International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Privacy Preserving in Healthcare Sector Using Blockchain Technology

Madhuri Shinde[1], Dr. S.V. Gumaste[2]

Submitted: 25/01/2023 **Revised:** 14/03/2023 **Accepted:** 08/04/2023

Abstract: A distributed, decentralized ecosystem free from the necessity for a centralized authority is made possible by blockchain technology. The application of cryptographic principles ensures the security and dependability of processes. The healthcare sector is one in which blockchain technology has great promise due to the need to connect dispersed systems, enhance the accuracy of electronic medical data, and take a more patient-centric approach to healthcare systems' Electronic Healthcare Records (EHRs). A blockchain performs better in user verification and has increased the security of a healthcare database. Developing a Blockchain-based healthcare management system to provide privacy and security to patients' and doctors' data to address the overabundance of security-related concerns. This proposed system involves interactions between many medical substances. It provides security for both patients' and doctors' data. Additionally, a patient can simply and securely request medical insurance, and the insurance company can obtain verified patient data in a secure manner that prevents outside access. This proposed system uses the Python, Flask framework, TF Encrypted and MongoDB database which is available online for the system implementation. The time, memory usage and indexing time achieved for the proposed model is 9.7 ms and 9.5 Kb and 63 ms.

Keywords*: implementation, verification, indexing, blockchain, Python*

1. Introduction

Blockchain is viewed as having a lot of potential in a lot of sectors, including healthcare [1]. With the use of blockchain technology, access management, data exchange, and keeping track of a medical activity's audit trail are all made possible. Blockchain technology benefits clinical trials, the exchange of medical records, credentialing the provider, medical billing and various aspects. These technologies may also help to consolidate patient data, making it easier for different healthcare facilities to share medical records [2]. Blockchain removes the single point of failure traditionally provided by a centralized authority by enabling two or more parties to perform transactions in a distributed environment. As a broadly suggested technology, blockchain is presently viewed as having applications in several industries and use cases, including access control, settlement of disputes, tender documents, systems integration, insurance, and healthcare [3] [4]. Medical data of patients must be stored in the healthcare industry. This data is extremely sensitive, making them a target for cyber assaults. It is a need to protect all of this sensitive data.

An Electronic Health Record (EHR) is a database that includes information on a person's medical history, including information on ailments, prescriptions, medical images, and billing data. Sharing data securely is the biggest problem in healthcare systems since this data is sensitive and needs to be secured from unauthorized access. Before uploading to a public cloud, EHRs can be encrypted, which would be a common or naive approach to transmitting medical data [5].

Every block in the blockchain consists of a header and various transactions. Each successive valid block after the first one is formed has to contain the block header's hash output. The hash function of the previous block, which is present in every valid block, serves as a link between it. By joining each block to the previous one, a chain of blocks is created. Security study shows that this suggested system is resistant to numerous assaults and offers several desirable security aspects. Performance analysis demonstrates that, when compared to other equivalent systems, the suggested scheme is more efficient. A blockchain-based secure health insurance claims system was presented for a variety

[1]*madhuris_ioe@bkc.met.edu*
[2]*shyamraog_ioe@bkc.met.edu*

of medical processes and to simplify challenging medical procedures. Additionally, we talked about the constraints and future possibilities for blockchain research as well as how blockchain technology might be used in the healthcare industry.

2. Literature Review

A private blockchain would be the most suitable sort of blockchain for confidential medical data. Without involving a third party in the communication and exchange of common data in a situation where the various parties do not trust each other, a blockchain can be implemented easily using the Würst and Gervais [6] decision model. When determining if a certain scenario calls for blockchain, their model outlines several characteristics that must be taken into account. For storage, various elements need to be taken [6]. The majority of the current medical data infrastructure is dependent on reliable outside parties. These can't always be completely trusted because of the blockchain, which does not require any central authority. Patients benefit from the solution's convenience while researchers may share medical data effectively. The data user can be very confident while receiving accurate search results. Before the information is shared with others, the desensitization technique should be employed to allow doctors and researchers access to patients' health data but with the condition of the personal information cannot be compromised [5].

The strategy used by Hu et al. [7] aims to address malicious attacks. It creates a search method that is financially fair by introducing fairness using smart contracts. The search methodology makes it easy for a doctor to swiftly find EHRs whose symptoms include the requested keywords [8]. An ABE-based fine-grained authorisation mechanism for a relational database was proposed by Guo et al. [9] which has a time efficiency of 30 ms. A dynamic SSE approach that supports forward privacy and delegated verifiability for EHR data was recently proposed by Yang et al. [10]. The authors enabled remote patient monitoring by utilising cloud storage and the Internet of Things. Also, it shows when dealing with the 1000 files the verification time taken by the model [10] is 135 ms.

A smart contract is computer software created to digitally enforce the terms of a contract, as first suggested by Nick Szabo [11]. By leveraging cryptographic methods and diverse security protocols, some cryptocurrencies have recently adopted various smart contracts. With the use of a digital smart contract, transactions may be executed reliably without the involvement of a third party, and all transactions are traceable and irrevocable. In other words, smart contracts lower transaction costs involved with contracting and offer security that is superior to that offered by traditional contract law [11].

