cardiac arrhythmia classification. 3. An increase in the accuracy of the SDA retraining operations faster uses the data site blockchain.	1. They have serious threats to attack their harmful data with manipulation and tampering.
Nguyen et al. (2019)[5]	1. Every single point cannot be failed. 2. High storage rate increases. 3. Further improvement in data retrieval rate using hash distribution.	1. Issues are that sensitive information can be leaked due to malicious attacks from employees.
Wang et al. (2018)[13]	1. It gave up relying on the third centralized authority. 2. Highly productive data usage and minimum cost compared to cloud storage units. 3. It cannot take out each piece of information from folders. 4. Only files can be downloaded encrypted by smart contract.	1. IPFS does not supply a powerful confidentiality cryptographic algorithm interface for user-uploaded files.
Seol et al. (2018)[25]	1. Control flexible and accurate access to files. 2. XML can powerful encryption of selective encrypted data.	1. Users can be subject to attacks without identifying identification.

The Proposed Scheme

We present the electronic health records system for managing patient's cases (see Figure 2). The main components of our work are: Patient (P_i), Health Care Center (HCC_i), Authenticated Server plays role of Blockchain Center (BC), and Doctor (D_i). Each P_i needs to register his sensitive data in the certain HCC_i which generates an electronic health record (EHR_i) connected with patient. These components exchange their information in securely manner. Additionally, the proposed scheme consists of two main phases: Registration Phase and Process Phase. Table 2 explains the main symbols are used in our work.

Table 2 The main Symbols

Symbol	Description	Symbol	Description
BC	Blockchain center	T_h	Hash function
HCC_i	Health care center	T_E	Symmetric key encryption
EHR_i	Electronic health record	T_D	Symmetric key decryption
D_i	Doctor	$T_{\oplus}$	XOR function
P_i	Patient	AES	Advanced Encryption Standard
SI	Sensitive information	Ph_i	Phone number
ID_i	Identity	BOD_i	Birth of day
PW_i	Password	TK_i	SMS token
Pn_i	Patient name	equ	Equation
ShK_i	Sharing key between blockchain and healthcare centers		
$ShKP_i$	Sharing key between patient and healthcare centers		

