Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2425-2434
Received 25 April 2021; Accepted 08 May 2021.

Towards Trustworthiness of Electronic Health Record system using Blockchain

Faheem Ahmad Reegu[1, 2], Salwani Mohd[1], Zaid Hakami[2], Kaiser Kariem Reegu[3], Shadab Alam[2*]

[1]Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia
[2]College of Computer Science & IT, Jazan University, Jazan, Saudi Arabia, 45142
[3]Sher-i-Kashmir Institute of Medical Sciences, Kashmir
Email: [2*]snafis@jazanu.edu.sa

ABSTRACT

The digital archive of the patient's personal health records is the Electronic Health Record (EHR) that has various advantages. For finding the best solution to resolve the associated issues, a detailed study is required to utilize modern technologies and standards so that these issues and errors can be minimized. There are several issues associated with implementing the EHR, including data management, privacy, and patient data security. This research aims to examine the use of the Blockchain in EHR frameworks as per the national and international standards of EHR to reduce the associated issues. A blockchain-based framework can be successful in solving the current challenges in EHR. It allows storing, sharing, managing, controlling, and maintaining patient information between healthcare providers. The study illustrated the related difficulties of integrating EHR and proposed Blockchain as a solution to help manage the records and preserve privacy, confidentiality, usability and protection of patient-related details. This study helps to understand the current challenges better and help in the proper implementation of Blockchain technology in EHR.

Keywords:

Healthcare; EHR; Blockchain; Privacy; Security

1. Introduction

As the healthcare sector has evolved rapidly across electronic health records (EHR), remote patient tracking (RPM) and technologies for population health management are significantly dependent on information technology (IT) [1][2]. The medical data provided by such mediums are huge and voluminous that create issues of data accuracy, complexity in data analysis, chances of privacy leakage and correct diagnosis and disease identification [3][4]. Because of the substantial assets reported from their perspective, hospital notes or medical documents have shown their relevance to patients. While it can increase diagnostic efficacy by sharing EHR patient data between different healthcare facilities, archiving clinical records can become a single point of failure. It is necessary to pursue attackers leading to ransomware attacks or service denials. In healthcare applications, data protection is also an essential feature and crucial to maintaining the security and privacy of sensitive health data. The healthcare experts require confidential records that cannot be revealed to third parties that possess privacy risks and data misuse. A collection of health information in medical archives collected from the start of patient injury through recovery requires this specific type of data. Consequently, this function will contribute to the exposure of patient details that do not conform with the provisions of the Portability and Transparency Act on Health Insurance 1996 (HIPAA) [5]. However, it is exceptionally necessary to exchange and view medical history in EHR to obtain smart and specialized medical services [6][7].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2425-2434
Received 25 April 2021; Accepted 08 May 2021.

Emerging technical breakthroughs in blockchain and smart contracts, while being exchanged and accessed via EHR, are supposed to offer exciting solutions to safe patient data. Integrating the blockchain healthcare infrastructure will substantially add to human wellbeing [8]. Multiple signatures between patients and service providers may be approved through smart contracts, enabling only authorized personnel or devices to view or connect with the registered EHR data [9]. It will ensure the authenticity of the records and support anonymity for the patients. In addition, smart contracts will include links to personal health details (PHI) for researchers and facilitate automated monetary transfers to assist users and organizations operating [10].

2. Overview of Blockchain

This technology was proposed by Satoshi Nakamoto in 2008 and was implemented in bitcoin cryptocurrency [11]. Blockchain technology is a decentralized distributed ledger that can store and share data securely and reliably. Records are kept anonymously and readily available to the users in a distributed manner, making it easier for community participants to view their history. Blockchain cryptology transforms trust trustees into third-party actors, yet all groups use complex algorithms to preserve entry credibility [12] [13]. This innovation provides HIE with another paradigm when trying to decentralize EHRs, improving the system's stability and security along these lines. In blockchain growth, consistency tools, digital databases and public-key cryptography are central elements [14][15]. Because of the following, blockchain technology has attracted significant business and research interest:

- **Decentralized Storage:** With the sender's permission, Blockchain easily stores data and moves it to third parties. Perhaps the most practical methods for ventilating data stockpiling are to store multiple duplicates of this information in several fields.
- **Consent:** calculations control the entrance, stockpiling and If all gatherings to the organization consent to this choice, information changes are permitted.
- **Immutability:** We can't adjust the data. If the data is put away in a particular square of the chain, further changes or modifications are not permitted [16].

