EAI Endorsed Transactions
on Pervasive Health and Technology
Research Article EAI.EU

Electronic Medical Records Using Blockchain Technology

G. Sucharitha[1*], G. Sai Aditya[2], J. Varsha[3] and G. Sai Nikhil[3]

[1]Department of Data Science, Institute of Aeronautical Engineering College, Hyderabad, Telangana
[2,3]Department of Computer Science and Engineering, Institute of Aeronautical Engineering College, Hyderabad, Telangana

Abstract

Blockchain technology has emerged as a crucial tool for ensuring security and reliability in various domains, particularly in healthcare. In this study, we utilize blockchain to establish an append-only chain of transaction blocks, ensuring the integrity and security of patient medical records. By employing blockchain, we aim to safeguard patient data, grant specific clinicians' access to medical records, and ensure user privacy. The doctor will only receive prescription information after the patient has granted access, ensuring comprehensive protection for both parties. Consensus mechanisms within the blockchain guarantee consistency among blocks and require agreement from existing nodes before adding new transactions. Traditional healthcare systems often result in delays in data exchange and strict restrictions on access due to concerns about sensitive data leakage. By integrating blockchain technology into healthcare records and data, this article seeks to enhance data sharing while mitigating the risks of data tampering and security breaches.

Keywords: Blockchain, End-to-End Encryption, Distributed Ledger, Medical Records, One-time Upload, Easily Accessible

Received on 06 August 2023, accepted on 17 October 2023, published on 31 October 2023

Copyright © 2023 G. Sucharitha *et al.*, licensed to EAI. This is an open access article distributed under the terms of the CC BY-NC-SA 4.0, which permits copying, redistributing, remixing, transformation, and building upon the material in any medium so long as the original work is properly cited.

doi: 10.4108/eetpht.9.4284

1. Introduction

Recently, interest has grown for employing blockchain technology to enhance healthcare and e-health services [1]– [3]. The safe sharing of electronic health records is just one area in which blockchain has demonstrated significant potential. Control of data access for EMR between various medical groups [4]– [6]. Therefore, employing blockchain technology has the potential to offer solutions for accelerating healthcare delivery, revolutionising the healthcare industry.
Modern technologies like Mobile Cloud Computing (MCC) and the Internet of Medical Things, or IoMT, have significantly changed how the healthcare industry operates in terms of e-health [7]– [8]. People can now gather their own personal health data at home using mobile devices (such smartphones and wearable sensors) and share it in cloud environments, which physicians can instantly access to examine patient records and offer immediate medical help. By enabling medical professionals to remotely monitor patients and administer ambulatory care at home, this clever e-health solution optimises the delivery of healthcare while also offering patients financial aid. In addition, having a full EMR in the cloud enables monitoring patient health and provides relevant medical services during the phases of diagnosis and therapy [9].

Despite these great benefits, the move towards EMR storage on the cloud also sparks security questions, which makes it difficult to integrate e-health applications there [10]– [11]. The sharing of EMRs by patients and healthcare

*Corresponding author. Email: sucharithasu@gmail.com

professionals on mobile cloud systems is one of these security challenges. Without the patients' permission, unauthorised individuals may gain access to the EMR and do harm, which has a negative effect on the security, integrity, and privacy of cloud-based e-health systems [12]. Additionally, people may find it challenging to manage and follow the cloud-based health records supplied by healthcare providers. For systems that share a mobile cloud EMR, it's critical to provide effective access control solutions.

The conventional approaches to providing access control EMR assumes that data owners have complete confidence in the servers to manage all access control and authentication rights before deciding to provide cloud servers this authority. This premise is invalidated by the existence of sincere but inquisitive cloud servers in mobile clouds. The cloud server will legitimately respond to data requests while also illegally collecting consumer personal information, which has serious ramifications for network security and information leaks. Furthermore, because traditional access control solutions generally rely on a single cloud server, they can become the e-health networks' single biggest point of failure.