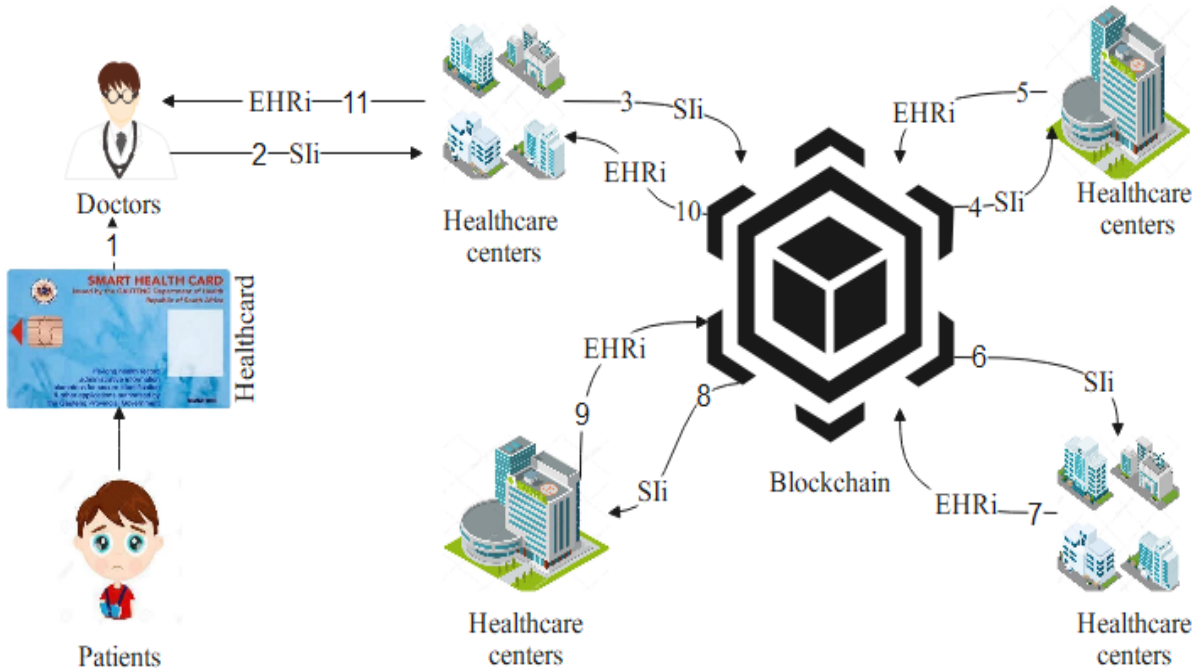

Figure 2 The proposed EHR system using blockchain

1. Registration Phase

Based on the current phase, the main two components (HCC_i, P_i) need to register in BC and HCC_i, respectively. Furthermore, BC and HCC_i compute some parameters used in the next phase to exchange information in securely way (see Figure 3).

Step1: Each of BC and HCC_i have agreement key to generate shared key ($ShK_i \in Z_n^*$); where $n = p * q$ and p, q are prime numbers.

Step2: HCC_i registers main information (ID_{HCC}) for exchanging information in the next phases.

Step3: The patient (P_i) should be registered the major information SI_i ((Identity (ID_i), Patient Name (PN_i), Phone number (Ph_i), Birth of Day (BOD_i), Password (PW_i), etc.) in the health care center(HCC_i)).

Step4: Upon receiving the major information from P_i, HCC_i generates shared key $ShKP_i \in Z_n^*$ and electronic health record ($EHR_i =< SI_i, ShKP_i >$). EHR_i can be health card, electronic file, and others. Then, HCC_i sends EHR_itoP_i.

$$P_i \leftarrow HCC_i: EHR_i$$

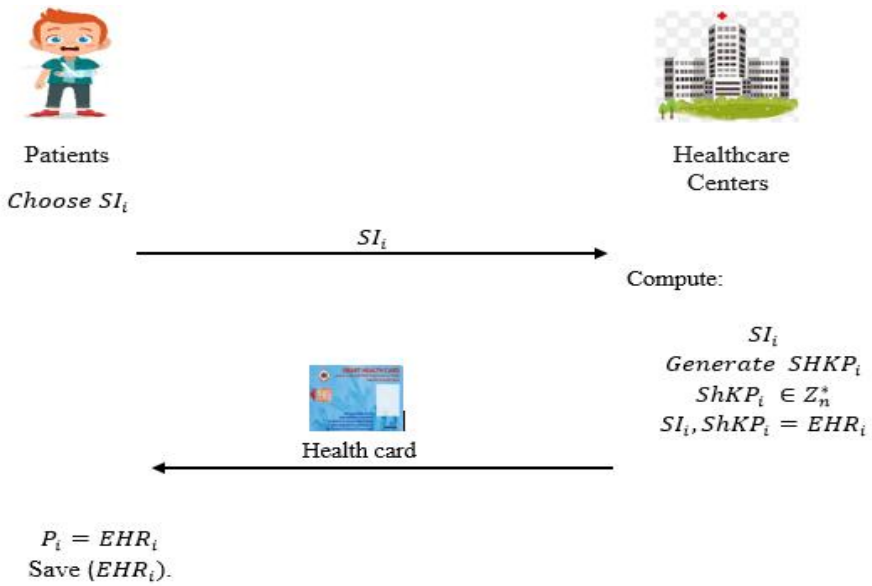

Figure 3 The Proposed Registration Phase

2. Hospitality Phase

In this phase, there are many steps that should be implemented between components as follows:

Step1 (Verification Patient). The doctor checks the validity of patient's health card based on SMS token (TK_i) which receives to patient's phone number (Ph_i). D_i Submits TK_i to