1.1 Blockchain types for the healthcare

The blockchain design demonstrates the way for sharing or authentication between hubs operating in the enterprise. The Blockchain is associated with individuals from various corners and is now familiar with the company; approvals such as Hyperledger texture [17]and swell [18] are referred to as the Blockchain. Since the protocol is generally available to individuals, each individual or corporate centre can be an individual from the company; these blockchains, such as Ethereum and Bitcoin, are often designed to be freely accessible [19].

- **Public Blockchain**
  A public blockchain is seen as an unapproved record if anyone can access the organization's hubs over the Internet (for example, Bitcoin or Ethereum).
- **Permissioned Blockchain (Private)**
  The relative return of the average entity is allowed by this kind of restricted Blockchain. Strictly regulate data connectivity on private blockchain networks.
- **Consortium blockchain (federated)**

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2425-2434
Received 25 April 2021; Accepted 08 May 2021.

It is a combination of public-private blockchain union, which can be seen as half-decentralized. Each information exchange can be public or private in the blockchain business, and hubs reserve the choice to choose.

3. Electronic Health Record

Approach to the collection of consistent knowledge from medical care providers (for example, emergency clinics). Nevertheless, the EHR scheme's current privacy and security concerns restrict the provision of data summaries of specific patients from separate healthcare provider databases. EHR systems are increasingly being used as an easy way of exchanging medical information between different healthcare entities [20][21]. However, it is also challenging to obtain required patient records from different EHRs, as the existing EHR databases are linked explicitly with a designated healthcare provider or limited to a regional boundary. They usually are based on centralized storage architecture that is prone to many security issues [22]. Based on the study released by the Office of the National Coordinator for Health Information Technology (ONC) [23], it is challenging to locate the addresses of the provider to determine the key hurdle to obtaining patient cords. Many projects attempt to address these issues, but the proposals developed by these projects are complicated and include restructuring or improving current EHR structures, which will entail considerable costs. They use a consolidated mechanism allowing patients and clinicians to scan for the dispersed medical history of a patient [24].

3.1 Issues in Electronic Health Record (EHR)

In summary of Table 1, electronic health records software has serious privacy concerns, which can be a vulnerable target for hackers. Central authorization, presentation of sensitive information of the patients, management, and scaling of a large volume of data are significant EHR challenges. Other risks are related to data integrity, sharing, tracking, and data reliability [25]. These challenges must be catered at first. Otherwise, hospitals may face lawsuits from their patients if any serious hacking issues will be raised. Hence, the software is needed to be updated, calibrated and verified so that the risks can be minimized.

Table1: Issues of EHR

S. No.	Ref	Issues in EHR
1	[26]	Security issue
2	[27]	Security and data integrity
3	[28]	Data sharing and privacy
4	[29]	Data sharing and privacy
5	[30]	Data integrity
6	[31]	Privacy
7	[32]	Central authorization
8	[33]	Incompatibility of different EHR representations
9	[34]	The complexity of the audit log
10	[35]	N/A
11	[36]	Central Authorization

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2425-2434
Received 25 April 2021; Accepted 08 May 2021.

12	[37]	Privacy
13	[38]	Security and data control
14	[39]	Privacy and access control
15	[40]	Safety, tracking, and reliability of data at systems
16	[41]	Scalability issues with the high volume of data