A cloud-based framework for securely transferring medical records was put forth by Au et al.[12]. Their study aims to allow healthcare authorities to share the patient's private data for research but also maintain the privacy of their personal information. Patients who access their medical data through aided APIs are the topic of William et al [13]. The success of the strategy is that patients act as the digital guardians of their health information, approving its release and sharing it with reputable organisations.

A Blockchain-based healthcare data gateway was proposed by Yue et al. [14]. Its goal is to maintain patient privacy and provide peoples control over their data. Here, the authors used the raw medical data for computation. But, they do not describe how to prevent a service from releasing the drug [15], a high-level Blockchain-based framework, was created by Xia et al. Medical records can be accessed from a shared repository by data owners and users after the keys and identities have successfully been authenticated. The identity-based authentication and the mechanism which is a key agreement mechanism proposed by [16], is used to perform user membership authentication. However, it must be emphasised that only those who have been authenticated and invited can securely communicate sensitive health data. The same writers also came up with MedShare [17], which is built on Blockchain which allows patients and physicians to use cloud repositories and share data.

After the start of blockchain technology and smart contract, a platform which is distributed for the suitable and immutable storage of data is implemented. Decentralized data storage solutions based on blockchain have recently been proposed in many studies [18][19][20][5][21][22]. Although several of these proposed techniques claim to offer data encryption, they don't. Many blockchain-based models have the capacity of encryption but simultaneously don't have the capability of searching [23] [19]. A centralized EMR record management system based on Blockchain technology was proposed by Azaria et al. [24]. Their method ensures immutable records, simple access, accountability, authentication, data exchange, and

privacy of highly sensitive medical information. A uniform architecture was presented by Roehrs et al. [25] to gather dispersed data from many sources. The OmniPHR solution, which incorporates Blockchain ideas, is sufficiently elastic and scalable to support large datasets.

Blockchain-based data exchange is also relevant in a variety of contexts, including smart health care, the internet of vehicles, etc.; blockchain plays a variety of functions in these contexts. Dong, Yue and others [26] created the Distributed EarthSystem Scientific Data Sharing Platform to connect scientific data resources and offer consumers one-stop data exchanging services. A framework for safely sharing sensitive data on big data platforms. The whole public has access to see all the data in the public permission-less blockchain. However, to protect a participant's anonymity, some elements of the blockchain may be encrypted [27]. Anyone can join a public permission-less blockchain and participate as a simple node or a miner without obtaining permission. These blockchains typically receive financial incentives [28] [2].

Table 1. Blockchain systems used for medical research

Blockchain-based system	Blockchain type	Consensus	Blockchain platform
FHIR chain [29]	Private	PoW	Ethereum
Trial chain [30]	Private	PoW	Ethereum
Dwarna [31]	Private	RBFT	Hyperledger
Medrec [32]	Private	PoW	Ethereum
Chainscript [33]	Private	PoC	Bitcoin
Blocktrial [34]	Private	PoC	Ethereum

