G.Shanmuga Priya/ Afr.J.Bio.Sc. 6(5) (2024). 3103-3108 **ISSN: 2663-2187**

https://doi.org/ 10.33472/AFJBS.6.5.2024. 3103-3108

African Journal of Biological Sciences

SECURED EHR IMPLEMENTATION USING HYPER LEDGER FABRIC BLOCKCHAIN NETWORKS

G.Shanmuga Priya
Assistant Professor
Department of Computer Science,
Sri Krishna College of Technology,
Coimbatore – 641030,
Tamilnadu, India,
priyagsp1987@gmail.com

Dr.P.Tamije Selvy
Professor,
Department of Computer Science,
Hindusthan College of Engineering and Technology
Coimbatore – 641030,
Tamilnadu, India,
tamijeselvy@gmail.com

Abstract— An EHR (Electronic Health Record) is a digital patient's medical history representation , comprising details like medications, diagnoses, laboratory test results, allergies, treatment plans, and other relevant healthcare information. EHRs are created to be easily available to authorized healthcare providers and patients, enabling the exchange of information across various healthcare environments and enhancing the quality and effectiveness of healthcare services. Ensuring the high security and accuracy of healthcare data is the top priority of the healthcare industry due to its direct impact on human life. Storing this data on decentralized systems increases its susceptibility to attacks. Blockchain technology can play a crucial role in preserving data due to its decentralized nature and ability to offer an effective solution to data security risks. EHR can be implemented using the Ethereum public blockchain. Here in the proposed work, EHR is implemented using Hyperledger a permissioned blockchain hence providing security to the data.

Keywords*, Ethereum, EHR, Hyperledge, Smart contracts.*

1. INTRODUCTION

An EHR is a digital representation of a patient's medical background, involving details like medications, allergies, diagnoses, lab test outcomes, treatment strategies, and other major healthcare information. EHRs are made to be accessible to patients and authorized healthcare professionals. This allows information to be shared across various healthcare settings, enhancing the effectiveness and quality of healthcare delivery [1]. The features and components of an EHR system include:

Patient Demographics: Basic information about the patient, including name, date of birth, contact information, gender, and insurance details.

Medical History: Comprehensive medical history, including past illnesses, surgeries, hospitalizations, medications, allergies, and immunizations.

Clinical Notes: Narrative descriptions of patient encounters, involving diagnoses, symptoms, treatments, and plans of follow-up, typically entered by healthcare providers during patient visits.

Medication Management: Information about prescribed medications, including dosage, frequency, duration, and instructions for use. EHR systems may include features for medication reconciliation and alerts for drug interactions or contraindications.

Laboratory and Diagnostic Test Results: Results of laboratory tests, imaging studies, and other diagnostic procedures, often displayed in a structured format for easy review by healthcare providers.

Orders and Referrals: Electronic orders for medications, laboratory tests, imaging studies, consultations, and referrals to other healthcare providers or specialists.

Clinical Decision Support: Tools and features to assist healthcare providers in making clinical decisions, such as drug-drug interaction alerts, clinical practice guidelines, and reminders for preventive care and screenings.

Interoperability: Standards and protocols for sharing EHR data securely as well asefficiently across different healthcare organizations and systems, enabling coordinated care and continuity of patient information.

Security and Privacy: Measures to protect the confidentiality, integrity, and availability of patient data, including authentication, access control, encryption, audit trails, and compliance with healthcare privacy regulations which are HIPAA (in the United States) or GDPR (in the European Union).

Patient Portals: Online platforms or apps that enable patients to securely access their health records, book appointments, communicate with healthcare professionals, check test results, and manage their healthcare data.

Integration with Health Information Exchange (HIE): Connectivity with regional or national health information exchange networks, enabling the exchange of patient data between different providers of healthcare, hospitals, clinics, and other stakeholders.

Blockchain technology came into existence with the invention of Bitcoin in the year 2008 by S. Nakamoto [2]. There are various kinds of blockchains available. They are public blockchain as well as private blockchain. Some of the blockchains are discussed below :

Ethereum: Ethereum is a widely used blockchain platform recognized for its backing of smart contracts and decentralized applications (dApps). The platform provides a strong ecosystem and advanced development tools, making it ideal for building intricate systems such as Electronic Health Records (EHR). However, Ethereum's public blockchain may not be ideal for storing sensitive healthcare data due to privacy concerns.