4. Blockchain in EHR

Blockchain highlights have many benefits in many business areas and can be a powerful instrument in implementing the medical care sector. Nonetheless, if the application does not need decentralization, blockchain innovation may not be the correct decision to take care of each business challenge [42]. If it is necessary to decentralize the software, blockchain innovation can be helpful. Today, in healthcare outcomes, this enthusiasm and resources have ventured into innovation. In 2016, the Office of the National Health Information Technology Coordinator published a white paper on the conceivable usage of Blockchain in medical services, perceiving the likely utility and importance of Blockchain in medical services. In light of this test, many proposed welfare strategies for Blockchain are proposed. Although the whole wellbeing record on the Blockchain would be put aside, it may be seen as a case in medical treatment utilization. Some possible deterrents to adoption, such as security and accuracy issues [43][44], have been established. The storage and distribution of documents require institutional standards and technical difficulties. Most temporary recommendations thus focus on awareness acceptance, analysis, and endorsement. An indication of usage is Guard Time, a Netherlands-based information technology organization, partnering with the Estonian government to set up a blockchain-based patient character validation structure [45][46]. All residents have a smart card that links a blockchain-based identity to EHR records. All DSE refreshes are hashed on the Blockchain and are registered. This strategy means that an unchanging review trail is contained in the EHR details and that the library is not malevolently adapted. Immovable history logs that are time-stamped will store records from current patient files and updates to the hospital website, such as appointment preparation, time stamping, and encrypting and signing blocks.

The Department of Veterans Affairs has recently focused on data transparency due to questions about counterfeit schedules and the possibility of data misuse of amputation medical instruments such as pacemakers. These programs are medical. Maintaining secure and capable improvements to the healthcare record has some potential benefits. The second execution for the EHR was MedRec, an association with the MIT Media Lab and Beth Israel Deaconess Medical Center. This phase provides a decentralized approach for monitoring the distribution of permissions, powers and details between frameworks for Wellness [47][42]. The use of Blockchain is expected to enable patients to have the most influential operational capacity in this application and to know who can access details about their wellbeing. These permissions can be shared on the Blockchain to make it possible for a more computerized approach to sharing knowledge for clinical and research purposes, regardless of whether the true wellbeing data is not installed on the Blockchain. Although permissions for external space and bookkeeping pathways are maintained on the Blockchain, all clinical data remains in EHR frameworks and needs additional programming components to ensure genuine interoperability [47]. The MedRec project has been tested as a concept verification for drug specifics, and engineers are trying to update the issue by adding more sources of knowledge, contributors of information and users. As this proof of

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 6, 2021, Pages. 2425-2434
Received 25 April 2021; Accepted 08 May 2021.

concept suggests, blockchain technology can benefit significantly from biomedical research and findings exploration to provide quick and reliable access from longitudinal examinations to knowledge [48]. Blockchain in electronic health records (EHR) enables a safer system for storage, exchanging, management, fine-grained access protection, and medical information integrity. Interoperability of clinical insurance increases the speed with which doctors provide their patients with care and can support their patients navigate across the ecosystem of health care. Therefore, it has been found that it is feasible to utilize blockchain technologies to solve the problems associated with EHR implementation. Further research is, however, necessary for the proper validation of the blockchain-based EHRs.

5. Advantages of applying Blockchain in EHR

Blockchain in electronic health records (EHR) allows storing, sharing, management, fine-grained access control, and integrity of patient information through the safer mechanism. Providing interoperability in healthcare records will facilitate the ease of use for medical practitioners in providing diagnosis and healthcare support to their patients by accessing the patient's medical history. Hence, it has been identified that blockchain technology will help overcome the issues with traditional EHRs and support interoperability. However, further research is required for the proper validation of the EHRs based on Blockchain.

Table2: Advantages of Applying Blockchain in EHR

S. No	Reference	Advantages
1	[49]	1. Enhanced modularity 2. Scalability, Data integrity and Access control 3. Trust
2	[50]	1.Interoperability 2.High throughput 3.Low Latency
3	[47]	1. Security 2.Auditability
4	[51]	1. Security.
5	[52]	1. Sharing of data among untrusted parties. 2. Secure data provenance and auditing.
6	[53]	1.Scalable 2.Lightweight 3.Secure
7	[54]	1. Authentication 2. Confidentiality 3. Accountability
8	[55]	1. User management 2.Authorization 3.Record management

9	[56]	1.security
10	[57]	1.Scalability
11	[58]	1.Privacy and security
12	[48]	1. Better scalability, robustness and immutability 2.Protected data exchange 3.data privacy
13	[59]	1.Privacy
14	[60]	1. The anonymity of the DPS 2. Reduce the possibility of privacy disclosure.
15	[61]	1.Data management 2.Sharing
16	[62]	1. Data integrity.