HCC_i to compare with original token and tells D_i about authority of P_i when the result is match. Figure (4) explain the verification phase.

$$D_i \xleftarrow{healthcard} P_i \dashleftarrow equ \qquad (1)$$

$$HCC_i \xrightarrow{TK_i} Ph_i \dashleftarrow equ \qquad (2)$$

Step 2 (Retrieval Information from other Communities)

- The D_i needs to retrieve medicine information (EHR'_i) of P_i from HCC_ior other health care center (HCC'_i).
- To get medicine information (EHR'_i), HCC_i sends request ($E = Enc_{ShK_i}(ID_{HCC}, ID_i)$) to$BC$.
- Upon receiving EfromHCC_i, BC decrypts E based on $Dec_{ShK_i}(E)$to detect one or more health care center HCC'_irelated with BC.
  - BCSends request to HCC'_i for retrieving EHR'_i as follows.
  - BCComputes$Ch = h(ID_i, ShK_j)$ and sends $< Ch, ID_i >$toHCC'_i.
  - HCC'_iComputes$Ch' = h(ID_i, ShK_j)$and compares $h' = Ch'$, if the result is true then HCC'_i sends sensitive information (EHR'_i) to BC based on $EHR''_i = EHR'_i \oplus ShK_j$ of patient.
- BC computes EHR''_i=$Enc_{ShK_i}(EHR''_i \oplus ShK_j)$ and sends back EHR''_i to HCC_i.
- HCC_i Retrieves EHR'_i by decrypting $Dec_{ShK_i}(EHR''_i)$.

Now, the doctor (D_i) has received all necessary information to diagnostic the case of patient without needing to makes quires to patient.

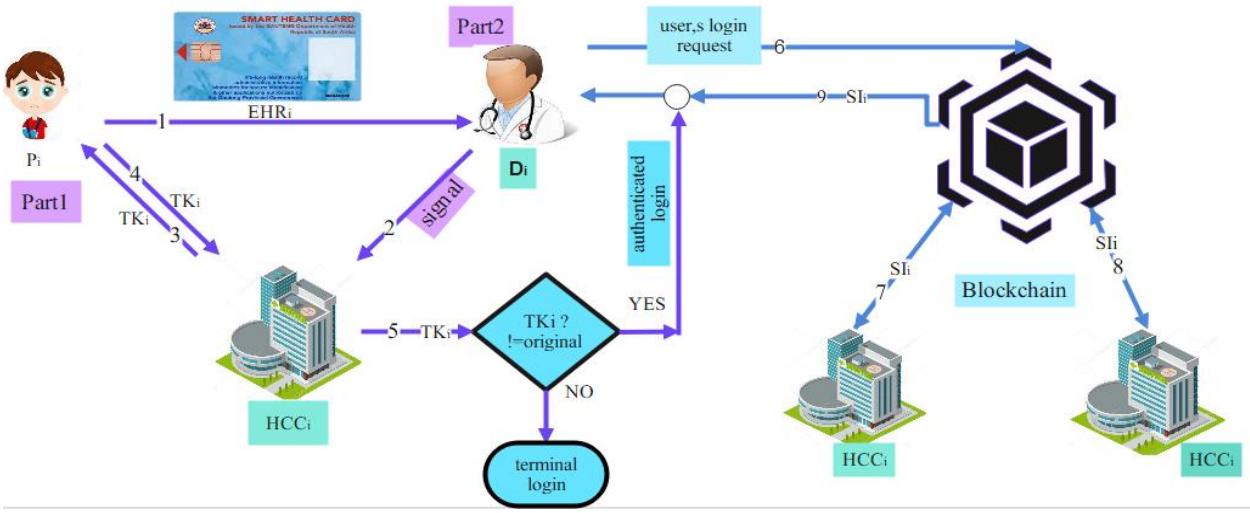

Figure 4 Explains the verification hospitality phase

3. On-Line Hospitality Phase

In this phase, our proposed scheme offers to patient to login the system via mobile application without needing to go the hospital or health care center. The following steps demonstrated the working of current phase:-