Hyperledger Fabric: Hyperledger Fabric is a controlled access blockchain structure managed by the Linux Foundation. It offers features like scalability, privacy, and modular architecture, making it suitable for enterprise use cases, including healthcare. Fabric allows fine-grained access control, private transactions, and integration with existing enterprise systems, making it a good choice for implementing EHR systems with strict privacy requirements.

Corda: Corda is a distributed ledger platform designed specifically for businesses and enterprise use cases. It focuses on privacy, scalability, and interoperability, making it suitable for building EHR systems that require privacy-preserving features. Corda's design allows for secure sharing of data between parties while ensuring confidentiality and regulatory compliance.

Quorum: Quorum is an enterprise-focused blockchain platform built on Ethereum. It offers features such as privacy, permissions, and consensus mechanisms tailored for enterprise use cases. Quorum is suitable for implementing EHR systems that require privacy features while leveraging Ethereum's ecosystem and smart contract capabilities.

IBM Blockchain Platform: IBM offers a blockchain platform based on Hyperledger Fabric, designed for enterprise use cases. It provides features like privacy, security, and integration with existing systems, making it suitable for building EHR systems in healthcare organizations.

EOSIO: EOSIO is a blockchain platform known for its scalability, high transaction throughput, and low latency. It may be suitable for implementing real-time EHR systems that require high performance and scalability. However, privacy features may need to be carefully implemented to ensure data confidentiality.

2. LITERATURE REVIEW

Current EHR techniques for maintaining patient information include cloud-based and distributed systems, which offer various functions but also face financial challenges [3]. EHRs have been important in healthcare, but security and privacy issues have not been fully resolved. Researchers have utilized the Ethereum blockchain as well as cloud-based systems to address these concerns, as demonstrated in the literature [4]. Macdonald et al. [5] compared five significant blockchain platforms. Ethereum is one of these platforms. IBM Open Blockchain (OBC), Eris, Intel Swatooth Lake, and BlockStream Side Chain Elements have various limitations. Ethereum is recognized as leading the way in solving various issues, particularly scalability. In a study, Yu et al. [6] compared the use of HF as well as Ethereum frameworks with the MultiChain. These researches fail to address the utilization of blockchain platforms in the sector of healthcare. [6].

Jack Huang et.al.,[7] suggest a standardized EHR system for New Zealand. There is no standardized EHR system shared among major healthcare organizations in this country, like medical centers, hospitals, and specialists. Considering its features, blockchain technology is often an appropriate platform for constructing a larger-scale healthcare electronic records system for the country. They introduce MedBloc, a blockchain-powered secure EHR system which allows patients and healthcare providers to access as well as share health records in a user-friendly yet highly secure manner. MedBloc provides a patient's health history comprehensive view and enables patients to retrieve their medical records. MedBloc uses encryption and a structured access control system to safeguard clinical data. MedBloc is a comprehensive, patient-managed, collaborative Electronic Health Record system which enables patients as well as healthcare providers to access and also to share health records conveniently by a user-friendly interface. Patients can provide or withdraw permission at any time using precise agreements and cryptographic methods. Healthcare providers may require permission and store encrypted records securely on the blockchain. By utilizing a weak scheme of encryption. MedBloc's access control measures prevent unauthorized actions.

3.1 EXISTING SYSTEM

Ethereum and Hyperledger Fabric are two significant Blockchain frameworks. They have distinct functions. The Ethereum platform offers both public (permissionless) and private (permissioned) blockchains. HF, a decentralized framework, is better suited for permissioned blockchains and can run distributed applications (Dapps). Both Ethereum along Hyperledger Fabric frameworks offer excellent features to users. The framework of HF has been considered more secure compared to the Ethereum platform. [8]. The HF framework excels in confidentiality, identity, scalability, and performance features when compared to the Ethereum framework [9].

4. PROPOSED SYSTEM

Storing and sharing medical data is essential for all healthcare systems. Transferring personal data among different parties through insecure methods can result in the exposure of sensitive information. Insufficient user control over personal information can result in unauthorized individuals gaining access to or altering personal medical information. The key challenges in electronic health records involve ensuring interoperability among different entities. Data security and privacy represent challenges in the current methods of storing and exchanging information via EHR systems.

