iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68965

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Hyperledger Fabric-Based Blockchain Framework for Secure and Interoperable Healthcare Record Management

Aniket Deo[1], Utkarsh Roy[2], Sharukhali Syed[3], Akhilesh Singh[4]
[1]*Assistant Professor,* [2, 3, 4]*Student, Artificial Intelligence and Data Science, Thakur College of Engineering and Technology, India*

Abstract: ***Patient mobility and specialized healthcare services have increased the issues associated with managing a distributed electronic health record. Traditional electronic health records systems lack the robustness for confidentiality, integrity, or data interoperability even with the support of standards like Fast Healthcare Interoperability Resources and Health Level 7. Most data- sharing methods nowadays are push, pull, and view, which normally give poor security and standard audit trails that may offer potential dangers of data shattering or unauthorized access. This paper introduces a decentralized healthcare record solution utilizing Hyperledger Fabric, a permissioned blockchain framework, to address those issues. The proposed system would leverage the secure and non-modifiable storage of the blockchain while enhancing interoperability among healthcare providers as well as protecting patient anonymity through the use of smart contracts and controlled access. Hyperledger Fabric's architecture, built on the idea of trust among network members, does not require centralized surveillance but instead is supported through Certificate Authorities and Membership Service Providers. This decentralization decreases the cost of the resources and ensures integrity, giving patients more control of their medical information.***

***Keywords*— blockchain, data integrity, electronic health records, Hyperledger Fabric, interoperability, patient privacy**

I. INTRODUCTION

The healthcare sector is much more complex with regard to mobility of patients increasing, accompanied by specialized services; it increases the complexity associated with EHR management and sharing. EHRs are virtual repositories of histories of patients and contain all their diagnoses, allergies, treatments, and lab results; therefore, informed decisions are made [1]. However, the current EHR infrastructures are severely challenged to ensure data confidentiality, integrity, and seamless interoperability across diverse healthcare providers [2]. Traditional EHR systems are based on centralized databases and standardized data exchange protocols like Fast Healthcare Interoperability Resources (FHIR) and Health Level 7 (HL7). Though these standards allow clinical data transfer, they fail to address most of the critical issues concerning data security and interoperability [3]. The current data- sharing models suffer from vulnerabilities toward unauthorized access, weak audit trails, and are characterized by potential data fragmentation at the very end, jeopardizing patient privacy and inefficient medical information exchange [4]. There is a significant amount of potential in blockchain technology; it would provide a secure and decentralized framework for handling data [5]. The Hyperledger Fabric or HLF can be thought of as an enterprise- wide permissioned block chain and is developed based on improved trust, security, and interoperability between different participants across the healthcare network, and so it differs from the public blockchains. HLF achieves controlled access through Certificate Authorities (CAs) and Membership Service Providers (MSPs) [6]. It prevents unauthorized access and exposure of sensitive medical data. The most important reason for using Hyperledger Fabric in healthcare record management is the support of an immutable and transparent ledger of transactions that can preserve the integrity of data [7]. Modular and scalable architecture supports the development of smart contracts in the form of chaincode that can automate and enforce access controls and data-sharing policies [8]. The ability to provide fine-grained permissions and decentralized management of data will help make the patient information more secure and private while promoting interoperability between different healthcare providers [9]. The current proposal will present a distributed solution for healthcare records built based on Hyperledger Fabric. It exploits the potential offered by blockchain, taking care of privacy but, in the same breath, considering interoperability. Its capacity to let patients take over as owners of their medical information, allowing them control of access and viewability over this digital asset, sets this proposal apart from any EHR system with usual deficiencies. This approach reduces the risk of data leakage and unauthorized access, decreases operational costs, and gives patients more control over their medical information, which in turn promotes a more secure and efficient healthcare ecosystem [10].

©IJRASET: All Rights are Reserved

II. LITERATURE SURVEY

Blockchain technology's inclusion into Electronic Health Record (EHR) systems has received much attention because of the need to address the ever-demanding factors within healthcare, including data security, privacy, and compatibility. The current CEHRs using standards such as FHIR and HL7 has some flaws such as data silos, security breaches, and poor data sharing among a variety of stakeholders within the healthcare sectors [11].

Blockchain-Based EHR Solutions have been proposed to address these challenges through decentralized storage of data and use of cryptographic measures in order to fully protect the data of the patients [12]. Azaria et al. (2016) proposed a system of blockchain EHR with distributed data storage, which leads to the elimination of unauthorized access to records and non-alterability of data [13]. In the same way, Roehrs et al. (2018) highlighted how blockchain provides for the establishment of permanent ledger records that improve compliance and accountability in data exchange between various healthcare stakeholders [14].