In the meanwhile, blockchain-based access control for e-health provides a variety of novel security features with important benefits over conventional access control techniques. As the first phase in the system for sharing data, the blockchain generates immutable transaction ledgers. As a result, business transactions can only be recorded on the blockchain; recovery activities are not permitted. No entity can modify or change records on the blockchain. As a result, System dependability and integrity are assured to be very high. In addition, blockchain-based access control can successfully address the problem of data escaping that can be brought on by intrepid servers, so promoting transparency and resolving the problem. Any illegal access to servers and data storage of other businesses will be reported to and recorded on the blockchain, alerting all network users. Any user of the blockchain can do this to manage data access and spot hazardous transactions so they can be stopped. Thirdly, the authentication and user verification functions will be made possible by employing smart contracts based on blockchain technology. Smart contracts effectively enable user access to the storage of health data by enforcing stringent access control criteria. Additionally, in a dispersed fashion, they can effectively recognise and neutralise potential threats to health networks.

Not to mention, the necessity for centralised servers to guarantee fairness among transaction parties can be eliminated when blockchain and smart contract technologies are combined. Each linked entity will have a copy of the smart contracts because they are public on the blockchain network, allowing them equal power over all contract actions. Due to the distributed nature of the system, which eliminates data loss, risks, or issues with confidence, blockchain-based access control in particular can continue to function properly even if one or more parties fail. We propose a unique EHR sharing model on a mobile cloud platform based on blockchain technology in this study as a result of these benefits of blockchain. Our suggested approach is built on a framework for user access management that governs how network entities can access data. Access control techniques can effectively prevent unauthorised users from using EHR resources while providing quick data retrieval for authorised parties.

In EMR, we use internet as a platform to communicate with the system so that we can access the servers of the EMR and retrieve the data. The EMR is so eco-friendly that the user can access within finger tips.

2. Related Work

Traditional strategies have been used to address the issue of secure EHR sharing in cloud platforms. For selective EHR sharing across different healthcare providers employing cloud computing, a broker-based access control mechanism was recommended in the study [13]. Their sharing concept was only tested in a computer simulation using virtual machines (VMs), therefore they neglected to consider how it would function on devices with limited resources, such cell phones. In order to meet the security requirements of e-health systems, the public key infrastructure (PKI) was used in the cloud to maintain authentication for medical users and the EMR sharing system [14].

The attribute-based encryption (CP-ABE) prototype used by the authors of [15] also utilised an attribute authority for distributing keys to data consumers in order to enable fine-grained access control for EMR sharing on the cloud. The potential of blockchain technology to simplify the exchange of e-health data has been looked at in certain research. In [16], blockchain technology was used to guarantee that trustworthy EMR were available to medical consumers. The authors used smart contracts to control how doctors used EMR. Because the authors concentrate on theoretical research, the viability of the suggested method hasn't been verified in actual EMR sharing scenarios. As a result, crucial EHR sharing characteristics including flexibility, accessibility, and identity management were not examined. Meanwhile, a blockchain-based data management idea was presented in [17] to assure safe EHR interchange among medical customers. A decentralised, blockchain-enabled solution was also put out to address the storage challenges associated with extensive medical records. The system MeDShare, it presented a solution to the problem of cloud service providers exchanging medical data. [18]. An access control framework that could trace data flows between untrusted parties, identify unauthorised access to EHR storage, and provide provenance and audits on medical data was created using smart contracts. The suggested system's performance was assessed only through network latency measurements and theoretical analysis, demonstrating that it may be used as a means of achieving effective data sharing with no potential for data privacy problems. An original user-centric approach to exchanging health data was presented by the authors in [19], and it has the potential

to improve identity management while protecting patients' privacy. They had not thought about the need for user authentication and identity management to safeguard data storage.

In order to better protect data accessibility and privacy on clouds, [20]'s engineers created a decentralised storage solution by fusing the Interplanetary File solution (IPFS), Ethereum blockchain, and attribute-based encryption (ABE) technologies. By employing these techniques, a data owner can create fine-grained access controls over cloud data by encrypting his data in accordance with established access laws and providing secret keys to users. The implementation of keyword searching in decentralised storage systems using smart contracts was created to solve the issue of standard cloud storage not accurately delivering search results. In order to demonstrate an improvement in data management, data search fairness on the cloud, and data privacy, the authors analysed the system design on the Rinkeby Ethereum official test network. Additionally, security studies were performed, and performance was assessed using cost tests for smart contracts. In order to enable data exchange in IoT scenarios, the authors of [21]– [23] provided models that combined the IPFS system with smart contracts, thus eliminating the issue of keeping enormous volumes of data on blockchain. IoT devices can now exchange data and connect with one another insecurely thanks to these designs.