Electronic Health Records (EHRs) store patients' confidential data, including personal details like name, address, medical background, social security number, and insurance information. Patients' data is valuable to stakeholders, and exposure of public data has negative consequences. The proposed method utilized the Hyperledger Fabric framework to develop and evaluate different data security scenarios in order to minimize the effects of patients' data exposure [10]. It establishes limitations on network membership and transaction participation. The Hyperledger Fabric framework adheres to the GDPR (General Data Protection Regulation) and addresses multiple areas. Compared to other frameworks, it excels at preventing cyber-attacks and is especially well-suited for healthcare applications. It can be used by organizations or companies for its internal usage.

The proposed system maps fabric components to EHR systems. Organizations in the fabric are mapped to hospitals. Hospitals of the same interest are connected on the same channel. New hospitals will be connected once approved by the channel configuration of owner hospitals. The assets in fabric are patient data which are accessible all over the network. All the data have been kept in a blockchain database. The patient is responsible for making his data available to the doctor. The doctor can see the history of a patient to understand their condition and prescribe proper medication.

The blockchain stores the data that are cryptographically secure. Authentication along with the authorization are ensured by fabric by providing CA aas well as MSP components which provide secure entities like private keys and certificates and validation is done when the connection is made on the network. The decentralized nature of blockchain enables data to be accessible to all authorized systems. Because all records are immutable, data integrity is guaranteed.

pBFT consensus algorithm is used. pBFT aims to offer an economical Byzantine state machine replication which remains functional in the existence of malicious nodes within the system. In a pBFT-enabled distributed system, nodes have been arranged in a sequential order, with one node designated as the primary (or leader node) and the rest as secondary (or backup nodes). When a primary node doesn't work, any eligible node in the system could take over as the primary node by moving from secondary to primary. The objective is for all truthful nodes to contribute to achieving a consensus on the system's state through the majority rule.

Practical Byzantine Fault A tolerant system can operate as longer as the number of malicious nodes does not exceed 1/3 of all nodes in the system. As the quantity of nodes grows, the system's security improves.

Fabric provides history API which helps doctors to analyze a patient's history. New organizations, peers, and users with different roles can be added. Modules are pluggable.

The Architecture

The network is created by a blockchain operator. All network peers are running Docker containers.

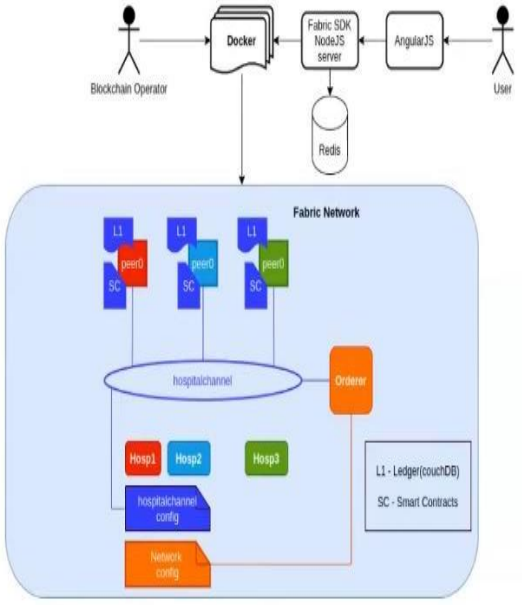

Fig 4.1 Architecture of EHR implemented using Hyperledger fabric

Figure 4.1 demonstrates the architecture of EHR implemented using Hyperledger fabric. The network is connected using Fabric SDK which is implemented using Java Script. The NodeJS is used to control the backend jobs. The front-end interface is developed using AngularJS. Redis-based database is used to store login credentials like username and password. Orderer in the organisation initiates the blockchain which means it creates the genesis block.

Hosp1 and Hosp2 form the channel. It is the initially created channel connected through the hospital configuration. Hosp3 is the additional channel. If Hosp3 wants to join the network Hosp1 and Hosp2 should give approval. Every hospital has its own peers. It contains one ledger and a smart contract. CouchDB is used for the ledger. Three smart contracts namely Admin, doctor, and patient are deployed in every peer.

ADMIN

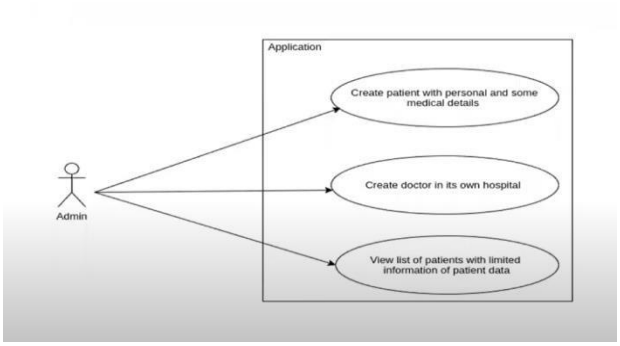

Fig 4.2 Use case diagram of admin

Figure 4.2 depicts the utilization of the case diagram of the Admin. The first module is admin. It's a simple module. It creates an application. It creates patients with personal and some medical details. It creates records of doctors in its own Hospital. Admin can view patient list. It can view only limited information on patient data.