Hyperledger Fabric is the most preferred blockchain platform in healthcare because it is permissioned, with controlled access through Certificate Authorities (CAs) and Membership Service Providers (MSPs). Wang et al. (2019) demonstrated the efficacy of Hyperledger Fabric to develop a secure and scalable EHR system through the implementation of fine-grained access control and interoperability through smart contracts or chain-code [15]. Chenthara et al. (2020) have demonstrated an integration framework involving Hyperledger Fabric with the pre-existing information systems of hospitals allowing smooth exchange of data with the consent of patients, while keeping their information private [16].

Data Privacy and Access Control are the core requirements for blockchain-based EHR systems. M.S Memon et al. proposed a mechanism that uses Hyperledger Fabric, where a patient's data is treated as an asset on the ledger and smart contracts have control over access permissions [17]. This mechanism allows patients to permit or deny access to their medical records, which helps in controlling personal information. Liu et al. extended the use of Attribute- Based Encryption (ABE) in Hyperledger Fabric to realize dynamic access policies where only authorized users can access certain data fields [18].

Interoperability Among Healthcare Providers is important for comprehensive patient care. Huang et al. (2021) created an interoperable EHR system using Hyperledger Fabric where every hospital functions as an organization within the Fabric network [19]. Patient data is maintained in the form of digital assets on the ledger with reference maintained in other databases for integrating with the existing systems. This architecture helps to achieve data consistency and integrity in the network [20].

Comparative Analyses indicate that Hyperledger Fabric comes with more privacy controls and scalability than public blockchains like Ethereum. Permissioned blockchains provide important security layers needed to process sensitive medical data; hence, Hyperledger Fabric is better suited for health-care applications.

III. METHODOLOGY

This section outlines the approach that is followed in designing a decentralized health care record system based on HLF. HLF is designed as a framework of six components which must be aligned with the requirements of EHR system, creating a secure blockchain network and provide access control for secure sharing of data for interoperability. Accordingly, in the context of the proposed system, each hospital is represented as an organization of the HLF network. record solution on Hyperledger Fabric (HLF). The methodology consists of mapping the components of HLF to the EHR system requirements, establishing a secure blockchain network, and implementing access controls for data privacy and interoperability. In the proposed system, every hospital is modelled as an organization within the HLF network. Since all this patient data will be creating a sort of digital assets that can be stored on the blockchain these separate references shall be hosted on another database to cater for real world scalability and EHR system inclusion. System Architecture The following represent the main components which have been shown in the system architecture:

1) Hyperledger Fabric SDK: It is used to interact with the blockchain. Fabric SDK include packages such as fabric- ca-client which deals with registration of participants and their enrollment; fabric-common is the contact point with the network; and fabric-network deals with ledgers and identities respectively.

2) Certificate Authorities (CAs) and Membership Service Providers (MSPs): These assist in identity management and authorization hence enable only specific people like admins, doctors and patients to access the network.

3) Smart Contracts (Chaincode): The business rules specifying the access control policies are encoded in form of custom smart contracts for the limitation of access with patient authority, and to safely enable data exchange. In figure 1 below is a diagram to show how the different component of the system interacts, different colors distinguish interactions stages.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

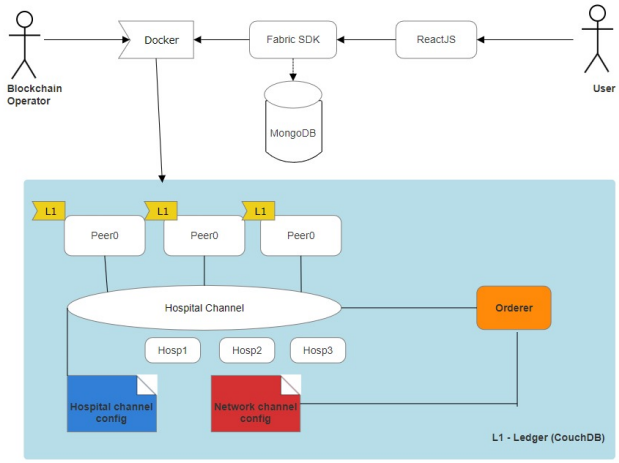


Fig. 1 System Architecture

The methodology involves aligning EHR system requirements with HLF components to ensure seamless data management:

4) Organizations as Hospitals: Each of them is schematically presented by an organization within the Fabric network, thus providing for the decentralized management of the hospitals' activities and the exchange of data between them.

5) Patient Data as Assets: Since patients' records pertain to their most personal and medical information (age, address, allergies, symptoms, treatment, follow-up), they are recorded as assets which belong to the ledger. This makes data integrity and access security guaranteed.