1. The P_i enters his user's identity (ID_i) and password (PW_i), encrypts $E' = Enc_{ShKp_i}(PW_i)$and then sends <E', ID_i>toHCC_i.
2. Up on receiving information, HCC_i computes $PW_i' = Dec_{ShKp_i}(E')$. After that, he checks the authority of P_i based on the result of comparing between PW_i, PW_i' . If the result does not hold, HCC_i terminates. Otherwise, HCC_i sends the TK_i via SMS to ph_i.
3. P_i Receives e-token via his phone number TK_i' and sends second factor $h = h(TK_i'||ShKp_i)$ to HCC_i.
4. The HCC_i checks the second factor of P_i by comparing $h$with$h(TK_i||ShKp_i)$, if the result is equal, HCC_i ensures from authority of P_i. Then, HCC_i applies the same pointesin the Step 2 inside Hospitality Phase.

There are many actions for login between P_i and HCC_i about online as following steps (see figure 5):

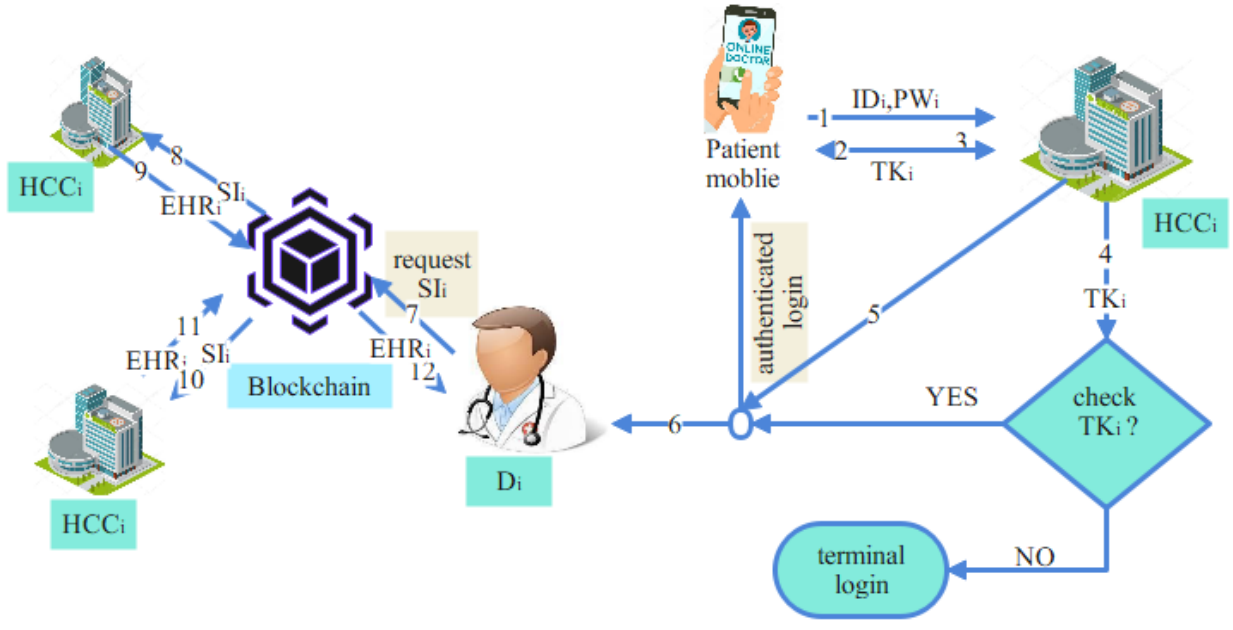

Figure 5 Explains the on-line hospitality phase

Performance Comparisons

We compared the computing costs of the phases (registration, Hospitality, On-Line Hospitality Phase) in our proposed work with related work (one-way cryptographic hash function (T_h), symmetric key encryption(T_E)/decryption (T_D), XOR function $T_{\oplus}$, additional operations such as generate random number, secret key (T_{Opr})), as shown in Table 3 and figure 6.