Patient

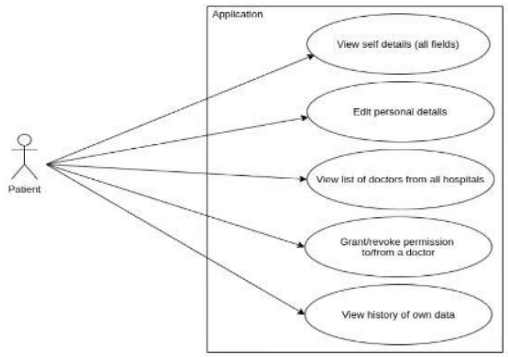

Fig 4.3 Use case diagram of Patient

The Fig 4.3 demonstrates the use case of the patient. The patient can view all his details, the self-details. The patient can edit all his personal information. He can view the doctor's list from all hospitals. Grand withdraws consent from a physician. view your own data's history.

Doctor

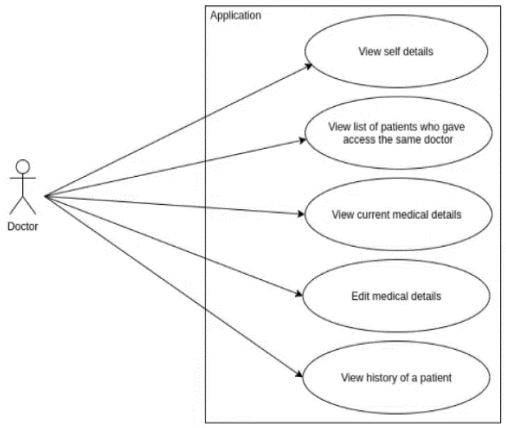

Fig 4.4 Use case diagram of doctor

Fig 4.4 describes the use case, the doctor. The doctor can access personal information. He is able to see the list of patients who granted permission to the same physician. He is able to access up-to-date medical information. He has the ability to edit medical information as well as access a patient's medical history.

Security Mechanisms

The EHR has two enhanced security mechanisms such as data re-encryption and private collections.

Private Collections

Hyperledger fabric provides security features for private collections.

Private collections = n!+1 number of the private collections

Where n denotes the number of hospitals and n private collections are available for each combination. Hosp1 will contain separate private collections. In Hosp2 data of Hosp1 and Hosp2 will be stored. If patient 1 visits hospital 1 his data is stored in the private collection of Hosp1. If the patient1 wants to visit hosp2 and if granted access the data is moved from the hosp1 private collection and moves to hosp2 private collections. The hospital can access the patient's details. The remaining data will be hashed and stored.

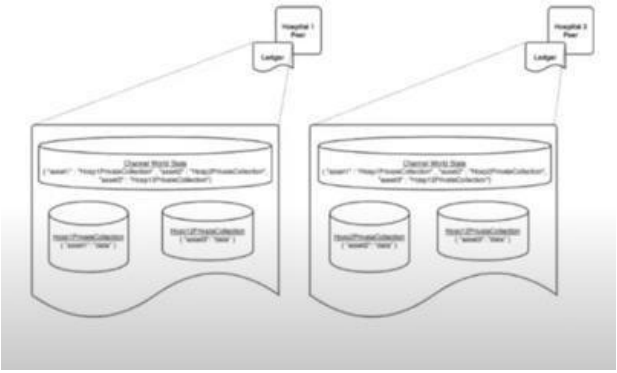

Fig 4.5 Private Collections

Data re-encryption

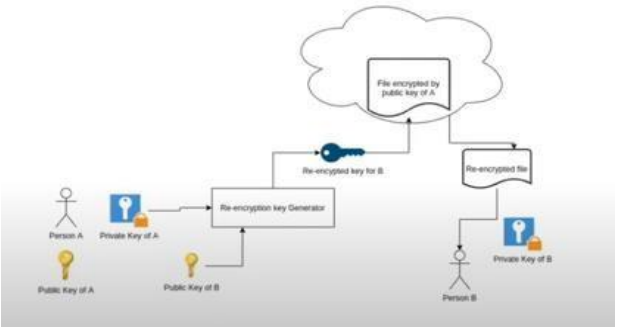

Fig 4.6 Data re-encryption

Smart Contract

Implementation

The application looks as if two servers the Backend server and the Front-end server are present. The user can choose the role. Admin, doctor, or patient can enter the hospital name and can enter the login credentials.