Despite the optimistic results, these current initiatives have a few drawbacks. The Public Key Infrastructure (PKI), which can be fairly complicated and frequently requires expensive resources, is required by traditional access control systems when requesting external key authority [24]. This is done in order to facilitate safe EMR sharing. For the security of the medical records, the inventors of BLOSOM claimed to have utilised a cryptographic hash method [25]– [26].

The hyper ledger fabric is proposed by the authors of novel framework for privacy of the health records [27]. In order to provide customers confidence in the platform, the authors of Integration of Health Care 4.0 said that the usage of IoT has helped ensure the security and accessibility of medical records [28]– [29]. Confirmatory factor analysis is employed, in accordance with research done on patient data by the authors of an empirical study for blockchain-based information sharing platforms in electronic health records, to confirm the model's validity. An examination of least squares regression in two stages was conducted to address this [30].

These centralised EHR systems may also cause an unjustifiable delay in the delivery of medical services when many organisations want medical information. Second, the mechanisms currently in use restrict the amount of personal data that patients may access on cloud EHR systems. When using the current EHR sharing models, it might be difficult for patients to control who should have access to their medical records and to identify who should not. In reality, some licenced healthcare providers might attempt to utilise patient health data for their own immoral purposes, which could result in the exposure of confidential patient information. On the prospect of access control on EMR sharing in blockchain, no research has been done in real-world circumstances.

3. Proposed Work

This article aims to merge blockchain technology with healthcare records and data to increase data interchange without having to worry about data tampering or security breaches.

The functional requirements or overall descriptions document also contain information on the user interfaces, the operating system, the operational environment, the graphical requirements, and the design constraints. A comprehensive perspective of the project, including its strengths and weaknesses and solutions to them, is provided by the efficient use of requirements and implementation limits.

The application works on 3 modules. When the admin logins through his credentials, he has the privilege to add doctors and hospitals to this application. Then the doctor logins to his credentials he has a privilege to access the patient's records and he can add the prescription to it.

At first the patient needs to create his profile in this application and needs to sing in to his account to add his details. After adding his details, he has a right to send his records to the hospital of his choice and the record will be reflected to that hospital. When the doctor logins to his account, he will read all the data given by the patient and he will give prescription in the form of records. This representation is shown in Figure.

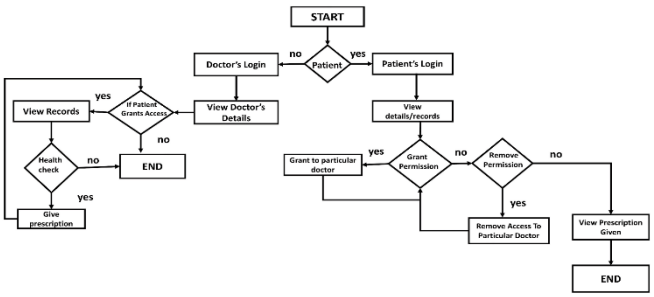

Figure1: Complete flow of the design

3.1. System Architecture

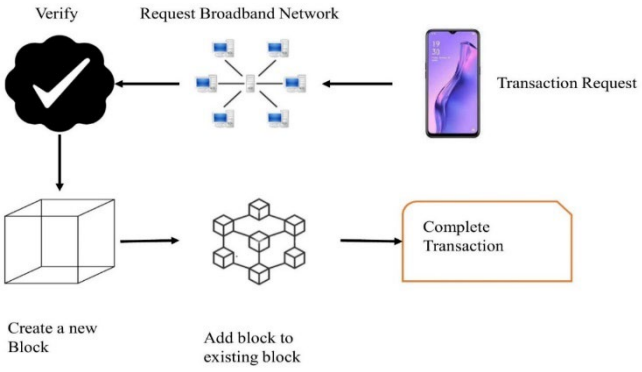

Figure 2: System Architecture

In accordance with the above-mentioned architecture, a user's request for a transaction is submitted to the broadcaster, a participant in the peer-to-peer network. After verification, the request will be converted into a new block of data and easily incorporated into the existing system. Connecting the new block to previous blocks completes the transaction, bringing the process to an end.

3.2 Implementation

Blockchain is gaining popularity across virtually all industries due to its inherent support for data integrity, dependability, and security. If hackers access healthcare data, which typically contain sensitive information like family diseases, patient sensitive disease information will be released or changed. Existing apps store data on a solitary, central server, and if this server is compromised or attacked, the server will be unable to supply any data.

