(International Print/Online Journal)

SJIF IMPACT FACTOR: 5.565
PUBMED-National Library of Medicine ID-101739732

ISSN (Print): 2209-2870
ISSN (Online): 2209-2862

International Journal of Medical Science and Current Research (IJMSCR)
Available online at: www.ijmscr.com
Volume 4, Issue 3, Page No: 973-981
May-June 2021

A Literature Review of Blockchain-based Related Frameworks in Medical Records: Methods Used and Results

Panadda Suparun
Naresuan University Secondary Demonstration School

***Corresponding Author:**
Panadda Suparun
Naresuan University Secondary Demonstration School

Type of Publication: Original Research Paper
Conflicts of Interest: Nil

ABSTRACT
Due to the popularity of blockchain technology, there are many researches aim to apply blockchain technology in health care system, such as electronic health record systems; because the old systems are prone to errors, hacking and invalidation. Therefore, in this paper I present the summary and methods of the chosen researches which are for beginners and easy to comprehend. As part of the review, I also introduce relevant background relating to blockchain and electronic medical record systems.

Keywords: Blockchain technology, Smart Contract, Electronic Medical Records

INTRODUCTION

The trend of Blockchain technology is rising rapidly by the popularity of cryptocurrencies, especially Bitcoin. A large number of institutions are trying to apply this technology to their systems as the technology is able to escalate transparency, trusts and validity. Moreover; the technology can decrease the loss of time spending in each data transaction. In health care system, where medical records need to be transferred between hospitals effectively without having invalid information; blockchain technology is used to protect the data and reduce time loss. This technology is known for its immutability, transparency, privacy, security, accessibility and access control. (Sam Daley, 2021) It is believed to be the solution of the difficult problems found in medical records; for instance, verifying the identity, preservation and synchronization of medical records. Therefore; there are several researches and prototypes of health record system based on blockchain technology which is going to be discussed in this paper. The content in this paper is included the background of the components in Blockchain technology, the methods used and the summarize of each research.

Background

Block chain technology

Blockchain is a data base which is cryptographically protected, it is distributed and decentralized. The process about storage, maintenance, verification, accounting and transmission is based on the distributed system structure; using pure mathematical methods instead of central institutions to gain trusts. Its ledger is replicated across locations and are interlinked. No individual user controls the blockchain, and each can change it to the extent that their own keys allow. Blockchain can be used to facilitate trustworthy and secure transactions with transparency, without relying on the third party. Moreover; it is a chronical sequence of blocks including a list of complete and valid transaction record. (Luke Conway, 2021) Each block has a timestamp as its mark to ensure the traceability of the blockchain. Each block is divided into two parts: Block Header and Block Body, each Block Header

contains the link pointers of the block headers of the previous block, and the block body records the data information in the network. There are two kinds of blockchain, Permissionless and Permissioned Blockchain. A public blockchain is also called Permissionless Blockchain and it is easily accessible; thus, everyone can participate in the system with pseudonymous identification. An individual organization performs a permissioned blockchain; it is designed where participants in the network are predefined for read or write actions within the system. (Jake Frankenfield, 2020)

Smart Contract

Smart Contract is an agreed computing protocol on top of blockchain, used especially in the Ethereum blockchain system. It was purposed to allow distributed ledger systems to regulate contracts which could be coded as computing protocols, stored inside blockchain systems, and self-executed. It is compiled using a Solidity compiler residing on a blockchain. Furthermore; Smart Contract is also a coded consensus protocol: all the users in a blockchain system must follow the protocols to make transactions. Smart Contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. (Stuart D.Levi et al. 2018)

Hyperledger Fabric

Hyperledger Fabric is a type of permissioned blockchain technology which works based on an open-source blockchain enterprise entertained by the Linux Foundation. Hyperledger is a constantly prevalent, collective permissioned or private blockchain that attempts at improving blockchain technology through industry applications. Generally, Hyperledger Fabric is a distributed network formulating a peer-to-peer system where every peer has a replicated, consistent copy of the blockchain data structure. Hyperledger Fabric gives the chance to increase the application range of blockchain technology beyond cryptocurrency trades which distinct various relational database application domains. (Matt Zand,2019)

Electronic Medical Record (EMR)

Electronic Medical Record (EMR) is an electronic (digital) collection of medical information about a person that is stored on a computer. An electronic medical record includes information about a patient's health history, such as diagnoses, medicines, tests, allergies, immunizations, and treatment plans. Electronic medical records can be seen by all healthcare providers who are taking care of a patient and can be used by them to help make recommendations about the patient's care. (Peter Garrett and Joshua Seidman,2011)