In the admin login list of patients, their first name and last name are available. Here the admin smart contract has been invoked and the patient ledger has been retrieved. The admin has permission to retrieve the patient's first name and last name. The smart contract is written such that the admin is blocked from other information about the patient.

New patient details can be added and saved by the admin. The patient object has been created. The patient detail acts as an entity as well as a valuable asset in the ledger. Temporary Password is given to the patient.

The patient goes to anyone in the hospital reaches the admin and provides the necessary details. The admin will invoke createAPI. The admin will connect the network and add the patient as the identity of the network. A certificate is generated for the patient and stored in the wallet. The patient wallet used is trusted by the network. FabricSDK will invoke the admin smart contract. The above transaction will be signed by the admin smart contract of the patient object and then sent to the adjacent peers with the temporary password.

Similarly, the admin will connect the network and add a doctor to the network. A certificate is generated for the doctor and stored in the wallet. The doctor wallet used is trusted FabricSDK which will invoke the admin smart contract. The above transaction will be signed by the admin smart contract of the doctor object.

The doctor is just an identity whereas else the patient is the identity and asset of the network.

Hospital admin page

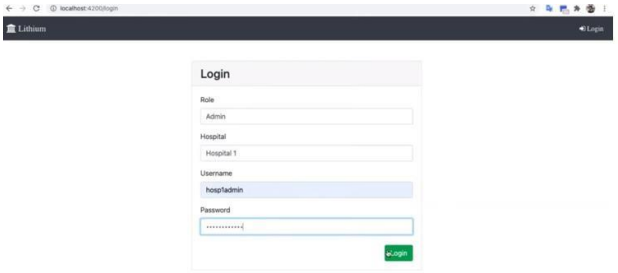

Fig 4.7 Admin page

The Fig 4.7 depicts screenshot is the implementation of the admin page in the Hyperledger blockchain. It contains Login credentials. It contains the options to choose the role, hospital, username, and password.

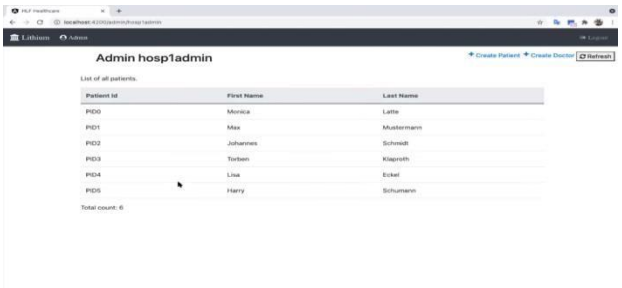

Fig 4.8 Hospital admin page

The above screenshot is the implementation of the Hospital admin page in the Hyperledger blockchain. The hospital admin page contains the patient's details such as patient identification, name, etc. There is an option to create new patient records.

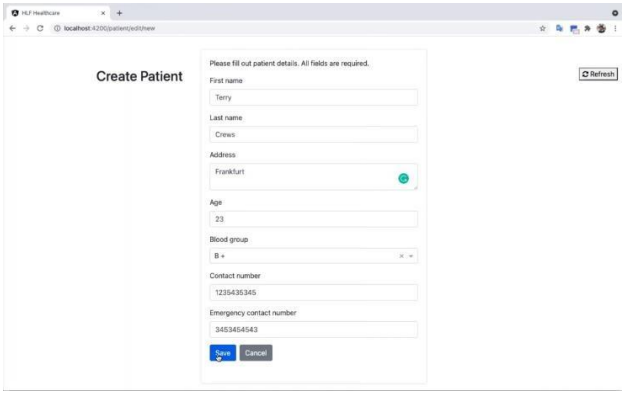

Fig 4.9 Patient page

Fig 4.9 is the screenshot of the create patient record page. It contains the option to register the name, address, age, blood group, contact information, etc.