The author of this paper introduces blockchain technology for the management of medical records as a solution to this issue. A blockchain maintains this data across various nodes or blockchain servers, stores all data as blocks or transactions, and gives each block a distinct hashcode. If one node or server fails, users can access services from other working nodes; the single centralized server does not currently provide this service. We have used SHA-256 Encryption and Decryption hashing algorithm in this paper is used to encrypt the data and to decrypt the data.

Data stored across several nodes can be accessed and shared by different users by granting each user access permissions. Patients can trade their data with multiple hospitals that have access privileges to the blockchain nodes, according to the study's author's idea.

1) We built Blockchain functions utilizing SOLIDITY code to manage healthcare data such patient disease reports and doctor details in order to put this idea into practice. Using the Python TRUFFLE Ethereum tool, we are deploying the aforementioned Solidity code on the blockchain. Once deployed, Python will be able to use the Solidity contract to access Blockchain services for storing and retrieving patient data. For patient functions, the screen below shows Solidity code.
2) Now, using the command below, we must execute the aforementioned code on Ethereum. Go inside 'hello-eth/node_modules/.bin' folder and then double click on 'runBlockchain.bat' file to get below window.

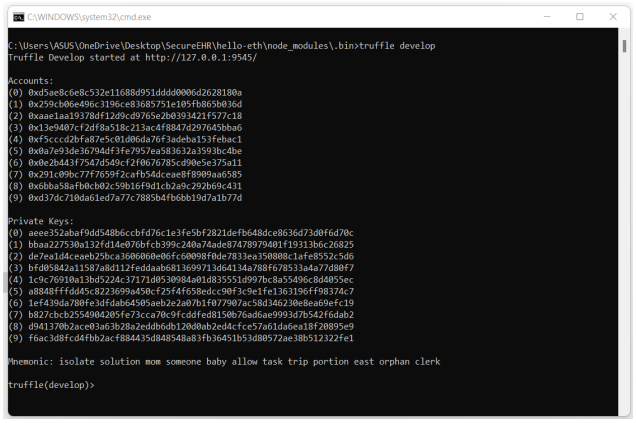

Figure 3: Private keys generated at the backend

In above screen, the application has generated some private keys and now type 'truffle migrate' command and press enter key to deploy Solidity EHR code on Ethereum and get below output

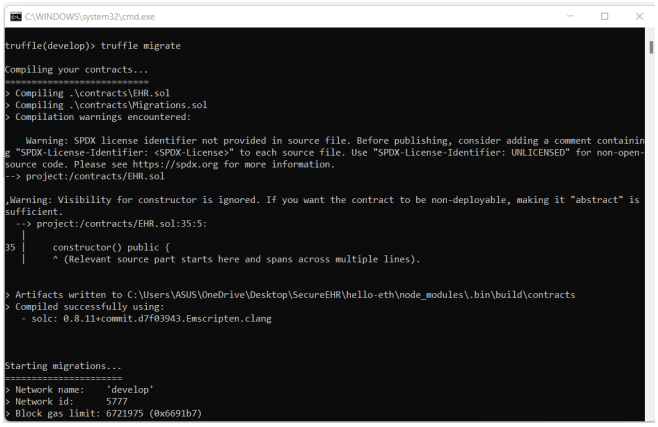

Figure 4: Migrate command

After we give migrate command, the console will start to develop the blocks as shown below.

Figure 5: Initial Migration

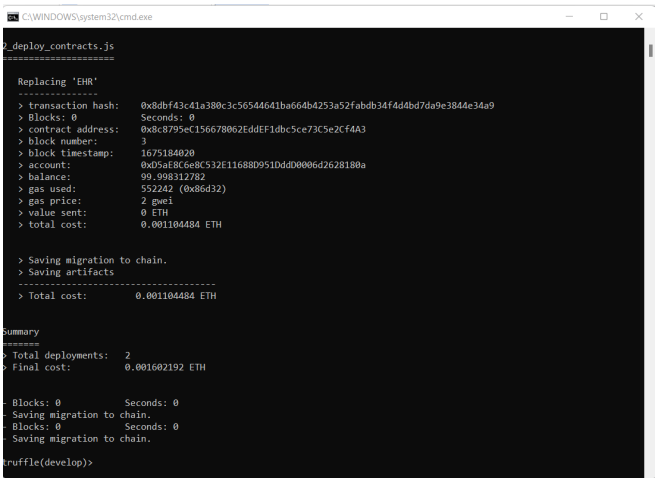

Figure 6: Summary

From the initial_migration.js we can see that how many blocks are created and the initial cost of the blockchain is shown. When we deploy contacts.js file it will generate block and it will calculate the remaining balance and the cost it has been taken to generate the file which are shown in Figure 5 and 6.