A. Fabric Network Configuration

Hyperledger fabric is the consensus platform which provides the secure and immutable ledgering within the system. The blockchain operator acquires and sets up the blockchain, setting fundamental decision and issuing keys to legitimate clients. While the above clients are active, each participating hospital manages operational Docker containers for the peer, orderer, and certificate authority (CA) services using Hyperledger Fabric images: fabric-peer, fabric-orderer, and fabric-ca. Containerized approaching is beneficial in such manner as it provides flexibility, modularity of networks and its components. Hospital organizations use one communication channel, known as hospital Channel. Designed to support two hospitals initially, integration of more hospitals to the existing channel is easily possible without affecting the compatibility and data coherency in the network.

B. Application Layer

Application layer is highly pluggable and modular for extensibility and uses a number of technologies to interact with Fabric network. Backend Services is developed using JavaScript with the Express.JS framework; providing a RESTful API to communicate between client and server. However, JavaScript, the preferred language of Hyperledger Fabric has other alternatives such as Java, Go, and TypeScript in backend development. Patient and doctor communication is well controlled by business logic that is installed in smart contracts commonly referred to as chaincode. The smart contracts are executed on the Fabric network and thus all the transactions are transparent and immutable.

C. Security Mechanisms

Security and privacy of data is always of extreme concern when it comes to applications in healthcare. Information security is fortified by a number of layers in the architecture. Membership Service Provider (MSP) takes care of identities within the network and only allowed entities can engage with the blockchain. What is more, each hospital has its own Certificate Authority (CA) that provides digital certificates proving the subject identity. Our Private Data Collections ensure that a patient's information is neither disclosed to a third party nor shared with the patient themselves without their doctor's consent. These collections make sure that patient's data is only used and retrieved by the right hospitals and doctors. This ensures that each hospital permission correlates with a private data collection which in turn gives fine-grained access control. Patient Record data re-encryption is done where patient records are encrypted using symmetric keys for efficiency is done here.

These symmetric keys are again protected by asymmetric encryption technologies, the re-encryption keys then allow only the authorized doctors to decrypt/access their data while the actual data remains secure. To enhance data privacy and security, the following measures are implemented:

- Smart Contracts: Strategies about the operational and logical execution of transactions in terms of creating, modifying, and capturing information on patient records. The contracts implemented also improve the usage of role-based access controls to ensure that certain actions can only be done by users with permission.
- Approval Policies: It specifies that several organizations have to accept approval for change to occur this will ensure integrity in the data.
- Encryption: It uses the combination of asymmetric keys to ensure that only authorized agents are able to access the information.

Access Control Mechanisms:

- Patients can grant or revoke access to their data for specific doctors through smart contracts.
- Doctors have permission to view limited fields (medical details, age, allergies), while patients can view all fields but only edit personal information.
- Separate Database for EHR References: In order to link real data from EHR systems, references to the data are stored in the external database that can be easily linked without the integration in the blockchain environment impacting its performance.

D. System Workflow

The architecture allows one to facilitate critical work processes for handling health records. During the first time consultation, an administrator through the Admin Contract brings a new patient into the ledger. The patient is issued with a temporary password through which he or she can access records through any of the hospitals within the network safely. Administrators uniquely identify and enroll doctors through the Doctor Contract. Doctor credentials are saved in MongoDB and their identities are connected to the blockchain network by MSPs. One can give or withdraw permission to the doctors who entered the patient's information in the EMR.

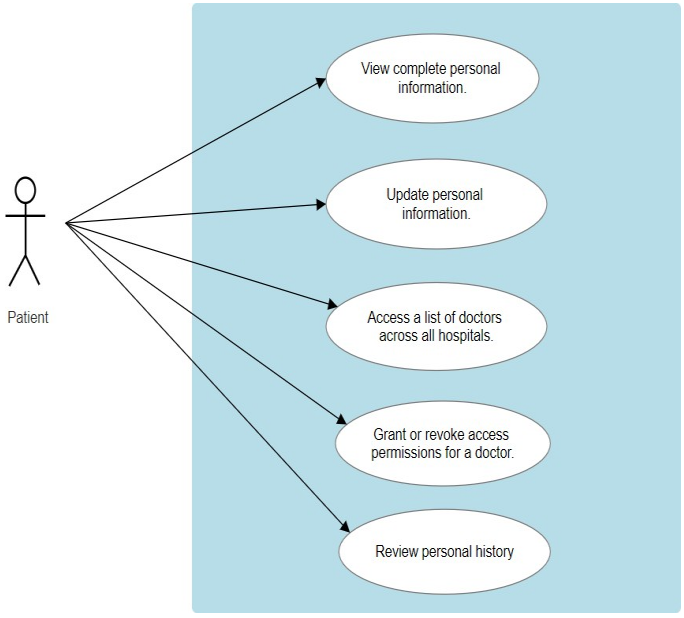


Fig. 2 UML use case diagram for a patient

The figure 2 illustrates the use case diagram for a patient in the health care system and the different things that he can do such as, view and edit account details, view/doctors list across different hospitals, permit/terminate doctor's account permission, and view personal details and treatment history.