3. Methodology:

3.1 Block diagram.

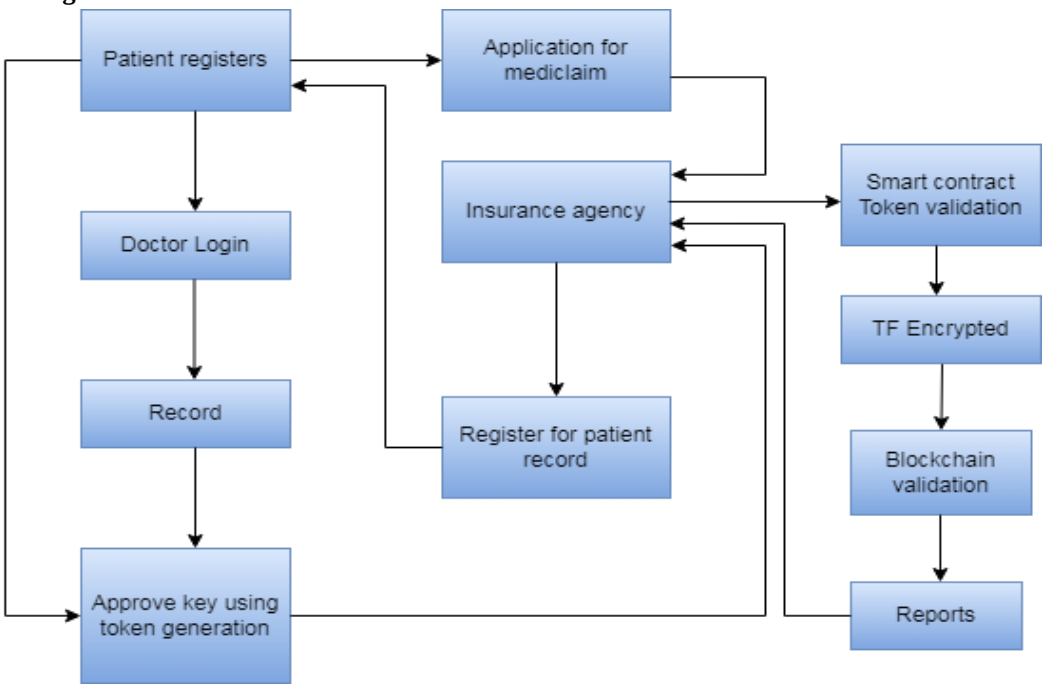

Fig1. Blockchain in secure health insurance claims

3.2 Description:

The proposed blockchain-system in secure health insurance claims provides secure health insurance claims by using Python and flask framework which here used as a frontend tool and the MongoDB database (which is available online) as a backend tool. When a patient registers with the hospital the doctors create the records of the patient. The created reports are stored in the cloud database server in an encrypted format where no third party can access the patient's records. After creating the patient's records this model also provide the facility of an Insurance agency to the patient through which a patient can easily apply to the mediclaim using the medical tokens. When the patient applies for the claim the tokens are created for the patient. The tokens are

created using the chaotic map technique. After this the validation of the token is essential and it is done through the blockchain network for the security of the system. The generated token is get secured by the TF encrypted method where the privacy of the users is get maintained. The TF encrypted method is used which combines two libraries such as Tensorflow and Keras to encrypt and secure the patient's data. The data validation process is implemented after the encryption of the data and it is the main aim of the proposed model. In this proposed model the healthcare patient record is get secured through TF encrypted which encrypts the data before validation. After token validation, the insurance agency can access the patient's data and get the patient's reports. This proposed model created simple registration forms for patients and doctors and stored the data in the cloud. The EHR stores the patient's record.

The EHR owner (i.e. the EHR user) instantiates the two completely random tokens security requirements during the searching symmetric encryption. It is employed to maintain the secrecy of the EHR. Then the credentials is feed into generator of key, which creates two distinct symmetric encryption keys. For the respective purposes of index encryption and EHR file encryption, two distinct symmetric keys are assigned. In this proposed system the insurance agency facility is also included. A token generation using a chaotic-map-based security protocol outperforms traditional cryptosystems cryptography. Passing this key as a validation token to the cloud server which will be validated on a blockchain architecture. If the key valid user health record will be decrypted as shown in the above methodology and once the time stamp is over user record will be again encrypted and privacy will be maintained which will be implemented in a further module.

$$KGEN(R_1, R_2) \rightarrow (A_1, A_2) \qquad (1)$$

Key generation:

Below equation (2) shows the key generation procedure that produces a symmetric key S using the user's security parameter p.

$$KGEN(p) \rightarrow S \qquad (2)$$

The owner of the EHR and the cloud service provider construct a pair of Cryptography Digital Authentication Methods. The methods are public and private keys. And create a hash function to enable two-side verification.

$$KGEN(User) \rightarrow (SP_K, SS_K) \qquad (3)$$

$$KGEN(CSP) \rightarrow (EP_K, ES_K) \qquad (4)$$

Further providing security parameters to the EHR the above equations show the movement and implementation of smart contract to the blockchain. The owner will then obtain the smart contract metadata needed to access and interact with the blockchain network's contracts.

3.2.1 Index making

All of the submitted electronic health records will be indexed in this suggested system before encryption. Bitmap indexing is a technique which is used to hold the extracted keywords together along with its matching EHRs unique identification pointer which is done in the blockchain-based healthcare system. Through the encrypted keywords the bitmap index a type of index matrix can search the EHR. A bitmap index is a type of index which enables the system to find EHR by searching through the encrypted keywords.

Index making:

Creates an encrypted index I using the secret key K and the outsourced document D.

$$IndexBuilder(D, K) \rightarrow I \qquad (5)$$

3.2.2 Token generation

For a private blockchain network, it is more beneficial that most doctors and pharmaceutical firms receive the medical tokens. It is also simple to use and purchase a hosting service. Doctors utilize medical tokens to provide telemedicine. Generating the tokens using the chaotic map technique

Generating tokens using chaotic map technique:

$$SToken(I, T) \rightarrow O_S \qquad (6)$$

Calculate the encryption key using the random number r1 and secret key K

$$KEY = r1(K) mod\ p \qquad (7)$$

3.2.3 TF Encrypted

TF encrypted is used to explore and unlock the effect of privacy-preserving machine learning. TF encrypted is an open-source framework which here used for secured multi-party communication. TF encryption method is used to encrypt the patient's data after the key generation. This model used two libraries in TF encrypted method i.e. Keras and Tensorflow library. Here also exploring how TF Encrypted can work together with Tensorflow and Keras. For instance, TF Encrypted can be used to realize secure aggregation for the former and can

provide a complementary approach to privacy concerning the latter. It provides privacy by adding secure computation to the mix.