Here we can see how many numbers of blocks are generated, the network id, cost etc..,. After this step, go to the main folder and click on RUN batch file to generate the port to execute the application.

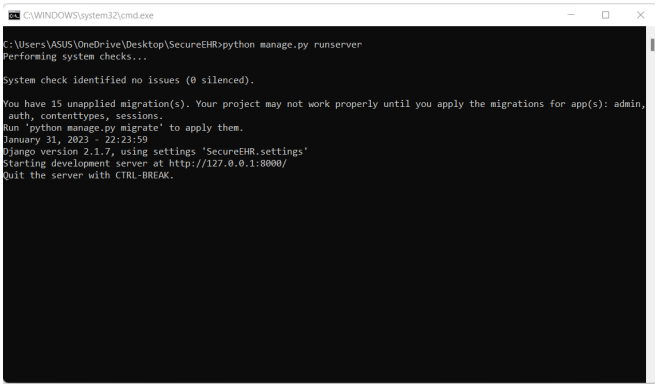

Figure 7: Run Console

Copy the server address and paste the path in which ever browser you need and add extension index.html to the url to go to the home page of the application.

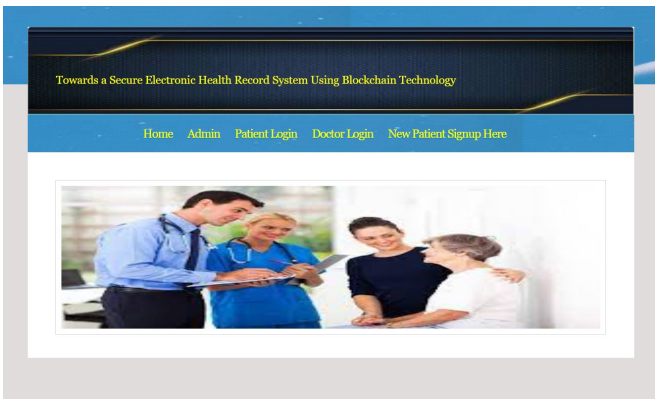

Figure 8: Home page of the EMR application

3.3 Modules

Modules Details: to implement this project we have designed the following modules

1. Admin Module: admin who can login to application by using username and password as ‘admin’, after login admin can add new Hospital and doctor details.
2. Doctor Module: using this module doctors from various hospitals can login to application and then can view all patients’ reports who has given permission to access their reports. Admin will give login details to doctors.
3. Patient Module: patient can sign up and login to application and then can add their health report and disease details. They can select multiple hospitals to share their reports with those hospital doctors.

3.4 Why not traditional system?

We used blockchain instead of traditional systems because of security features. The existing systems used HTML and the databases to connect to the architecture and implement it. With the old systems the hackers or the unauthorized persons can easily authorize the system and modify the contents of the records and use it as their convenience.

But in EMR, we use blockchain technology because it has a feature which enables the user to add the record. The added record will be non-editable and the record will link to other nodes to track the data so that no one can misuse the medical information.

4. Results

The EMR, is so friendly that it can be accessible using any device such as mobile, tablet or Fi even desktop. At first

the admin will create the doctor and add his details into the blockchain.

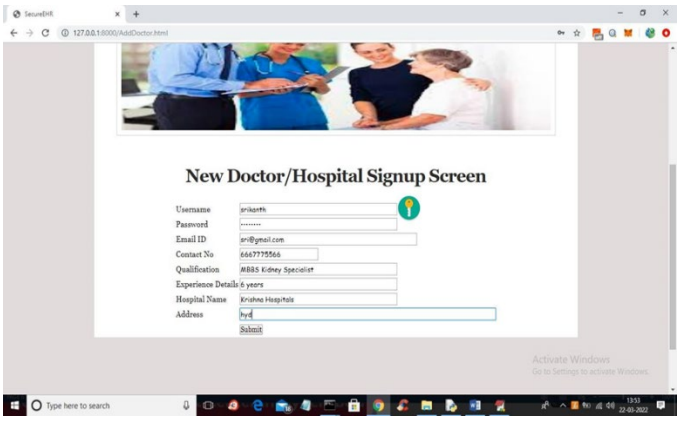

Figure 9: Admin adding doctor to EMR

When the patient registers and add his health records, then the records are encrypted with the help of private keys and it will be stored in the EMR.