Personal Health Record (PHR)

The Personal Health Record (PHR) is an electric, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. (Jill Burrington-Brown et al., 2005)

Proxy Re-encryption

Proxy re-encryption is a set of algorithms which allows an untrusted proxy to transform ciphertext from being encrypted under one key to another, without learning anything about the underlying plaintext. Proxy re-encryption algorithms usually work as public-key encryption, in which a public-private key-pair is used to encrypt and decrypt the data, respectively. (Giuseppe Ateniese et al, 2009)

Consortium Block chain

This type of blockchain is one that possesses no access restriction, meaning that absolutely anyone with an internet connection can become a participant of a public blockchain. More specifically, anyone in the world is able to read data that is included on the blockchain, and anyone in the world is allowed to execute transactions on a public blockchain. Importantly, there is also no restriction as to who can participate in the consensus process for blockchains, which is the process that determines the individual or entity that can add a block to the blockchain. Public blockchains are considered to be fully decentralized, with control over the blockchain not being in the hands of any single individual or entity. (Mark, 2018)

Remote Procedure Call server

Remote Procedure Call (RPC) is a protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. RPC is

Volume 4, Issue 3; May-June 2021; Page No 973-981

used to call other processes on the remote systems like a local system. RPC uses the client-server model. The requesting program is a client, and the service-providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned. (Alex Onsman, 2018)

Summarizing

A blockchain-based framework for electronic medical records sharing with fine-grained access control

There is an issue in using Electronic Medical Records (EMRs), which is how to ensure the privacy, security and shareability of EMRs while achieving fined-grained access control. Thus, the key of this paper is to achieve data sharing with security and privacy preservation. Therefore; this framework performs a harsh calculation on the electronic medical data and store the corresponding value on the blockchain to ensure its integrity and authenticity, then encrypt the electronic medical data and store it in the interplanetary file system which is a distributed protocol.

The encrypted keyword index information of electronic medical records was stored on the Ethereum blockchain, while a smart contract deployed in the Ethereum blockchain is used to realize keyword search instead of depending on a centralized third party. Furthermore; by using attributing based encryption scheme, the users can be ensured that only the attributes meeting the access policy can decrypt the encrypted electronic medical records. Lastly, the presented system reduces stress from data store and high-frequency access to blockchain. For security, this paper provides its framework with secure storage, privacy protection and tamper-proofing

Methods:

A point-to-point distributed storage system IPEs

1. Files are encrypted and stored in it. The system eliminates the needs to put the data on the chain, and it can make up for the shortcoming of the existing blockchain system in file storage
2. CP-ABE technology: In order to achieve doctor-centric access control, CP-ABE technology is contributed. It allows doctors and patients the set the policy about who has the right to access EMRs; and Only the data requesters who were authorized and their attributes satisfy the access policy in the ciphertext can decrypt the EMRs.
3. Encrypted Keyword Index: It is stored in a blockchain, and smart contract is deployed on the Ethereum blockchain.
4. An application example of a medical insurance scenario: It is given for safety analysis and performance analysis.

Evaluate its performance by three aspects:

1. characteristic of the scheme
2. time cost of cryptographic algorithm
3. Smart Contract cost

Conclusion

The system enables doctors firstly encrypt electronic medical records with appropriate access policies and then upload the ciphertext to IPFs. The combination of IPFs and blockchain allows doctors to process large amounts of electronic medical data via IPFs and eliminate the need of putting the data on the chain and to save the bandwidth in the blockchain. (S. J. R. L. W. S. Y. X; "A blockchain-based framework for electronic medical records sharing with fine-grained access control," PloS one. [Online]. Available:

https://pubmed.ncbi.nlm.nih.gov/33022027/. [Accessed: 26-May-2021])

A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition

Traditional personal health records in emergency condition lacks a sufficient control policy tool to limit the access permissions of any third-party person in traditional emergency system, it also lacks of tracking PHRs in traditional emergency systems. Moreover; it takes much time; solve the issue by defining security policies that a patient can assign which type of users can access the PHR without requiring any inquiry from other persons. Due to the popularity of blockchain technology and its immutability characteristics, it is used in this paper to create higher quality of accessibility, privacy, emergency, access control and data auditing.