Table 3 Computational of Comparison Cost

Scheme	Registration Phase	Hospitality Phase	On-Line Hospitality Phase	Total
Our Scheme	$2T_{Opr}$	$T_{Opr} + 2T_E + 2T_D + 2T_h + T_{\oplus}$	$2T_{Opr} + 4T_E + 4T_D + 4T_h + 2T_{\oplus}$	$5T_{Opr} + 6T_E + 6T_D + 6T_h + 3T_{\oplus} \cong 4832bits$
[9]	$4T_{Opr}+3T_h$	$T_{Opr} + 2T_E + 2T_D + 3T_h$	$3T_{Opr} + 4T_E + 3T_D + 3T_h$	$8T_{Opr} + 6T_E + 5T_D + 9T_h \cong 5536bits$
[23]	$2T_{Opr} + 6T_h + 3T_{\oplus}$	$4T_{Opr} + 4T_E + 4T_D + 4T_h$	$3T_{Opr} + 2T_E + 2T_D + 9T_h + 5T_{\oplus}$	$9T_{Opr} + 6T_E + 6T_D + 12T_h + 8T_{\oplus} \cong 6432bits$
[13]	$20T_{Opr} + 4T_h + 11T_{\oplus}$	$4T_{Opr} + 4T_h + T_{\oplus}$	$12T_{Opr} + T_{\oplus}$	$36T_{Opr} + 8T_h + 13T_{\oplus} \cong 7040bits$
[14]	$10T_{Opr} + 2T_E + 2T_D + 4T_h + 2T_{\oplus}$	$6T_{Opr} + T_E + T_D + 2T_h$	$2T_{Opr} + T_E + T_D + 6T_h$	$18T_{Opr} + 4T_E + 4T_D + 6T_h + 2T_{\oplus} \cong 5888\ bits$
[18]	$11T_{Opr} + 2T_E + 2T_D + 6T_h + 4T_{\oplus}$	$9T_{Opr} + 2T_E + 2T_D + 5T_h + 3T_{\oplus}$		$20T_{Opr} + 4T_E + 4T_D + 11T_h + 7T_{\oplus} \cong 7008bits$

*hospitality phase in other proposed call authentication phase.