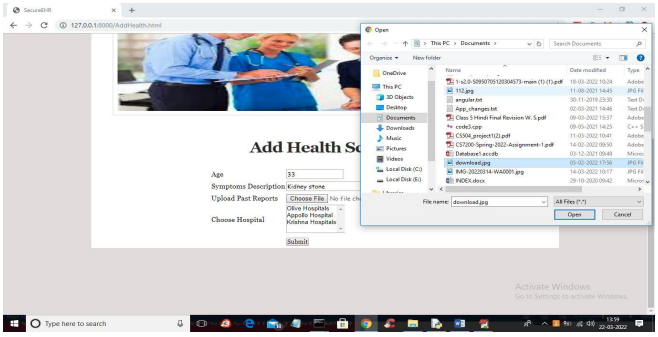

Figure 10: Patient adding the records

After adding the records, the patient chooses the hospital to share his/her records and then the affiliated doctor will react to the patient's records.

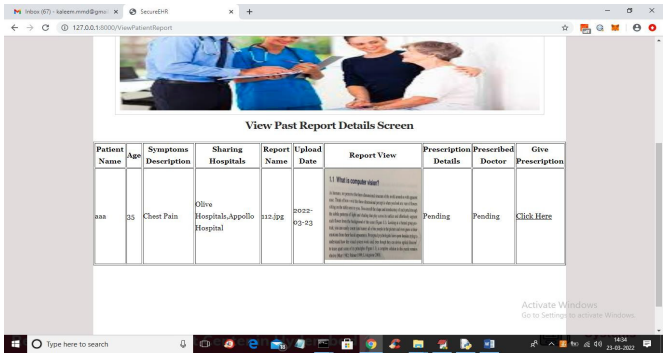

Figure 11: The records which is shared by the patient to the doctor before prescription

After sharing the records, the doctors will see the patient's previous health records and then will be generating the prescription based on those records. The doctor will click on "click here" button and then he will be redirected to the prescription page.

4.1. Results when we compare it to other systems

When we compare EMR with other electronic record systems, The EMR has low latency because we use iterative model rather than computational models. The iterative models work based on if else conditions. When the action required, it checks the condition if the condition is satisfied, then it will go to next step. If the condition failed it will not proceed. This will give us the time complexity of O(n), where n indicates number of conditions.
Some of the systems have space complexity. In EMR, we use cloud architecture to store the details. This will enable us to use EMR at any corner of the world. This will also provide low latency for the systems and will respond to the user queries quickly.

5. Conclusion

This article proposes an architecture and a mechanism for creating an EMR system based on blockchain. By utilizing blockchain's append-only structure and cryptographic hash function, patient medical records can be safeguarded and accessible to authorized clinicians. This approach ensures privacy for user data, allowing doctors to access information and prescribe appropriate treatments only after the patient grants permission. Consensus techniques in blockchain guarantee the consistency of transaction blocks and enable agreement among nodes to add new transactions. In traditional systems, personal healthcare information is stored separately by each hospital, leading to slow data exchange and strict access restrictions due to privacy concerns. A justification is also given for the kind of blockchain that can be applied in this case. The suggested methodology is put into practice using the Hyperledger fabric and Hyperledger composer tools.

References

[1] Mettler, Matthias. "Blockchain technology in healthcare: The revolution starts here." *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*. IEEE, 2016.

[2] Gordon, William J., and Christian Catalini. "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability." *Computational and structural biotechnology journal* 16 (2018): 224-230.

[3] Kuo, Tsung-Ting, Hyeon-Eui Kim, and Lucila Ohno-Machado. "Blockchain distributed ledger technologies for biomedical and health care applications." *Journal of the*

American Medical Informatics Association 24.6 (2017): 1211-1220.

[4] Hölbl, Marko, et al. "A systematic review of the use of blockchain in healthcare." *Symmetry* 10.10 (2018): 470.