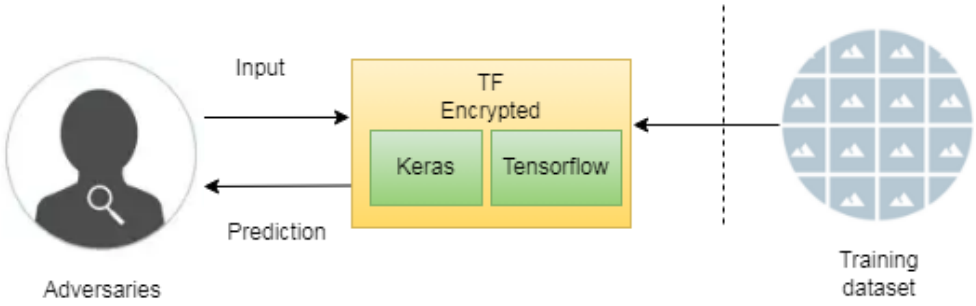

Fig 2. TF encrypted stops the model from transferring sensitive information

A. Keras and Tensorflow:

Here this proposed model used the Keras and Tensorflow library because it is simple, flexible and powerful. The Keras is also known to be the high-level API of Tensorflow. Using Keras it is simple to run new experiments and Tensorflow is a type of architecture used for implementing ML techniques and describing them for executing things properly. Tensorflow provides the user to take full control over their data. Tensorflow is the second-generation technique used for the development and implementation of major machine learning models. Tensorflow has the capability of handling multiple threats only on a single machine and provides graph visualization using the Tensorboard.

3.2.4 Smart contract

A smart contract is used by the blockchain for self-executing the programme. It is used for searching and uploading the bitmap index. Also for supporting ECDSA digital signature verification the smart contract is used in index matrix finding against unauthorized access during token searching and token generation. The implementation of blockchain can lower the count of engaged system entities which helps to reduce the failure that is single point. The smart contract owner, who is the owner of the EHR, must provide access information to every organization wants to search the EHR.

3.2.5 Blockchain network:

Public key management and index searches employ smart contracts. The EHR owner uploads the index, which is then securely saved as a block of data inside the blockchain. Enabling the private blockchain technology to interact with the backend libraries. This involves compression, encryption, decryption, and a key management system. The private blockchain operates on the provider side. The link between the entities is made trustworthy and data transparency is provided by this cloud-based support. Without the involvement of outside parties, the service processed stored data.

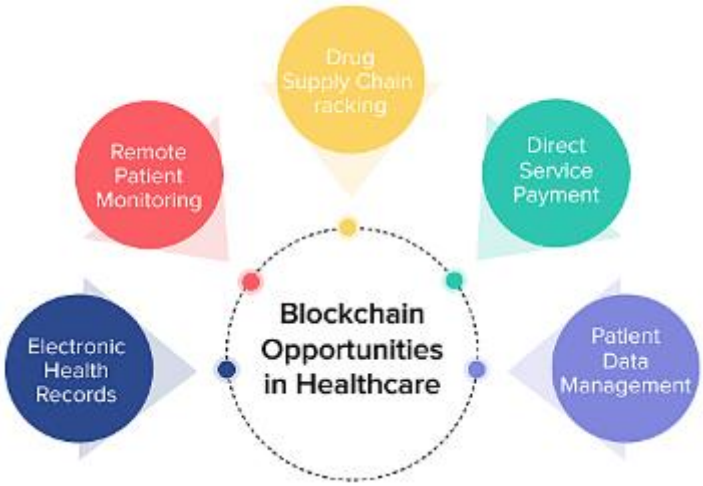

Fig 3. Services gave by blockchain in the healthcare sector

Key Generation Phase at Cloud Server:

When the data is encrypted, send the encrypted data *C*2 to the medical Centre server MCS

$$KMMCS = Th(IDMCS)(SKM) mod\ p \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (8)$$

3.3 **Symbols** [35]

KGEN	Generated encrypted keys
A_1, A_2	Symmetric key encryption with searchable keys
R_1, R_2	Passwords generated at random
SP_K, SS_K	User's public and secret key
EP_K, ES_K	Server's ECDSA public and secret key
E_K	Secure keywords
EHR_C	Ciphertext for EHR
CSP	Cloud Service Provider
O_S	Search outcome
SToken	Search Token
D	Outsourced document
I	Encrypted Index
K	Secret Key

4. Results and Discussion:

This proposed Blockchain-based secure health insurance claim system is implemented using the PYTHON scripting language and flask framework at the front end and also store the data on cloud database using MongoDB. In this proposed system the tokens are generatedusing a chaotic key algorithm. A chaotic algorithm is producing a unique random key based on user input and mathematical parameter mentioned in the above methodology. In this proposed system the tokens are generated for the patients. Further patient can decide whether to apply for an insurance agency or not. The token generation process is done through a chaotic mapping technique. Once the token is verified the insurance agency can get access to the patient's data created by the doctors. The blockchain identifies whether the token is valid or not, after the token confirmation the insurance agency can access the patient's data.

A simple website that enables users to log in as an admin, doctor, or patient and carry out their particular specialist procedures has been built using Python. The micro framework in Python is used for blockchain implementation. A block is formed with a hash based on attributes of the medical record and it holds the previous hash as well as the timestamp of creation.