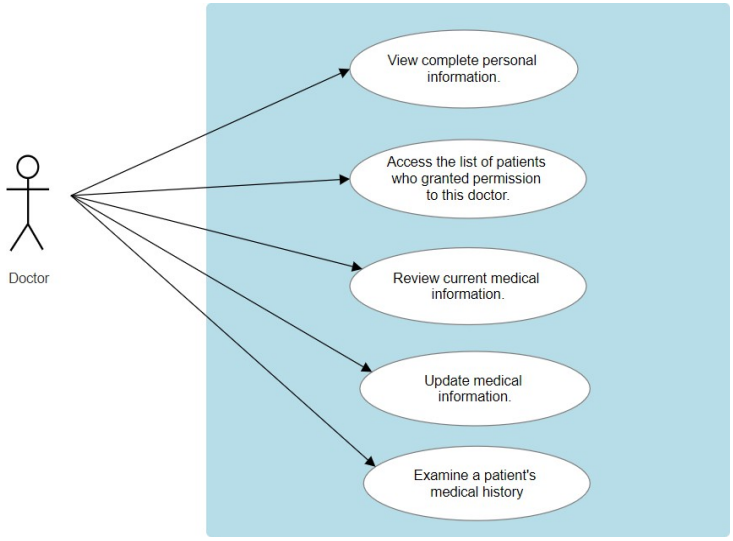


Fig. 3 UML use case diagram for a doctor

The figure 3 illustrates a use case diagram for a doctor, showing the various actions the doctor can perform. These include viewing complete personal information, accessing the list of patients who granted permission, reviewing current medical information, updating medical information, and examining a patient's medical history. These permissions are managed through private data collections, ensuring that only authorized personnel can view or modify sensitive information. The figure 4 depicts a use case diagram for an admin, showing the various actions the admin can perform. These include viewing complete personal information, accessing the list of patients who granted permission, reviewing current medical information, updating medical information, and examining a patient's medical history.

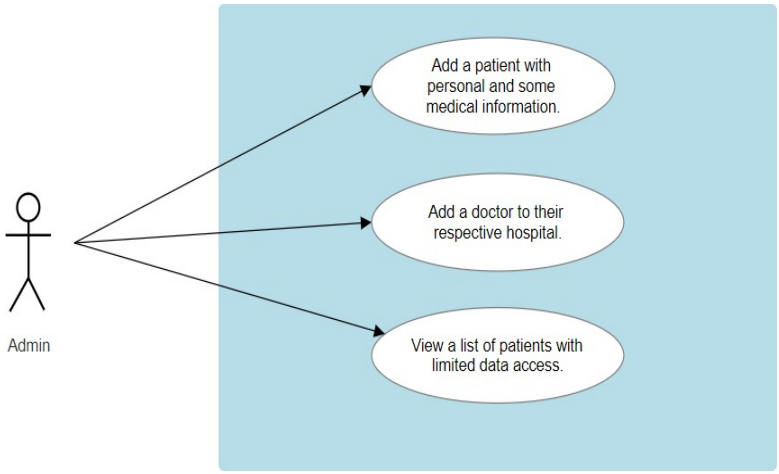


Fig. 4 UML use case diagram for an admin

E. Integration of Hyperledger Fabric

The realized architecture effectively leverages core Hyperledger Fabric components to satisfy a secure and interoperable healthcare record solution. One chaincode package has multiple smart contracts encapsulated within the interaction manager between different roles such as patients, doctors, and administrators. This approach allows us to maintain precise control over all operations and processes.

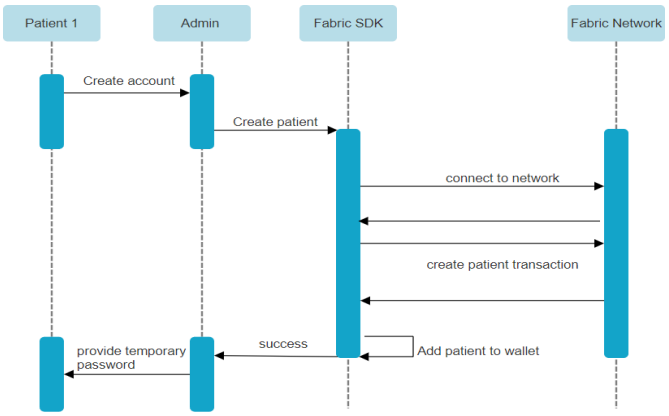


Fig. 5Creation process of a Patient

Figure 5 shows a sequence diagram demonstrating the process of creating a patient account within a Hyperledger Fabric based network. Patient 1 accesses Admin and requests it to create an account. The Fabric SDK will connect to the Fabric Network upon an Admin sending a request. Once established the network then goes ahead to make the patient's record. When the Fabric SDK confirms the patient created, it adds the patient to the network's wallet, and sends a success message back to the Admin. The patient is then given a temporary password by the Admin to create the account.