Volume 4, Issue 3; May-June 2021; Page No 973-981

The use of blockchain technology in healthcare system management system can provide five mechanisms including patient identity, data aggregation, data liquidity, digital access rules and data immutability. Blockchain technology provides the system with adequate cooperative manner and care options for patients. Some distinct access control policies become limited because no specific policy would admit an emergency staff to obtain the patients' records. In this paper, Hyperledger composer based on Hyperledger Fabric is introduced, it affords some permissions for participants that allow limited access during an emergency condition. In conclusion, Blockchain technology can enhance the security and accessibility of the PHR by different participants in the proposed model while patients are in the emergency concerning confidentiality, non-repudiation authenticity, and accountability. It also can guarantee the patient's privacy by presenting expediency for designing well-arranged access control to the PHR. In this system, it limits the user's access to the PHR by employing smart contracts. Patient predefined access permissions rules to share their PHR by smart contracts on the blockchain without the lack of control and can also empower access to his/her PHR only under predefined conditions of an appropriate type and for a provided time limit.

The frame work will respond with a message unauthorized user and perform security policies according to the specific participant's IDs. It prevents the PHR data from being accessed by malicious users, and protects the data against ransomware and similar security breaches such as unauthorized access. Blockchain makes the process of adopting the system much simpler and less costly; it can also improve security, privacy, availability and auditing by storing access control lists and logs directly on the blockchain. It provides better efficiency compared with the traditional emergency access system. Smart contracts used for time control, verification and classification that reduce the response time during the processing of queries. The frame work provides accessibility to the PHR data items without approval by trusted members in the contact list for an emergency. Lastly, the frame work provides the security policies for PHRs that can improve healthcare system usability in emergency cases.

Methods:

1. Blockchain Network 2.Hyperledger Fabric 3.Hyperledger Composer Conclusion

This paper proposed new access control framework. The frame work preserves PHR data privacy where a patient is in an emergency condition. Its works based on the permissioned blockchain Hyperledger Fabric and Hyperledger Composer.

Smart contract is used to provide security policies. Patients can manage the access rules of other participants in the healthcare system using the consortium strategy. The system affords the historian records for auditing that stores the history of transactions while patients are in an emergency. It can also allow users to trace the history of the records. The framework assures the secret data sharing of the PHR by considering the immutability, auditing and emergency access control policies and enables the health management system to eliminate the time to emergency contact. ("A Blockchain-Based Secret-Data Sharing Framework for ..." [Online]. Available: https://res.mdpi.com/d_attachment/healthcare/healthcare-09-00206/article_deploy/healthcare-09-00206.pdf. [Accessed: 26-May-2021])

A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain

Stroke is a major chronic noncommunicable disease that seriously endangers the health of Chinese people; therefore, it is essential to obtain the patient's past medical history and physical examination for referral treatments. Centralized storage has high risk of electronic medical record data leakage and tampering, the security, integrity and immutability of electronic medical records cannot be guaranteed.

In order to solve these problems, the scheme is this paper is analyzed and evaluated from three aspects of medical record integrity, user privacy and data security by using blockchains to store medical data is too expensive and cannot restrict the identity of network participants, thus the consortium blockchains are more suitable for medical data storage. Proxy Re-encryption is a crypto graphic concept for converting ciphertexts; it is used in this scheme to enhance the reliability and security of the data. In this paper, one-way one-hop proxy re-encryption technology is adopted to ensure that the privacy of the patient's

Volume 4, Issue 3; May-June 2021; Page No 973-981

private key during the medical record sharing process and reduce the number of user interaction. Lastly, this paper designed blockchain-based stroke electronic medical record model.

Methods:

Block chain Technology 2.Searchable Encryption 3.Proxy Re-encryption

To achieve security and privacy

There are 2 types of encryption used in this paper

1. symmetric or Searchable Encryption (SSE)
2. asymmetric or Searchable Encryption (ASE)

The purpose of the constructions

1. to clarify the patient's ownership of medical record data and realize strict access control rights of patients to medical record data
2. to realize the privacy protection of patient identity and medical record data in the process of storage and sharing
3. to construct an efficient and secure sharing protocol to reduce user redundant operation
4. to realize the secure storage of massive high-privacy electronic medical record data