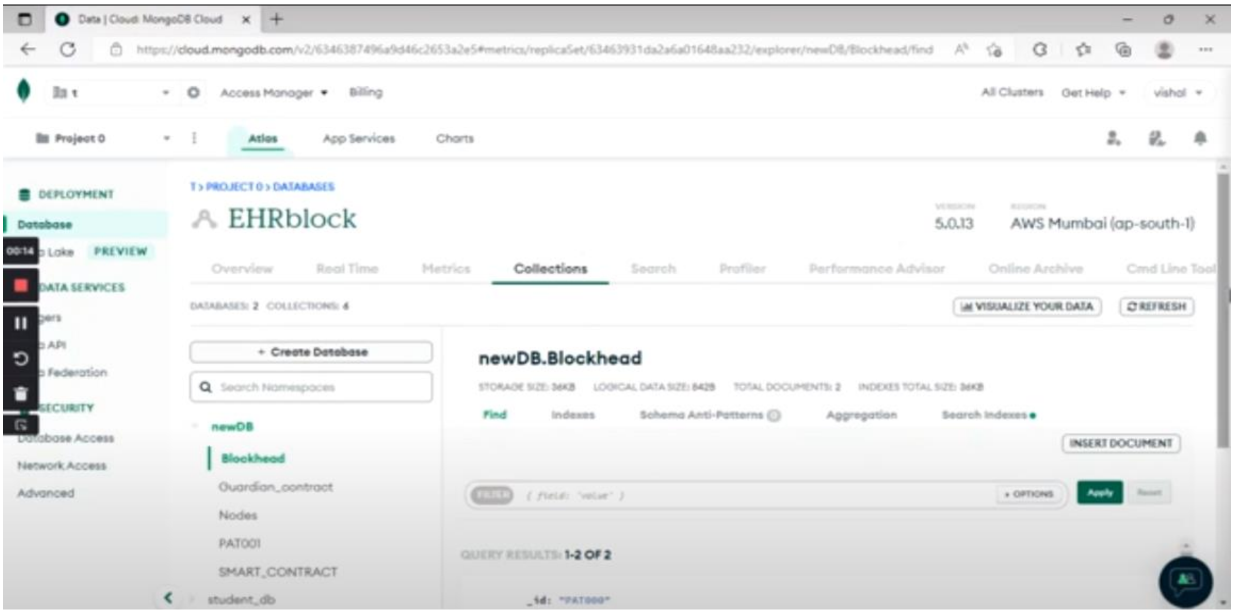

Fig 4. Electronic health record block creation

Figure 4 depicts the Electronic Health Record block creation in a blockchain-based healthcare management system where the data of the patient is stored in the cloud using a cloud database.

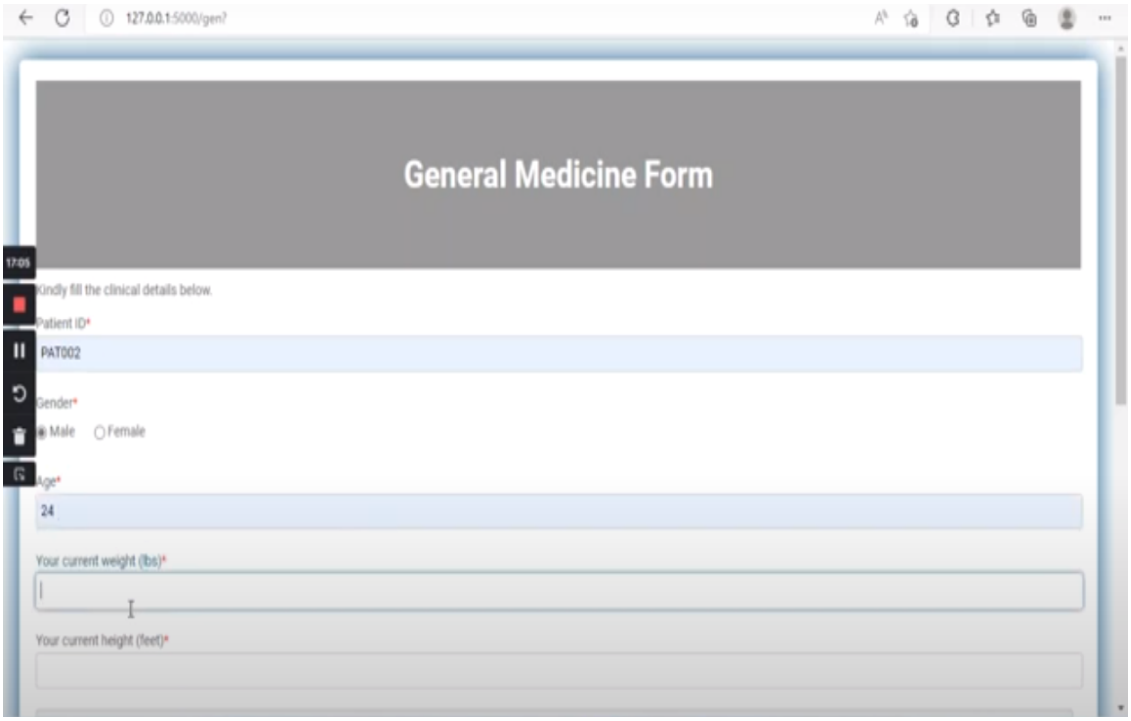

Fig 5. Medicine form for the proposed system

Figure 5 shows the creation of the general medicine form which takes the patient's personal information and processes the data through the blockchain. The forms are created using various collections in the database. The form consists of various entities such as Patient id, name, height, weight, gender, age, etc.