Similarly, the sequence diagram in figure 6 shows how a doctor's account is created in the system. The Doctor requests the Admin to create an account. The Admin adds the doctor's credentials in MongoDB, and upon success, the Fabric SDK is called to connect to the Fabric Network. Once connected, the doctor appears as a client to the network. Then the Fabric SDK adds the doctor to the wallet, and the network replies saying that it was successful in adding the doctor as a client to the network.

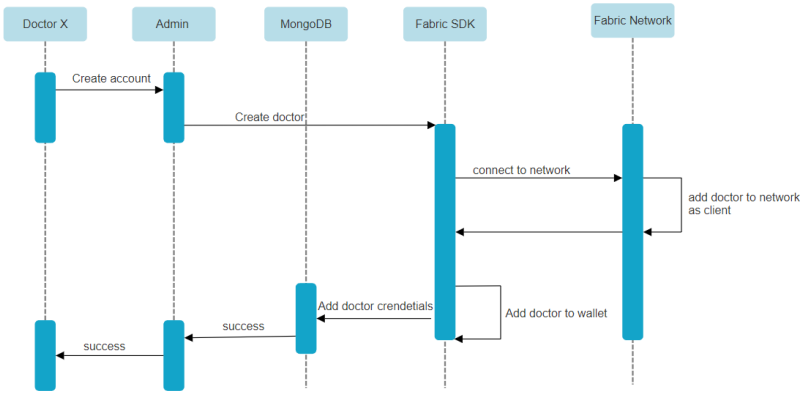


Fig. 6Creation process of a Doctor

F. Data Management

Healthcare records need to be available and in an intelligible format. CouchDB is chosen as our primary world state database, due to its flexibility and advanced (but also slow) querying capabilities through indexing. CouchDB stores all patient data, without a separate Electronic Health Record (EHR) repository. A completely audited trail of all transactions from the genesis block, creating an immutable log. The world state is maintained in CouchDB, and reflects the lastest values of each asset, as well as allowing for efficient and quick read and write operations without traversing through the whole transaction log. We store doctor credentials — usernames and hashed passwords in MongoDB. The Fabric SDK manages additional user attributes to ensure secure and efficient access control.

G. Private Data Collections

Efficient healthcare data management is crucial for preserving the integrity and availability of the records. The primary world state database in the system is CouchDB because of its flexibility and advanced querying capabilities via indexing.

However, in this case, all patient data is stored inside CouchDB, the need for additional private data collections for the storage of sensitive patient information only available to the authorized parties is all taken care of. Each private data collection consists of:

- Actual Private Data: Available only to designated hospitals or doctors.
- Hash of Private Data: Ensuring data integrity without revealing the actual content to unauthorized peers are stored in the ledger.

Collection Management: We support multiple private data collections so that they can accommodate different access levels. In particular, in an example that has three hospitals, there are seven private data collections corresponding to all possible combinations of hospital access.

Data Movement: That data transfer happens automatically when a patient grants or revokes access, in that data is passed between private collections maintaining a single source of truth, with no data duplication.

H. Data Re-encryption

Data re-encryption helps to secure data by ensuring that data stays secure when data transitions are made.

Encryption Strategy:

- Symmetric Encryption: A symmetric key is used for encryption to make the process fast.
- Asymmetric Encryption: And the patient's public key is used to further secure the symmetric key.
- Re-encryption Process:
- Initial Encryption: The symmetric key is used to encrypt data.
- Key Protection: The patient's public key encrypts the symmetric key that is stored into the ledger.
- Granting Access: A re-encryption key is generated when a patient allows a doctor access, so that the doctor can decrypt the symmetric key without exposing it.

Security Benefits: Such dual layer encryption means that even if the re-encryption key is compromised, unauthorized parties cannot read the data without the doctor's private key.