Conclusions

In this paper, cloud server is used to store the ciphertext of the original medical records, and the blockchain saves traceable log information and medical record index. The PBFT consensus algorithm is proposed to improve the reliability and security. The proposed scheme can resist the tampering attack of doctors and semi-trusted cloud and guessing attacks of malicious nodes on patient identity and privacy. Furthermore; the scheme has increasing flexibility and scalability in storage capacity and security in data privacy protection. It ensures that patients have ownership of medical records and provides patients with instant revocation of the right to access in access control. (Q. Qin, B. Jin, and Y. Liu, "A Secure Storage and Sharing Scheme of Stroke Electronic Medical Records Based on Consortium Blockchain," BioMed research international,01-Feb-2021.[Online].Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7875637/?fbclid=IwAR18UsQQosTQTtx3w7kWhyoU-o64uMs5jE4FrHcrSyGJZSVABajh_d-RSU8. [Accessed: 26-May-2021])

Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability

The goal is to build a system to access patient records easily among EHRs without relying on a centralized supervisory system. The application used Consortium blockchain to compose a distributed system and Hyperledger Fabric, in order to protect patient's privacy and generate proxy re-encryption scheme. As a result, the system can be used by doctors to find patient's records and verify patient's consent on access to the data. Patients also can seamlessly receive their past records from other hospitals. The access log is stored transparently and immutably in the ledger that is used for auditing purpose. Moreover; the system is feasible, flexible with scalability and availability in adapting to existing EHRs for strengthening security and privacy in managing patient records.

Methods:

Hyperledger Fabric 2.System Conceptual Design 3.Cryptographic scheme 4.Web-based application Conclusion

To protect patient privacy, the researchers adopted the Advanced Encryption Standards AES algorithm for symmetric key encryption of patient data and the Elliptic Curve EIGamel (EC-EIGamel) algorithm for asymmetric-key encryption of the symmetric key in the proxy re-encryption scheme. The asymmetric-key pair is also used for the signature on the transaction proposal. Adopted AFGH algorithm for proxy re-encryption. The system can be used to constitute a large-scale HER system. It is flexibly configurable to be a top layer of existing HER systems to strengthen security in the management and exchange of medical records. (D. Tith, J.-S. Lee, H. Suzuki, W. M. A. B. Wijesundara, N. Taira, T. Obi, and N. Ohyama, "Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability," Healthcare Informatics Research, 31-Jan-2020. [Online]. Available: https://www.e-hir.org/DOIx.php?id=10.4258%2FHiR.2020.26.1.3. [Accessed: 26-May-2021])

Volume 4, Issue 3; May-June 2021; Page No 973-981

Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials

Health Information Exchange (HIE) has its benefits as it decreases rates of readmission, avoiding medication errors, improving diagnosis and decreasing duplicate testing. However; there are persistent challenges surrounding HIE, for instance poor clinical efficiency, threats to patient privacy, data insecurity, poor integration of disparate data resources and dependency on centralized data storage and high cost of maintenance. Therefore; patients lack personal access and cannot get their data, which means patients cannot benefit from HIE. There are also data sharing issues like imprecision medicine. It is difficult to audit every clinical trial from each clinical site frequently due to the complexity of the system. Blockchain technology is applied for Health Information Exchange to solve these problems with smart contract engaged within it. After receiving a request from the smart contract, the RPC server queries data from different EHR databases and pushes the required data back to smart contract. The users need to utilizing a public key and a private key to validate their identities. The keys will link to their personal information in the hospital's RPC servers rather than the blockchain system.

In the clinical trial setting, only the FDA knows the role of each address: either trial sponsor or trial subject. All data in the blockchain system are encrypted using hashing algorithms. Under Smart Contracts regulations, all transactions follow rigorous protocols under secure conditions. Merkle-tree structure inside the blockchain make the system secure, stable and efficient to search.

The private chain the researchers have implemented for the HIE process provides authorization means for users in different applications without a requirement of specialized hardware. There is no third party in the validation process of the blockchain system. This saves cost and time to work with intermediate parties. This blockchain system provides a platform for advanced data analytics using artificial intelligence AI.

Methods:

Blockchain 2.Smart Contract

RPC / Remote Procedure Call server = to more actual health data around the participating clinical sites

Conclusion

This has shown that blockchain technology is able to facilitate an automatic validation process for HIE and clinical trials without third-party involvement. Using Smart Contracts, blockchain could perform HIE from distributed databases in a secure environment. It could also ensure data provenance and data security. (Y. Zhuang, L. Sheets, Z. Shae, J. J. P.