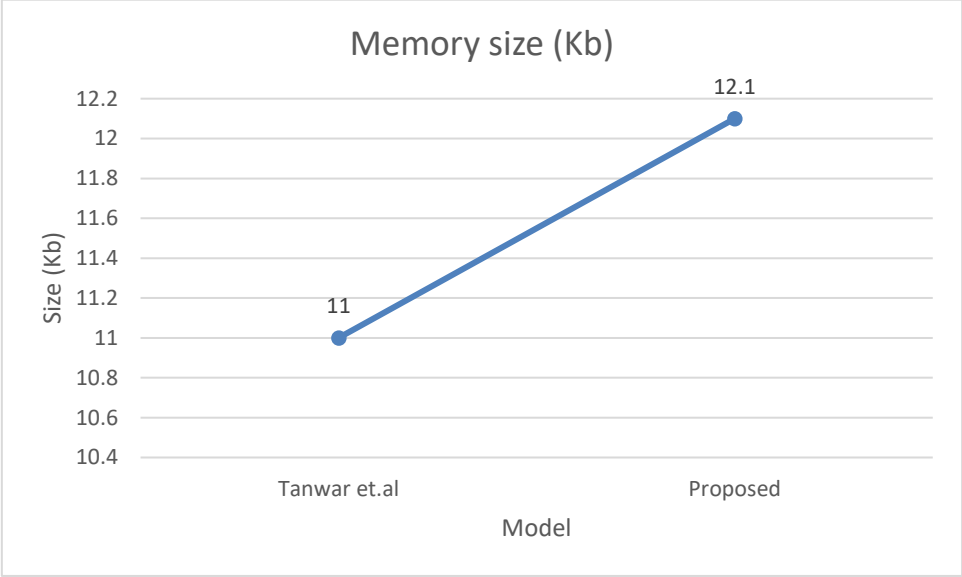

Fig 6. Comparison of memory usage for various methods [35]

Figure 6 shows the memory usage of the proposed model as compared to the previous method. The memory usage for this proposed model is increased by 1.1 Kb per transaction when compared to [35] this happens because we improvise the security of this model which takes time to perform security functions hence takes more time.

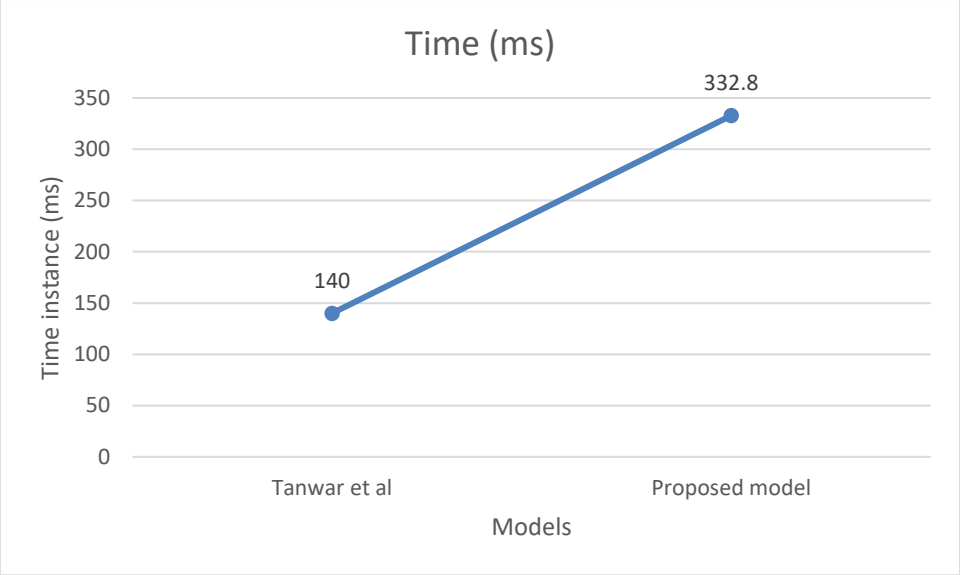

Fig 7. Comparison of various methods on time instance [35]

Figure 7 explains that as compared to previous method this proposed model shows the performance based on time instance. The time instance for this proposed model is increased by 192 ms per transaction when compared to [35] this happens because of increasing the security of this model which takes time to do the transaction.