[5] Jiang, Shan, et al. "Blochie: a blockchain-based platform for healthcare information exchange." *2018 ieee international conference on smart computing (smartcomp)*. IEEE, 2018.

[6] Dubovitskaya, Alevtina, et al. "Secure and trustable electronic medical records sharing using blockchain." *AMIA annual symposium proceedings*. Vol. 2017. American Medical Informatics Association, 2017.

[7] Islam, SM Riazul, et al. "The internet of things for health care: a comprehensive survey." *IEEE access* 3 (2015): 678-708.

[8] Lo'ai, A. Tawalbeh, et al. "Mobile cloud computing model and big data analysis for healthcare applications." *IEEE Access* 4 (2016): 6171-6180.

[9] Bahga, Arshdeep, and Vijay K. Madisetti. "A cloud-based approach for interoperable electronic health records (EHRs)." *IEEE Journal of Biomedical and Health Informatics* 17.5 (2013): 894-906.

[10] Meingast, Marci, Tanya Roosta, and Shankar Sastry. "Security and privacy issues with health care information technology." *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*. IEEE, 2006.

[11] AbuKhousa, Eman, Nader Mohamed, and Jameela Al-Jaroodi. "e-Health cloud: opportunities and challenges." *Future internet* 4.3 (2012): 621-645.

[12] Ghazvini, Arash, and Zarina Shukur. "Security challenges and success factors of electronic healthcare system." *Procedia Technology* 11 (2013): 212-219.

[13] Wu, Ruoyu, Gail-Joon Ahn, and Hongxin Hu. "Secure sharing of electronic health records in clouds." *8th international conference on collaborative computing: networking, applications and worksharing (CollaborateCom)*. IEEE, 2012.

[14] Ibrahim, Ahmed, Baban Mahmood, and Mukesh Singhal. "A secure framework for sharing electronic health records over clouds." *2016 IEEE International Conference on Serious Games and Applications for Health (SeGAH)*. IEEE, 2016.

[15] Ying, Zuobin, et al. "A lightweight policy preserving EHR sharing scheme in the cloud." *IEEE Access* 6 (2018): 53698-53708.

[16] Ramani, Vidhya, et al. "Secure and efficient data accessibility in blockchain based healthcare systems." *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018.

[17] Rifi, Nabil, et al. "Towards using blockchain technology for eHealth data access management." *2017 fourth international conference on advances in biomedical engineering (ICABME)*. IEEE, 2017.

[18] Xia, Q. I., et al. "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain." *IEEE access* 5 (2017): 14757-14767.

[19] Liang, Xueping, et al. "Integrating blockchain for data sharing and collaboration in mobile healthcare applications." *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE, 2017.

[20] Wang, Shangping, Yinglong Zhang, and Yaling Zhang. "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems." *Ieee Access* 6 (2018): 38437-38450.

[21] Chen, Yongle, et al. "An improved P2P file system scheme based on IPFS and Blockchain." *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, 2017.

[22] Steichen, Mathis, et al. "Blockchain-based, decentralized access control for IPFS." *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018.

[23] Ali, Muhammad Salek, Koustabh Dolui, and Fabio Antonelli. "IoT data privacy via blockchains and IPFS." *Proceedings of the seventh international conference on the internet of things*. 2017.

[24] Ausanka-Crues, Ryan. "Methods for access control: advances and limitations." *Harvey Mudd College* 301 (2001): 20.

[25] Johari, Rahul, et al. "BLOSOM: BLOckchain technology for Security of Medical records." *ICT Express* 8.1 (2022): 56-60.

[26] Shi, Shuyun, et al. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." *Computers & security* 97 (2020): 101966.

[27] Chenthara, Shekha, et al. "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology." *Plos one* 15.12 (2020): e0243043.

[28] Mahajan, Hemant B., et al. "Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems." *Applied Nanoscience* 13.3 (2023): 2329-2342.

[29] Abu-Rumman, Ayman, et al. "Entrepreneurial networks, entrepreneurial orientation, and performance of small and medium enterprises: are dynamic capabilities the missing link?." *Journal of Innovation and Entrepreneurship* 10.1 (2021): 1-16.

[30] Hajian, Ava, Victor R. Prybutok, and Hsia-Ching Chang. "An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective." *Computers in Human Behavior* 138 (2023): 107471.