6. Conclusion

EHR is the digital record of the medical history of the patient. It has solved many issues related to data transfer and storage. However, several issues associated with it are still not appropriately resolved. A detailed study is required under modern technology standards so that errors related to EHR can be identified and possible solutions can be made to minimize the associated issues. The previous literature has identified that EHR implementation is mired with numerous issues, including data management and privacy concerns; therefore, researchers need to improvise it. It has been identified that the Blockchain is a suitable technology to overcome the issues associated with the implementation of the EHR. This paper has provided a very detailed review and further highlighted the various advantages of blockchain application in the domain of EHR. Hence, blockchain-based methods can be applied to reduce the challenges in data management and security breaches in implementing EHR.

References:

[1] H. O. Alanazi, M. L. Mat Kiah, A. A. Zaidan, B. B. Zaidan, and G. M. Alam, "Secure topology for electronic medical record transmissions," *Int. J. Pharmacol.*, vol. 6, no. 6, pp. 954–958, 2010.

[2] O. H. Salman, A. A. Zaidan, B. B. Zaidan, Naserkalid, and M. Hashim, "Novel methodology for triage and prioritizing using 'big data' patients with chronic heart diseases through telemedicine environmental," *Int. J. Inf. Technol. Decis. Mak.*, vol. 16, no. 05, pp. 1211–1245, 2017.

[3] M. Hussain *et al.*, "Conceptual framework for the security of mobile health applications on android platform," *Telemat. Informatics*, vol. 35, no. 5, pp. 1335–1354, 2018.

[4] F. A. Reegu, M. O. Al-Khateeb, W. A. Zogaan, M. R. Al-Mousa, S. Alam, and I. Al-Shourbaji, "Blockchain-Based Framework for Interoperable Electronic Health Record," *Ann. Rom. Soc. Cell Biol.*, vol. 25, pp. 6486–6495, Mar. 2021, [Online]. Available: http://annalsofrscb.ro6486.

[5] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Compliance with HIPAA and GDPR in blockchain-based electronic health record," *Mater. Today Proc.*, no. xxxx, Mar. 2021, doi: 10.1016/j.matpr.2021.03.059.

[6] S. G. Alonso, J. Arambarri, M. Lopez-Coronado, I. de la Torre Diez, M. López-Coronado, and I. de la Torre Díez, "Proposing New Blockchain Challenges in eHealth," *J Med Syst*, vol. 43, no. 3, p. 64, Mar. 2019, doi: 10.1007/s10916-019-1195-7.

[7] F. Masoodi, S. Alam, and S. T. Siddiqui, "Security and privacy threats, attacks and

countermeasures in Internet of Things," *Int. J. Netw. Secur. Appl*, vol. 11, no. 02, pp. 67–77, 2019, doi: 10.5121/ijnsa.2019.11205.

[8] A. H. Mohsin *et al.*, "Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions," *Comput. Stand. Interfaces*, vol. 64, pp. 41–60, 2019.

[9] M. Shuaib, S. Alam, and S. M. Daud, *Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme*, vol. 1347. Springer Singapore, 2021.

[10] M. Shuaib, S. Alam, M. Shahnawaz Nasir, and M. Shabbir Alam, "Immunity credentials using self-sovereign identity for combating COVID-19 pandemic," *Mater. Today Proc.*, no. xxxx, Mar. 2021, doi: 10.1016/j.matpr.2021.03.096.

[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[12] M. Shuaib, S. M. Daud, S. Alam, and W. Z. Khan, "Blockchain-based framework for secure and reliable land registry system," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 5, pp. 2560–2571, Oct. 2020, doi: 10.12928/TELKOMNIKA.v18i5.15787.

[13] M. Shuaib, S. Alam, S. Daud, and S. Ahmad, "Blockchain-Based Initiatives in Social Security Sector," in *EAI 2nd International Conference on ICT for Digital, Smart, and Sustainable Development (ICIDSSD)*, 2021, p. 8, doi: 10.4108/eai.27-2-2020.2303256.

[14] M. U. Bokhari, S. Alam, and S. H. Hasan, "A Detailed Analysis of Grain family of Stream Ciphers.," *Int. J. Comput. Netw. Inf. Secur.*, vol. 6, no. 6, 2014.