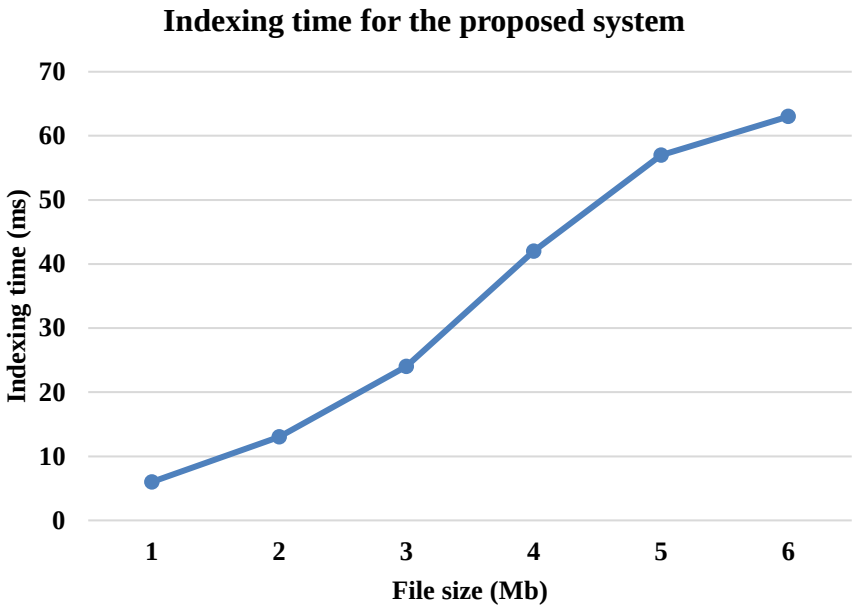

Fig 8. Indexing the different file sizes of HER

Figure 8 shows the electronic health record for different file sizes. When the file size increases, the indexing time does not increase as much.

5. Conclusion:

This proposed model achieves privacy protection during the remote diagnosis process and the security of medical data communicated over open channels. It allows the patient to receive secure healthcare promptly. The suggested scheme can withstand a variety of attacks and the evaluation process has demonstrated that it performs better than previous analogous schemes. Therefore, the suggested system is better suitable for usage in practical situations. For handling the healthcare data this proposed system obtain, store and exchange Electronic Health

Records for administering the management of hospital's operational system and supporting decisions of healthcare policy. It interacts with several pharmaceutical substances. By implementing a smart contract method on the blockchain for replacing the centralized server, this system can create a reliable and private blockchain approach which do not need a verification mechanism. This is achieved by combining powerful data from the Python scripting language and Flask framework. It uses MongoDB and TF encryption methods for storing cloud data beneath numerous libraries to carry out a variety of medical and healthcare operations. When we rise the security parameters of the proposed system it accesses more memory which is 1.1 Kb for one transaction and also increases performance time to 192 ms. Furthermore, the increase in file size grows the indexing time to 63 ms. This happens because security parameters take more memory and time to analyze threats. The security and performance analyses indicate that the proposed model's performance is very effective.

References:

[1] S. Bittins, G. Kober, A. Margheri, M. Masi, A. Miladi, and V. Sassone, "Healthcare Data Management by Using Blockchain Technology," in *Studies in Big Data*, vol. 83, Springer Science and Business Media Deutschland GmbH, 2021, pp. 1–27. doi: 10.1007/978-981-15-9547-9_1.

[2] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry (Basel).*, vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.

[3] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, p. 102407, 2020, doi: 10.1016/j.jisa.2019.102407.

[4] C. Agbo, Q. Mahmoud, J. E.- Healthcare, and U. 2019, "Blockchain technology in healthcare: a systematic review," *mdpi.com*, Accessed: Oct. 12, 2022. [Online]. Available: https://www.mdpi.com/440052

[5] L. Chen, W. K. Lee, C. C. Chang, K. K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Futur. Gener. Comput. Syst.*, vol. 95, pp. 420–429, 2019, doi: 10.1016/j.future.2019.01.018.

[6] J. Ross and M. I. T. Sloan, "Do you need a Blockchain?," *IACR Cryptol. ePrint Arch.*, no. 5, p. 2013, 2013, Accessed: Oct. 19, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8525392/

[7] S. Hu, C. Cai, Q. Wang, C. Wang, X. Luo, and K. Ren, "Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization," in *Proceedings - IEEE INFOCOM*, 2018, vol. 2018-April, pp. 792–800. doi: 10.1109/INFOCOM.2018.8485890.

[8] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu, and C. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search," *Soft Comput.*, vol. 20, no. 8, pp. 3243–3255, Aug. 2016, doi: 10.1007/s00500-015-1699-0.

[9] C. Guo, R. Zhuang, Y. Jie, Y. Ren, T. Wu, and K. K. R. Choo, "Fine-grained Database Field Search Using Attribute-Based Encryption for E-Healthcare Clouds," *J. Med. Syst.*, vol. 40, no. 11, Nov. 2016, doi: 10.1007/s10916-016-0588-0.

[10] L. Yang, Q. Zheng, X. F.-I. I. 2017-IEEE, and undefined 2017, "RSPP: A reliable, searchable and privacy-preserving e-healthcare system for cloud-assisted body area networks," *ieeexplore.ieee.org*, Accessed: Oct. 19, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8056954/

[11] Szabo N, "Smart contracts: building blocks for digital markets," *EXTROPY: The Journal of Transhumanist Thought*, 1996. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed Oct. 19, 2022).

[12] M. H. Au *et al.*, "A general framework for secure sharing of personal health records in cloud system," *J. Comput. Syst. Sci.*, vol. 90, pp. 46–62, 2017, doi: 10.1016/j.jcss.2017.03.002.