IV. RESULTS AND DISCUSSION

The Hyperledger Fabric-deployed decentralized healthcare record solution does show promise in privacy, integrity of data, and interoperability. Patient information is stored securely as assets in a distributed ledger, which controls access and cannot be modified. Modelling hospitals as organizations in the fabric network allowed decentralized control, data sharing, and lack of central authority control. This architecture granted control of fine- grained permissions at the patient level; access was permitted or forbidden appropriately. Using Certificate Authorities and Membership Service Providers made it even safer since access could only come through entities authorized to access the network. Private data collections prevent exposure of data contents but do allow selective data sharing among hospitals and practitioners given some access rules set.

On interoperability, Hyperledger Fabric showed that it was compatible with the existing systems for EHR by storing the references of the data in an external database to integrate without affecting the functionality of blockchain. Smart contracts (chaincode) ensured the process was smooth for the information to be shared and distributed as well as accessed within access control, hence protecting patient information while enabling medical information to be viewed. Further, policies of endorsement, combined with asymmetric encryption, ensured that only the sensitive information used was secure from risks due to unauthorized access and ensures data accuracy. The table 1 depicts a comparative analysis of traditional EHR systems and the proposed Hyperledger Fabric-based decentralized solution.

Category	Existing System (Traditional EHRs)	Problems Addressed	Hyperledger Fabric- Based EHR Solution
Data Management	Centralized databases for Electronic Health Records (EHRs).	Risk of unauthorized access, data breaches, and single- point failure.	Decentralized blockchain-based storage with secure data encryption.
Interoperability	Uses standards like HL7 & FHIR but lacks seamless integration across hospitals.	Fragmented data, inconsistent records, and difficulty in data sharing.	Blockchain ensures a unified and interoperable data-sharing framework.

Security & Privacy	Basic encryption and access control mechanisms.	Weak authentication, vulnerable to breaches, lack of fine-grained access control.	Uses smart contracts and encryption for role-based access control.
Audit Trails	Limited or inconsistent audit mechanisms.	No transparent tracking of access and modifications to records.	Immutable blockchain ledger ensures complete audit trails.
Access Control	Hospitals control patient records.	Patients have limited control over who accesses their data.	Patients have full access control using smart contracts.
Data Sharing	Uses push, pull, and view models.	Lack of trust, security loopholes, and inefficient data sharing.	Blockchain-based secure and permissioned data sharing.
Scalability	Centralized servers limit scalability.	Performance bottlenecks with increasing data.	Hyperledger Fabric enables distributed processing and efficient scaling.

Table 1 - Comparison of Traditional EHR vs. Hyperledger Fabric-Based Decentralized EHR Systems