[15] M. U. Bokhari and S. Alam, "BSF-128: a new synchronous stream cipher design," in *Proceeding of international conference on emerging trends in engineering and technology*, 2013, pp. 541–545.

[16] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Self-sovereign identity for healthcare using blockchain," *Mater. Today Proc.*, no. xxxx, Mar. 2021, doi: 10.1016/j.matpr.2021.03.083.

[17] E. A. A. B. V. Bortnikov *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in *EuroSys*, 2018, vol. 18.

[18] B. Chase and E. MacBrough, "Analysis of the XRP ledger consensus protocol," *arXiv Prepr. arXiv1802.07242*, 2018.

[19] MT Quasim, A Shaikh, M Shuaib, A Sulaiman, S Alam, and Y Asiri, "Smart Healthcare Management Evaluation using Fuzzy Decision Making Method," Apr. 2021, doi: 10.21203/RS.3.RS-424702/V1.

[20] T. Greenhalgh, S. Hinder, K. Stramer, T. Bratan, and J. Russell, "Adoption, non-adoption, and abandonment of a personal electronic health record: case study of HealthSpace," *Bmj*, vol. 341, 2010.

[21] B. A. Pandow, A. M. Bamhdi, and F. Masoodi, "Internet of Things: Financial Perspective and Associated Security Concerns," *Int. J. Comput. Theory Eng.*, vol. 12, no. 5, 2020.

[22] A. Raghuvanshi, U. Kumar Singh, M. Shuaib, and S. Alam, "An investigation of various applications and related security challenges of Internet of things," *Mater. Today Proc.*, no. xxxx, Mar. 2021, doi: 10.1016/j.matpr.2021.01.821.

[23] Y. Pylypchuk, C. Johnson, J. Henry, and D. Ciricean, "Variation in Interoperability among US non-federal acute care hospitals in 2017," *ONC Data Br.*, vol. 42, pp. 1–15, 2018.

[24] I. Abrar, Z. Ayub, and F. Masoodi, "Current Trends and Future Scope for the Internet of Things," *Internet Things Bus. Transform. Dev. an Eng. Bus. Strateg. Ind. 5.0*, pp. 185–209, 2021.

[25] M. Shuaib, S. M. Daud, and S. Alam, "Self-sovereign Identity framework development in compliance with Self sovereign Identity principles using components," *Int. J. Mod. Agric.*, vol. 10, no. 2, p. 2021, May 2021.

[26] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, p. 102481, 2020, doi: 10.1016/j.jnca.2019.102481.

[27] Y. Meng, Z. Huang, G. Shen, and C. Ke, "SDN-Based Security Enforcement Framework for Data

Sharing Systems of Smart Healthcare," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 308–318, 2019.

[28] H. van der Linden, D. Kalra, A. Hasman, and J. Talmon, "Inter-organizational future proof EHR systems. A review of the security and privacy related issues," *International Journal of Medical Informatics*, vol. 78, no. 3. Elsevier, pp. 141–160, Mar. 2009, doi: 10.1016/j.ijmedinf.2008.06.013.

[29] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, no. September 2019, pp. 311–335, 2020, doi: 10.1016/j.comcom.2020.02.018.

[30] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: a survey," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 746–789, 2019.

[31] G. Ramu, B. E. Reddy, A. Jayanthi, and L. V. N. Prasad, "Fine-grained access control of EHRs in cloud using CP-ABE with user revocation," *Health Technol. (Berl).*, vol. 9, no. 4, pp. 487–496, 2019.

[32] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, vol. 154. Elsevier Ltd, p. 113385, Sep. 2020, doi: 10.1016/j.eswa.2020.113385.

[33] W. Bani Issa *et al.*, "Privacy, confidentiality, security and patient safety concerns about electronic health records," *Int. Nurs. Rev.*, pp. 1–13, 2020, doi: 10.1111/inr.12585.

[34] Ε. Καραμητρούσης *et al.*, "Ο ρόλος της ανοσοθεραπείας στον καρκίνο των ωοθηκών Περίληψη Corresponding author," *Τόμος 2|Τεύχος*, vol. 4, pp. 1–34, 2016.