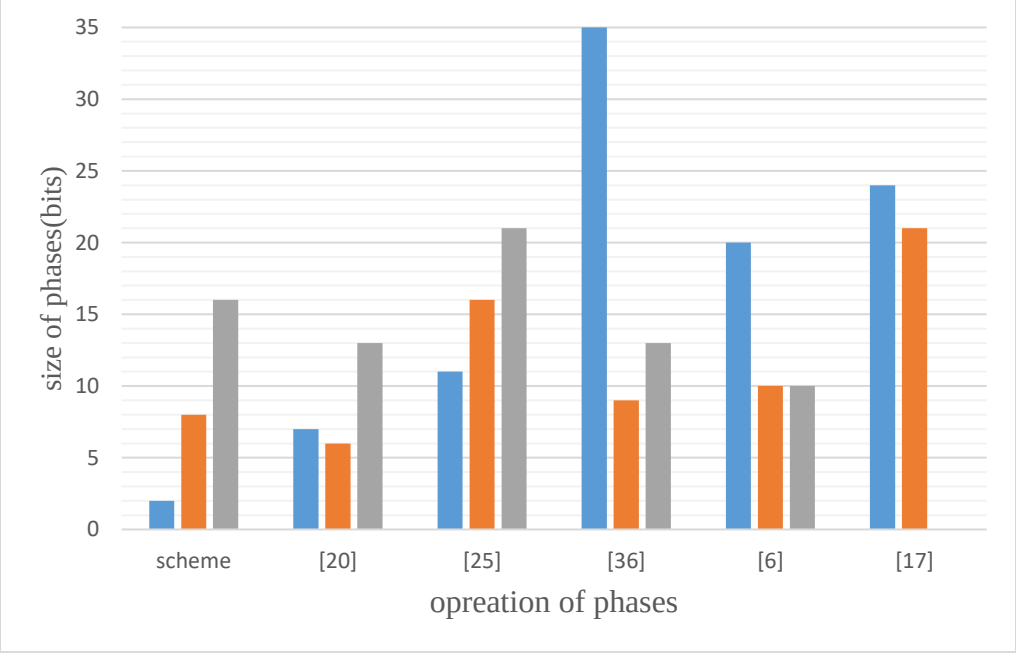

Figure 6 The Comparison cost with other phases

1. Communication Costs

The cost of communications between the components of our proposed system during the patient processing based on the bits sent /received during registration and confirming the patient's reliability within the system at the health centers during the login process. We evaluate the cost of communications in our system based on the PN and PW, it is assumed that modular operation requires $160\ bits$, an AES operation requires $256\ bits$, and a hash operation requires $160\ bits$. During the validation and communication phases between the health centers, Table 4 shows the cost of communication between components with other protocols.

Table 4 Comparison of communication costs

Scheme	Registration Phase	Hospitality Phase	On-Line Hospitality Phase	Total
Our scheme	$\approx 0.022\ ms$	$\approx 0.107\ ms$	$\approx 0.214\ ms$	$\approx 0.329\ ms$
[9]	$\approx 0.21\ ms$	$\approx 0.00296\ ms$	$\approx 0.21296\ ms$	$\approx 0.42592\ ms$
[23]	$\approx 0.204\ ms$	$\approx 0.00382\ ms$	$\approx 0.20782\ ms$	$\approx 0.41564\ ms$
[13]	$\approx 0.012\ ms$	$\approx 0.00144\ ms$	$\approx 0.0134\ ms$	$\approx 0.02684\ ms$
[14]	$\approx 0.1262\ ms$	$\approx 0.0047\ ms$	$\approx 0.1309\ ms$	$\approx 0.2618\ ms$

2. Comparison of Computational Complexity

The cost of our proposed system calculation with other related systems of similar currency is presented within the subsection of the research. The computation cost of the system has been evaluated with the results of the systems approaching our proposed system.it has to interest in the implementation environment for our work to simulate our system using the related devices to obtain approximate results with our proposed system, we have implemented the mentioned operations in the device Computer. According to the results for our system, T_{Opr} takes $0.00078\ ms, T_e \backslash T_d$takes $0.00122\ ms$ while T_h takes $0.0024\ ms$. Where the results were approximate by the patient. Since the execution time, $T_{\oplus}$ and sequence ($||$) operations are very few and do not affect the execution time, they are ignored in the system cost calculation. After analyzing Table 3, Table 4, and Figure 6. We can see the degree of convergence in the results for our proposed system, which has less computational power than all systems similar to ours.