Create doctor

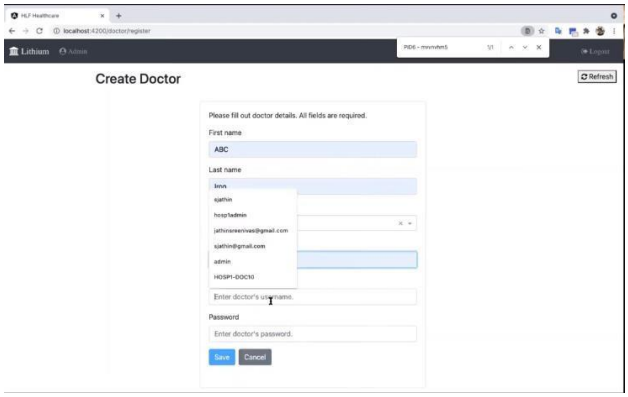

Fig 4.10 Doctor details

The above screenshot contains the options to collect and store the doctor's details such as Name, specialization, username, and password.

5. CONCLUSION AND FUTURE WORK

In conclusion, the implementation of Electronic Health Records using Hyperledger offers a promising solution for securely managing and sharing patient health information. The use of Hyperledger technology provides a decentralized and permissioned framework that ensures data integrity, privacy, and security. By leveraging smart contracts and distributed ledger technology, healthcare providers can streamline the management of EHR while maintaining compliance with regulatory requirements. Furthermore, the immutability and audit trails provided by Hyperledger ensure transparency and accountability in the access and modification of patient records. This can lead to improved patient care, reduced administrative burden, and enhanced interoperability among healthcare systems. Overall, the adoption of Hyperledger for EHR implementation holds great potential in revolutionizing the healthcare industry by enabling secure and efficient management of patient health information. As technology continues to advance, further research and development in this area will be crucial in realizing the full benefits of Hyperledger in healthcare.

While the implementation of Electronic Health Records using Hyperledger fabric presents significant advantages, there are several areas for future work and research that can further enhance the system's capabilities. Scalability: The scalability of Hyperledger fabric for accommodating a large volume of EHR data while maintaining performance and efficiency can be improved. Interoperability: Different ways to enhance interoperability between different healthcare systems and organizations through the integration of Hyperledger fabric with Integration with IoT Devices: To securely capture and manage real-time patient data for EHR purposes the integration of IoT devices with Hyperledger fabric can be explored.

REFERENCES

1. Sharma, Y, and Balamurugan, B. Preserving the privacy of electronic health records using blockchain. *Proc. Comp. Sci.* (2020) 173:171–80. doi: 10.1016/j.procs.2020.06.021

2. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, URL https://bitcoin.org/bitcoin.pdf.

3. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., and Wang, F. Secure, and Trustable Electronic Medical Records Sharing Using Blockchain. Amia annual symposium proceedings, (2017). American Medical Informatics Association, 650.

4. Sabu, S, Ramalingam, H, Vishaka, M, Swapna, H, and Hegde, S. Implementation of a secure and privacy-aware E-health record and IoT data sharing using Blockchain. *Glob. Trans. Proc.* (2021) 2:429–33. doi: 10.1016/j.gltp.2021.08.033

5. Macdonald, M, Liu-Thorrold, L, and Julien, R. The Blockchain: a comparison of platforms and their uses beyond Bitcoin. *Work Pap*. (2017):1–18. doi: 10.13140/RG.2.2.23274.5216

6. Yu, H., Sun, H., Wu, D., and Kuo, T.T. Comparison of smart contract blockchains for healthcare applications. Amia annual symposium proceedings, (2019). American Medical Informatics Association, 1266.

7. J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y. Tu, "MedBloc: A Blockchain- Based Secure EHR System for Sharing and Accessing Medical Data," 2019 18th IEEE International Conference On Trust, Security

And Privacy In Comput ing And Communicat ions/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 594-601.

8. Polge, J, Robert, J, and Le Traon, Y. Permissioned blockchain frameworks in the industry: a comparison. *ICT Express*. (2021) 7:229–33. doi: 10.1016/j.icte.2020.09.002

9. Corradini, F., Marcelletti, A., Morichetta, A., Polini, A., Re, B., Scala, E., et al. Model-driven engineering for multi-party business processes on multiple blockchains. Blockchain: Research and Applications, (2021) 2:100018. doi: 10.1016/j.bcra.2021.100018

10. Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A. I., and Abid, M. Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. 2021 17th international conference on wireless and mobile computing, networking and communications (WiMob). (2021) Bologna, Italy: IEEE. 200–205. doi: 10.1109/WiMob52687.2021.9606362