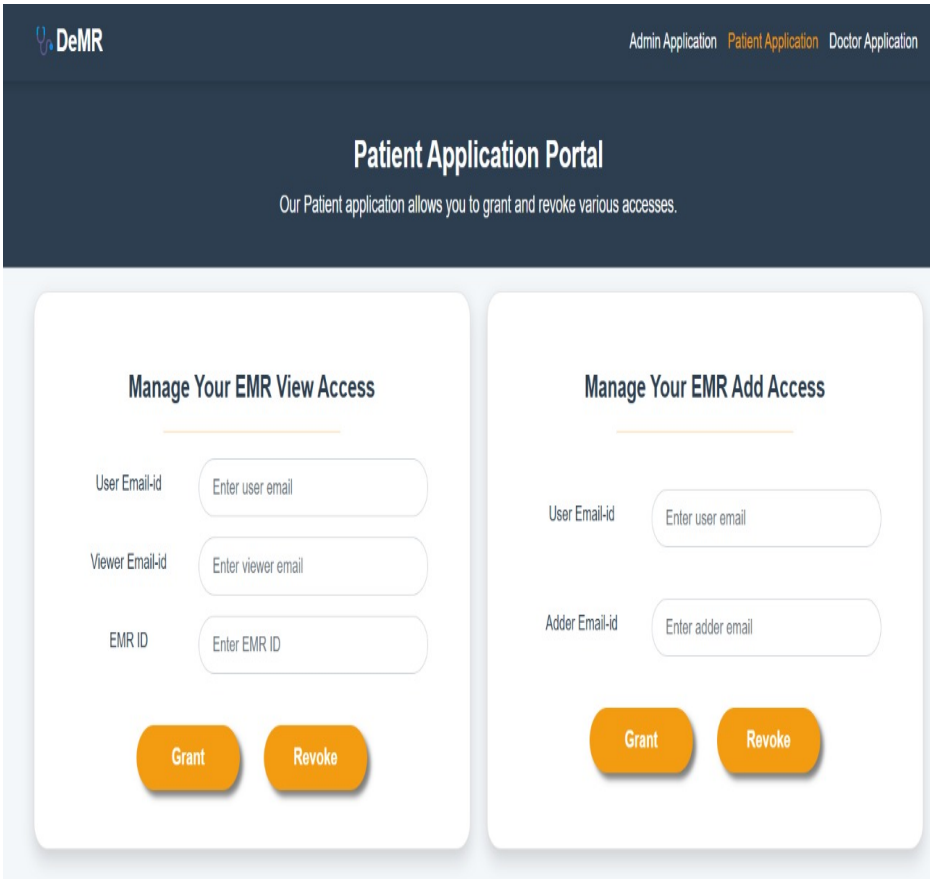


Fig. 7(a) Patient Portal – Manage EMR Add and View Access

This interface as displayed by figure 7(a) enables patients to grant or revoke a doctor's permission to either view or add entries to the Electronic Medical Record (EMR). By specifying the user's email address and EMR ID, patients maintain full authority over who can access or modify their medical data, in line with patient-centric frameworks proposed in [10], [13].

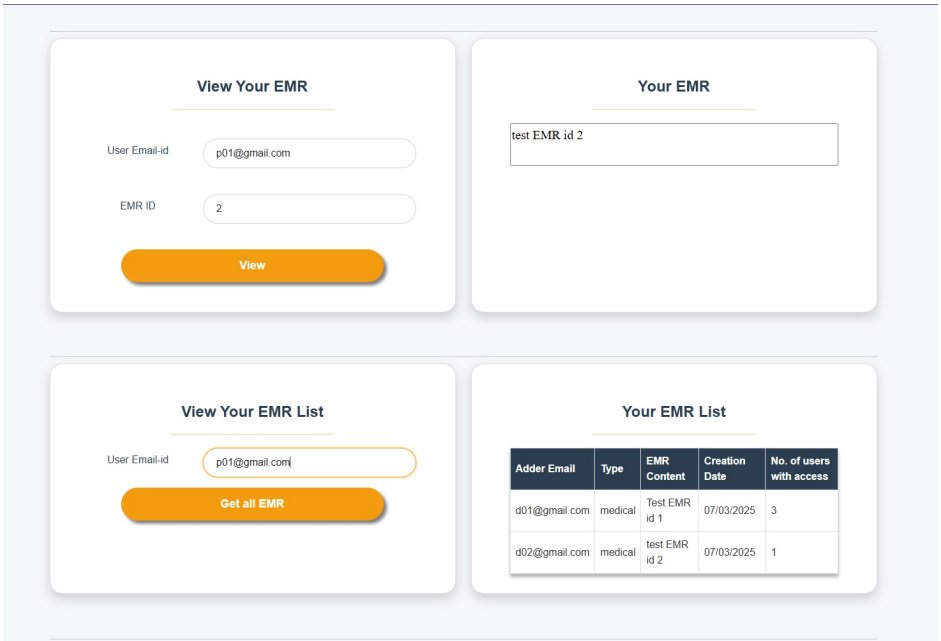


Fig. 7(b) Patient Portal – EMR Details and Listing

Patients can retrieve a specific EMR by entering its ID or display all EMRs associated with their account as indicated by figure 7(b). The portal lists EMR content, creation date, and the number of users who have access. Such transparency ensures that patients remain informed about the lifecycle and sharing status of their healthcare records, consistent with secure and immutable record management approaches outlined in [7], [9].