[13] W. Gordon, C. C.-C. and structural biotechnology journal, and undefined 2018, "Blockchain technology for healthcare: facilitating the transition to patient-driven

interoperability," *Elsevier*, Accessed: Oct. 19, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S200103701830028X

[14] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, vol. 40, no. 10, Oct. 2016, doi: 10.1007/S10916-016-0574-6.

[15] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Inf.*, vol. 8, no. 2, 2017, doi: 10.3390/info8020044.

[16] L. Wu, Y. Zhang, Y. Xie, A. Alelaiw, and J. Shen, "An Efficient and Secure Identity-Based Authentication and Key Agreement Protocol with User Anonymity for Mobile Devices," *Wirel. Pers. Commun.*, vol. 94, no. 4, pp. 3371–3387, Jun. 2017, doi: 10.1007/S11277-016-3781-Z.

[17] Q. Xia, E. Sifah, K. Asamoah, J. Gao, … X. D.-I., and undefined 2017, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *ieeexplore.ieee.org*, Accessed: Oct. 19, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7990130/

[18] A. R. Lee, M. G. Kim, and I. K. Kim, "SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR," in *Proceedings - 2019 IEEE International Conference on Bioinformatics and Biomedicine, BIBM 2019*, 2019, pp. 1087–1090. doi: 10.1109/BIBM47256.2019.8983415.

[19] R. Guo, H. Shi, D. Zheng, C. Jing, C. Zhuang, and Z. Wang, "Flexible and Efficient Blockchain-Based ABE Scheme with Multi-Authority for Medical on Demand in Telemedicine System," *IEEE Access*, vol. 7, pp. 88012–88025, 2019, doi: 10.1109/ACCESS.2019.2925625.

[20] N. Andola, Raghav, S. Prakash, S. Venkatesan, and S. Verma, "SHEMB: A secure approach for healthcare management system using blockchain," in *2019 IEEE Conference on Information and Communication Technology, CICT 2019*, 2019. doi: 10.1109/CICT48419.2019.9066237.

[21] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," in *2020 2nd International Conference on Advanced Information and Communication Technology, ICAICT 2020*, 2020, pp. 35–40. doi: 10.1109/ICAICT51780.2020.9333488.

[22] C. Devi Parameswari and V. Mandadi, "Healthcare data protection based on blockchain using solidity," in *Proceedings of the World Conference on Smart Trends in Systems, Security and Sustainability, WS4 2020*, 2020, pp. 577–580. doi: 10.1109/WorldS450073.2020.9210296.

[23] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 693–703, Jan. 2022, doi: 10.1007/s12652-021-03163-3.

[24] A. Azaria, A. Ekblaw, … T. V.-2016 2nd international, and undefined 2016, "Medrec: Using blockchain for medical data access and permission management," *ieeexplore.ieee.org*, Accessed: Oct. 19, 2022. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7573685/

[25] A. Roehrs, C. Da Costa, R. da R. R.-J. of biomedical, and undefined 2017, "OmniPHR: A distributed architecture model to integrate personal health records," *Elsevier*, Accessed: Aug. 18, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1532046417301089

[26] R. N. Nortey, L. Yue, P. R. Agdedanu, and M. Adjeisah, "Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain," in *2019 4th IEEE International Conference on Big Data Analytics, ICBDA 2019*, 2019, pp. 369–374. doi: 10.1109/ICBDA.2019.8713188.

[27] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 2017, pp. 557–

564. doi: 10.1109/BigDataCongress.2017.85.

[28] S. Squarepants, "Bitcoin: A Peer-to-Peer Electronic Cash System," *SSRN Electron. J.*, 2022, doi: 10.2139/ssrn.3977007.

[29] P. Zhang, J. White, D. Schmidt, … G. L.-C. and, and undefined 2018, "FHIRChain: applying blockchain to securely and scalably share clinical data," *Elsevier*, Accessed: Oct. 21, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2001037018300370

[30] M. Benchoufi, D. Altman, and P. Ravaud, "From Clinical Trials to Highly Trustable Clinical Trials: Blockchain in Clinical Trials, a Game Changer for Improving Transparency?," *Front. Blockchain*, vol. 2, Dec. 2019, doi: 10.3389/fbloc.2019.00023.

[31] N. Mamo, G. M. Martin, M. Desira, B. Ellul, and J. P. Ebejer, "Dwarna: a blockchain solution for dynamic consent in biobanking," *Eur. J. Hum. Genet.*, vol. 28, no. 5, pp. 609–626, 2020, doi: 10.1038/s41431-019-0560-9.

[32] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 2016, pp. 25–30. doi: 10.1109/OBD.2016.11.

[33] M. Benchoufi, R. Porcher, and P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," *F1000Research*, vol. 6, 2018, doi: 10.12688/f1000research.10531.5.

[34] D. M. Maslove, J. Klein, K. Brohman, and P. Martin, "Using blockchain technology to manage clinical trials data: A proof-of-concept study," *JMIR Med. Informatics*, vol. 6, no. 4, 2018, doi: 10.2196/11949.

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