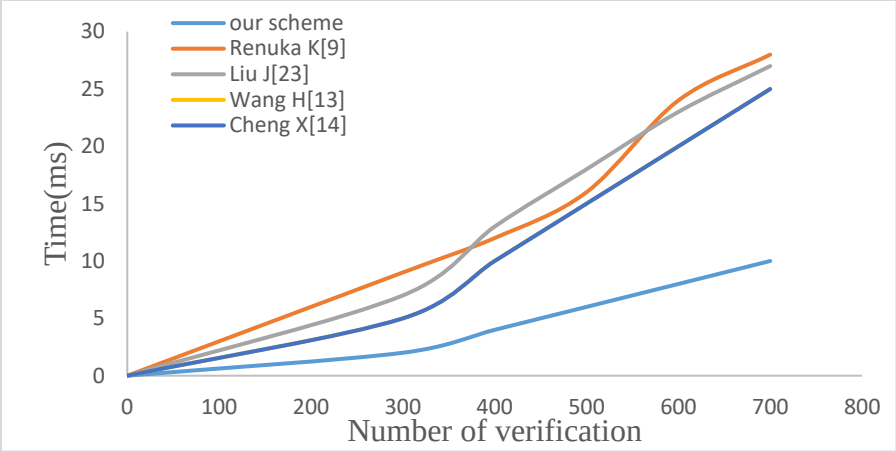

Figure 7 Complexity of computation

3. Comparison of Security Features

It is shown via the released security features of the proposed system with the other features of the related systems as shown in Table 5. The security features will be displayed vertically with the features of the systems displayed horizontally in order to compare them with the features of our proposed system for the purpose of providing more security features from the related systems with our system (K. Renuka, S. Kumari, and X. Li, 2019). To establish that our proposed system provides the maximum required security features. Our system is able to the transaction with attacks and security threats compared to related systems (J. Liu *et al.*, 2018).

Finally, after reviewing Tables 3 and 4 and figure 4 and 5, we can conclude that our proposed system provides higher and better efficiency and performance in terms of computational costs and communication compatibility compared to other related systems (S. Wang, Y. Zhang, and Y. Zhang, 2019). In addition, our proposed system can resist more security attacks Known while providing better security features than related systems.

Table 5 Security features comparison

	Security Feature	[9]	[23]	[13]	[14]	**Our scheme**
1	provides access data securely	No	No	No	No	Yes
2	Provides mutual authentication	Yes	Yes	Yes	No	Yes
3	Provides data securely search	No	No	No	No	Yes
4	Provides anonymity and privacy	Yes	Yes	Yes	Yes	Yes
5	provides data untraceability	Yes	No	Yes	Yes	Yes
6	Resistant to an insider to attack	Yes	No	No	No	Yes
7	Resistant to a password guessing attack	No	Yes	No	No	Yes
8	Resistant to a user impersonation attack	Yes	Yes	Yes	No	Yes
9	Resistant to a user impersonation and Server impersonation attack	Yes	Yes	Yes	No	Yes
10	provides a once session key for perfect secrecy and anonymity	No	Yes	Yes	Yes	Yes
11	Resistant to man-in-the-middle attack	No	No	Yes	No	Yes
12	provides No clock synchronization	No	No	No	No	Yes

No: Not offer Security Feature, Yes: Offers Security Feature

Conclusion

Blockchain has played an important role in the field of health care, advances in the field of information technology through some health applications that have emerged at the present time. In this researched, we focused on de-centralizing authority by providing the blockchain-based model to protect patient information and officially access data through its network and decentralized system after verifying private keys. The patient can share data with other health care centers and information within the network. Through the policy of controlling access to data and EHR and security them from external attacks by the privacy and security of patient EHRs. Also, by implementing our proposed blockchain network based EHR sharing system. Which the abolition of the central authority in the system unit. Achieving secure in the system through implementation and the non-changeable ledger technology by the user to modify the ledger data. In order to reach a high level of security and authentication to preserve patient data within the network. Blockchain is an effective solution for management EHRs with other departments and health centers. The development and maturity of blockchain will become more important in future data through decentralized networks.

References

Celesti, A., Ruggeri, A., Fazio, M., Galletta, A., Villari, M., & Romano, A. (2020). Blockchain-based healthcare workflow for tele-medical laboratory in federated hospital IoT clouds. *Sensors, 20*(9). http://doi.org/10.3390/s20092590

Alkhushayni, S., Al-Zaleq, D., & Kengne, N. (2019). Blockchain technology applied to electronic health records. *In Proceedings of 32nd International Conference on, 63,* 34-42. http://doi.org/10.29007/2x3r

Benil, T., & Jasper, J.J.C.N. (2020). Cloud based security on outsourcing using blockchain in E-health systems. *Computer Networks, 178,* 107344.