Tsai, and C.-R. Shyu, "Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials," AMIA ... Annual Symposium proceedings. AMIA Symposium, 05-Dec-2018.[Online].Available:https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6371378/?fbclid=IwAR0fmHgWE4waSGO_c8VG6eRpKQpKQtJfFMgGeoncEe4EpGEPQyXOiNo0uAA. [Accessed: 26-May-2021])

Blockchain vehicles for efficient Medical Record management

Due to the lack of interoperability in Britain's medical records systems which leads to clinical errors and patients must recount their history multiple times which can lead to confusion. This paper focuses on how electronic medical records in particular can be managed by Blockchain, and how the introduction of this novel technology can create a more efficient and interoperable infrastructure to manage records that leads to improved healthcare outcomes, while maintaining patient data ownership and without compromising privacy or security of sensitive data. As a result; with Blockchain, a record of the data's previous existence would always be maintained on the chain.

Blockchain would need to guard against intruders and it is more secure than older methods. It can allow a healthcare system to rule out any possibility of this style of attack. This method limits those who can run full nodes, issue transactions, execute smart contracts and read transaction history to approved computers and users. Moreover; it is used to secure patient data and to empower patients in a way that has not previously been possible. This method creates the ability to analyze the information with artificial intelligence and makes the system easier to determine population trends, which can be used to achieve population level health. It also requires careful integration, to allow sufficient integration without

Volume 4, Issue 3; May-June 2021; Page No 973-981

compromising privacy of patient data or security against hackers.

Methods:

1.Blockchain Technology 2.Smart Contract Conclusion

Blockchain saves medical and financial sacrifices and reduces administrative delays. The use of Smart Contracts allows patients' consent preferences to be executed immediately, and reducing administrative costs. Blockchain data lake is scalable and can store a variety of data types, making it versatile and suitable enough for the developing forms of data brought about by the Internet of Things. It also supports high-throughput data analysis. Its weakness is that the majority of people do not understand it and its functions. And costs ae involved in concealing these and assimilating data from various legacy systems while maintaining adherence to various regulatory restrictions. Blockchain represents an innovative vehicle to manage medical records, ensuring interoperability but without compromising security. It also protects patient privacy, allowing patients to choose who can view their data. (A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient Medical Record management," Nature News, 06-Jan-2020. [Online].

Available: https://www.nature.com/articles/s41746-019-0211-0. [Accessed: 26-May-2021])

Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology

Due to the challenge of sharing of medical records between participants that the data might be revealed or tampered during the operational process, this paper introduced secure electronic medical records storage and sharing using blockchain technology. Hyperledger is also introduced in this paper to ensure privacy, security and easy accessibility and availability of medical records, in order to solve public healthcare issues. The information stored in medical records is highly sensitive and private. Furthermore; this technology is thought to be helpful with case referring as it creates flexibility, efficiency and has less error-prone.

Methods:

Blockchain Technology

Conclusion

This paper has proposed a blockchain based Electronic Medical Records Management System. It stores and shares the medical records effectively. This solution ensures the security and privacy of patients' medical records by using permissioned blockchain platform. Lastly, patients can play an active role in management of their medical records and can control who can add new records and can view their medical history. (M. Usman and U. Qamar, "Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology," Procedia Computer Science, 27-Jul-2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920316136. [Accessed: 26-May-2021])

Conclusion

Blockchain technology has become popular and used in many fields. Therefore, Blockchain technology is applied in medical field, in order to enhance security, privacy and for other profits. There are frameworks on how Blockchain technology is used in Electronic Medical Records (EMRs) and some are mentioned in this paper. Blockchain is expected to be helpful by applying it in the original systems. This paper provides seven frameworks about Blockchain technology and Electronic Medical Records (EMRs). Furthermore; the background information, methods and the results are also mentioned in this paper. In order to be understood easily, this paper is written briefly by extracting the main points of each paper. In conclusion, Blockchain technology has many essential abilities for Electronic Medical Records (EMRs). Despite some limits, for instance; users' ability to understand Blockchain technology, the speed of the process etc. The technology is expected to be the future tool for more effective systems.