[35] N. Huynh, M. Frappier, H. Pooda, A. Mammar, and R. Laleau, "SGAC: A Multi-Layered Access Control Model with Conflict Resolution Strategy," *Comput. J.*, vol. 62, no. 12, pp. 1707–1733, 2019, doi: 10.1093/comjnl/bxz039.

[36] C. Huang, S. Wei, and A. Fu, "An Efficient Privacy-Preserving Attribute-Based Encryption with Hidden Policy for Cloud Storage," *J. Circuits, Syst. Comput.*, vol. 28, no. 11, p. 1950186, 2019.

[37] E. Sundvall, A. Terner, H. Broberg, and C. Gillespie, "Configuration of Input Forms in EHR Systems Using Spreadsheets, openEHR Archetypes and Template," *Stud. Health Technol. Inform.*, vol. 264, pp. 1781–1782, 2019, doi: 10.3233/SHTI190645.

[38] E. Lau, "Decoding the hype: Blockchain in healthcare," no. June, 2018.

[39] E. Saweros and Y.-T. Song, "Connecting Personal Health Records Together with EHR Using Tangle," in *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, 2019, pp. 547–554.

[40] G. I. Fragapane, A. B. Bertnum, H. Hvolby, and J. O. Strandhagen, *Medical Supplies to the Point-Of-Use in Hospitals. In: Ameri F., Stecke K., von Cieminski G., Kiritsis D. (eds) Advances in Production Management Systems. Towards Smart Production Management Systems.*, vol. 567, no. November. Springer International Publishing, 2019.

[41] F. A. Satti, W. A. Khan, G. Lee, A. M. Khattak, and S. Lee, "Resolving Data Interoperability in Ubiquitous Health Profile using semi-structured storage and processing," in *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 2019, pp. 762–770.

[42] F. Reegu *et al.*, "A Reliable Public Safety Framework for Industrial Internet of Things (IIoT)," in *2020 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET)*, Nov. 2020, pp. 189–193, doi: 10.1109/ICRAMET51080.2020.9298690.

[43] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

[44] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, no. August 2017, pp. 283–297, 2018, doi: 10.1016/j.scs.2018.02.014.

[45] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th*

international conference on e-health networking, applications and services (Healthcom), 2016, pp. 1–3.

[46] F. A. Reegu, S. M. Daud, S. Alam, and M. Shuaib, "Blockchain-based Electronic Health Record System for efficient Covid-19 Pandemic Management," 2021, doi: 10.20944/preprints202104.0771.v1.

[47] 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*, Aug. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[48] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. S. Tavares, and V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cogn. Syst. Res.*, vol. 52, pp. 1–11, 2018.

[49] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, 2018, doi: 10.1016/j.csbj.2018.07.004.

[50] Y. Wu, Z. L. Jiang, X. Wang, S.-M. Yiu, and P. Zhang, "Dynamic data operations with deduplication in privacy-preserving public auditing for secure cloud storage," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 2017, vol. 1, pp. 562–567.

[51] B. Sharma, R. Halder, and J. Singh, "Blockchain-based Interoperable Healthcare using Zero-Knowledge Proofs and Proxy Re-Encryption," in *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2020, pp. 1–6.

[52] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[53] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, 2017.

[54] E. Meinert, "Implementing Blockchains for Efficient Health Care: Systematic," *J Med Internet Res*, vol. 21, no. 2, p. e12439, 2019.

[55] J. Chen, X. Ma, M. Du, and Z. Wang, "A blockchain application for medical information sharing," in *2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE)*, 2018, pp. 1–7.

[56] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *2018 27th International conference on computer communication and networks (ICCCN)*, 2018, pp. 1–9.

[57] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *2018 21st Euromicro conference on digital system design (DSD)*, 2018, pp. 699–706.

[58] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the design of a blockchain-based system to facilitate healthcare data sharing," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 1374–1379.

[59] X. Zhang and S. Poslad, "Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR)," *IEEE Int. Conf. Commun.*, vol. 2018-May, 2018, doi: 10.1109/ICC.2018.8422883.

[60] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, 2018.

[61] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data

sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–11, 2018.

[62] S. Rahmadika and K.-H. Rhee, "Blockchain technology for providing an architecture model of decentralized personal health information," *Int. J. Eng. Bus. Manag.*, vol. 10, p. 1847979018790589, 2018.