Mukherjee, P., & Singh, D. (2020). The opportunities of blockchain in health 4.0. *In Blockchain Technology for Industry 4.0, Springer, Singapore,* 149-164. http://doi.org/10.1007/978-981-15-1137-0_8

Nguyen, D.C., Pathirana, P.N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access, 7,* 66792-66806. http://doi.org/10.1109/ACCESS.2019.2917555

Capece, G., & Lorenzi, F. (2020). Blockchain and Healthcare: Opportunities and Prospects for the EHR. *Sustainability, 12*(22), 9693. http://doi.org/10.3390/su12229693

Feng, Q., He, D., Wang, H., Zhou, L., & Choo, K.K.R. (2019). Lightweight collaborative authentication with key protection for smart electronic health record system. *IEEE Sensors Journal, 20*(4), 2181-2196. http://doi.org/10.1109/JSEN.2949717

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability 2020, 12*(17). http://doi.org/10.3390/su12177002

Renuka, K., Kumari, S., & Li, X. (2019). Design of a secure three-factor authentication scheme for smart healthcare. *Journal of medical systems, 43*(5), 1-12. http://doi.org/10.1007/s10916-019-1251-3

Harshini, V.M., Danai, S., Usha, H.R., & Kounte, M.R. (2019). Health record management through blockchain technology. *In 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 1411-1415. http://doi.org/10.1109/icoei..8862594

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health informatics journal, 25*(4), 1398-1411. http://doi.org/10.1177/1460458218769699

Jeong, Y.S., Kim, D.R., & Shin, S.S. (2019). Efficient Mutual Authentication Protocol between Hospital Internet of Things Devices Using Probabilistic Attribute Information. *Sustainability*, *11*(24), 7214. http://doi.org/10.3390/SU11247214

Wang, S., Zhang, Y., & Zhang, Y. (2019). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access*, *6*, 38437–38450. http://doi.org/10.1109/ACCESS.2018.2851611

Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a secure medical data sharing scheme based on blockchain. *Journal of medical systems, 44*(2), 1-11. http://doi.org/10.1007/s10916-019-1468-1

Yang, G., & Li, C. (2018). A design of blockchain-based architecture for the security of electronic health record (EHR) systems. *In IEEE International conference on cloud computing technology and science (CloudCom)*, 261-265. http://doi.org/10.1109/CloudCom.00058

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N.C. (2017). Towards using blockchain technology for eHealth data access management. *In fourth international conference on advances in biomedical engineering (ICABME)*, 1-4. http://doi.org/10.1109/ICABME.8167555

"Blockchain in health," no. September, 2016. https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf

Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An efficient authentication scheme for blockchain-based electronic health records. *IEEE access, 7*, 41678-41689. http://doi.org/10.1109/ACCESS.2904300

Shamshad, S., Mahmood, K., Kumari, S., & Chen, C.M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications, 55*. http://doi.org/10.1016/j.jisa.102590

McClung, A., & Archer, N.P. (2014). *Health information dissemination from hospital to community care: current state and next steps in Ontario.*

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems, 40*(10), 1-8. http://dx.doi.org/10.1007/s10916-016-0574-6

Zheng, X., Geng, X., Xie, L., Duan, D., Yang, L., & Cui, S. (2018). A SVM-based setting of protection relays in distribution systems. *In IEEE Texas Power and Energy Conference (TPEC),* 1-6. http://doi.org/10.1109/TPEC.2018.8312071

Liu, J., Li, Y., Tang, Y., Cheng, J., Wang, J., Li, J., & Liu, Z. (2018). Rhein protects the myocardiac cells against hypoxia/reoxygention-induced injury by suppressing GSK3β activity. *Phytomedicine, 51,* 1-6. http://doi.org/10.1016/j.phymed..06.029.

Juneja, A., & Marefat, M. (2018). Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. *In IEEE EMBS International Conference on Biomedical & Health Informatics (BHI),* 393-397.

Seol, K., Kim, Y.G., Lee, E., Seo, Y.D., & Baik, D.K. (2018). Privacy-preserving attribute-based access control model for XML-based electronic health record system. *IEEE Access, 6,* 9114-9128.

Noruzi, A. (2018). Patent citations to webology journal on the USPTO database. *Webology, 15*(1), 1-7.