References

1. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient Medical Record management," Nature News, 06-Jan-2020. [Online]. Available: https://www.nature.com/articles/S41746-019-0211-0. [Accessed: 26-May-2021]
2. "A Blockchain-Based Secret-Data Sharing Framework for ..." [Online]. Available: https://res.mdpi.com/d_attachment/healthcare/healthcare-09-

Volume 4, Issue 3; May-June 2021; Page No 973-981

00206/article_deploy/healthcare-09-00206.pdf. [Accessed: 26-May-2021]

3. A.Lipton and S. Levi, "An Introduction to Smart Contracts and Their Potential and Inherent Limitations," The Harvard Law School Forum on Corporate Governance, 26-May-2018. [Online]. Available: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent- limitations/. [Accessed: 26-May-2021]
4. D. N. Network, D. Nuez, Network, I. A. Network, I. Agudo, J. L. Network, J. Lopez, Contributor MetricsExpand All David Nuez Universidad de Malaga Publication YeARS2017 - 2017Publication cou, David Nuez Universidad de Malaga Publication YeARS2017 - 2017Publication counts1Available for Download0Citation count1Downloads (cumulative)0Downloads (6 weeks)0Downloads (12 months)0Average Citation per Article1Av, and Authors:
5. D. Tith, J.-S. Lee, H. Suzuki, W. M. A. B. Wijesundara, N. Taira, T. Obi, and N. Ohyama, "Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability," Healthcare Informatics Research, 31-Jan-2020. [Online]. Available: https://www.e-hir.org/DOIx.php?id=10.4258%2FhiR.2020.26.1.3. [Accessed: 26-May-2021]
6. David Nuez Network, "Proxy Re-Encryption," Journal of Network and Computer Applications, 01-Jun-2017. [Online]. Available: https://dl.acm.org/doi/10.1016/j.jnca.2017.03.005. [Accessed: 26-May-2021]
7. "Defining the Personal Health Record," Defining the Personal Health Record / AHIMA, American Health Information Management Association. [Online]. Available: https://library.ahima.org/doc?oid=59377#.YJT-QrUZY2W. [Accessed: 26- May-2021]
8. "EMR vs EHR – What is the Difference?," Health IT Buzz, 26-Aug-2011. [Online]. Available: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference. [Accessed: 26-May- 2021]
9. "Hyperledger Fabric," Hyperledger, 29-Jun-2020. [Online]. Available: https://www.hyperledger.org/use/fabric. [Accessed: 26-May-2021]
10. J. Frankenfield, "Permissioned Blockchains," Investopedia, 19-May-2021. [Online]. Available: https://www.investopedia.com/terms/p/permissioned-blockchains.asp#:~:text=What%20Is%20a%20PermissionED%20Blockchain,from%20public%20and%20private%20blockchains. [Accessed: 26-May-2021]
11. L. Conway, "Blockchain Explained," Investopedia, 06-May-2021. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: 26-May-2021]
12. M. Usman and U. Qamar, "Secure Electronic Medical Records Storage and Sharing Using Blockchain Technology," Procedia Computer Science, 27-Jul-2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920316136. [Accessed: 26-May-2021]
13. P. V. Kakarlapudi and Q. H. Mahmoud, "A Systematic Review of Blockchain for Consent Management," Healthcare (Basel, Switzerland), 01-Feb-2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7912759/?fbclid=IwAR194aEyYzhhghxEk7lJwNA7zzMkjaV6EFwiktv8qrT7jv1sWLx7j8TOq3s. [Accessed: 26-May-2021]
14. Q. Qin, B. Jin, and Y. Liu, "A Secure Storage and Sharing Scheme of Stroke

Volume 4, Issue 3; May-June 2021; Page No 973-981

Electronic Medical Records Based on Consortium Blockchain," BioMed research international, 01-Feb-2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7875637/?fbclid=IwAR18UsQQosTQTtx3w7kWhyoU-o64uMS5JE4FrHcrSyGJZSVABajh_d-Rsu8. [Accessed: 26-May-2021]

15. Remote Procedure Call (RPC). [Online]. Available: https://www.tutorialspoint.com/remote-procedure-call-rpc. [Accessed: 26-May-2021]
16. S. Daley, "How Using Blockchain in Healthcare Is Reviving the Industry's Capabilities," Built In. [Online]. Available: https://builtin.com/blockchain/blockchain-healthcare-applications-companies. [Accessed: 26-May-2021]
17. S. J. R. L. W. S. Y. X; "A blockchain-based framework for electronic medical records sharing with fine-grained
18. access control," PloS one. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/33022027/. [Accessed: 26-May-2021]
19. Y. Zhuang, L. Sheets, Z. Shae, J. J. P. Tsai, and C.-R. Shyu, "Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials," AMIA ... Annual Symposium proceedings. AMIA
20. Symposium, 05-Dec-2018. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6371378/?fbclid=IwAR0fmHgWE4WASGO_C8VG6eRpKQpKQtJfFMgGeoncEE4EpGEPQyXOiNo0uAA. [Accessed: 26-May-2021]

Volume 4, Issue 3; May-June 2021; Page No 973-981