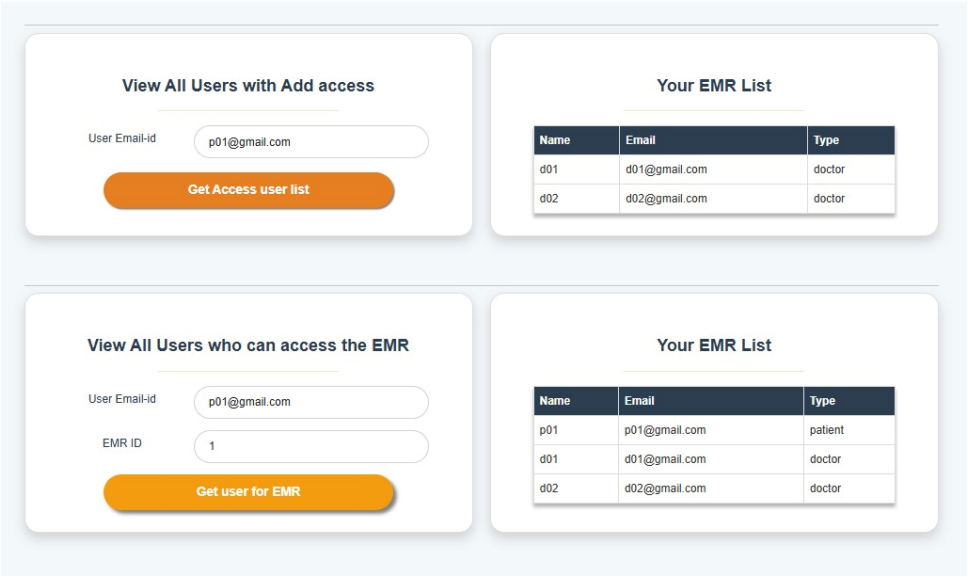


Fig. 7(c) Patient Portal – View All Users with Add Access and EMR Access

This section displays the list of users who possess “Add Access” privileges to a patient’s EMR as can be seen in figure 7(c). By providing real-time visibility of authorized contributors, patients can swiftly revoke or adjust permissions to safeguard data integrity. This granular control resonates with fine-grained access mechanisms recommended in [8], [14].Here, the system shows all users (e.g., doctors, other healthcare staff) who have been granted viewing or editing permissions for a given EMR. Patients can filter by email address or EMR ID to refine the list. Such selective sharing of medical information underscores the decentralized and privacy-preserving principles advocated by Hyperledger Fabric [6], [18].

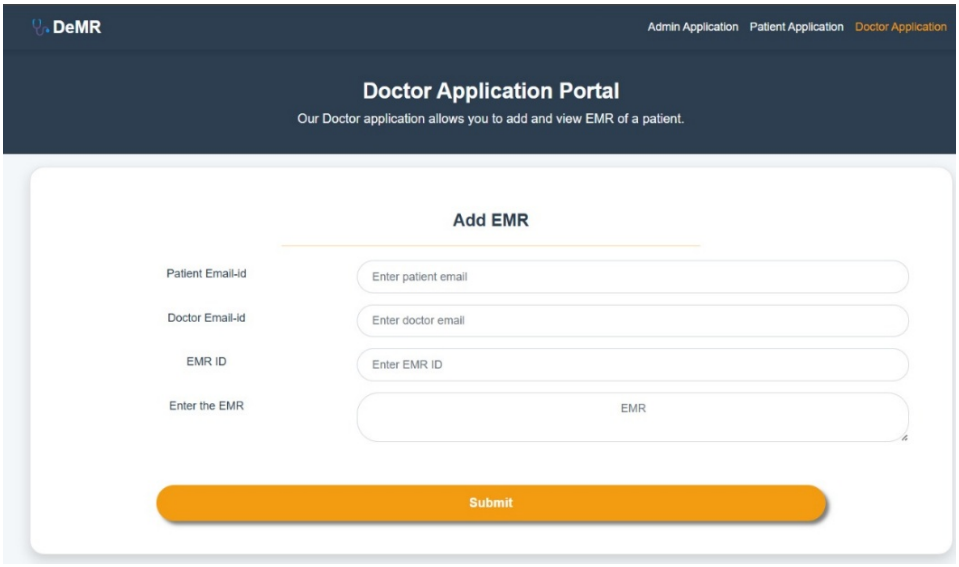


Fig. 8(a) Doctor Portal – Add EMR

This interface as displayed in figure 8(a) enables an authorized doctor to add a new EMR entry for a specific patient by providing the patient's email, doctor's email, EMR ID, and the record details. Once submitted, the data is recorded on the blockchain, ensuring immutable storage and traceability as described in [8], [10].

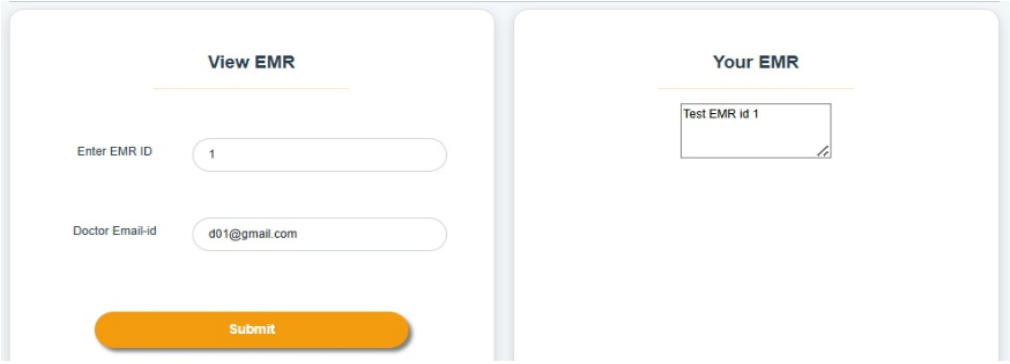


Fig. 8(b) Doctor Portal – View EMR

As we can see in the figure 8(b), the doctor can retrieve a patient's EMR by entering the relevant EMR ID and verifying their own email address. Access is granted only if the patient has authorized the doctor, illustrating the fine-grained, patient-centric permission model enforced by the underlying Hyperledger Fabric network [6], [13].

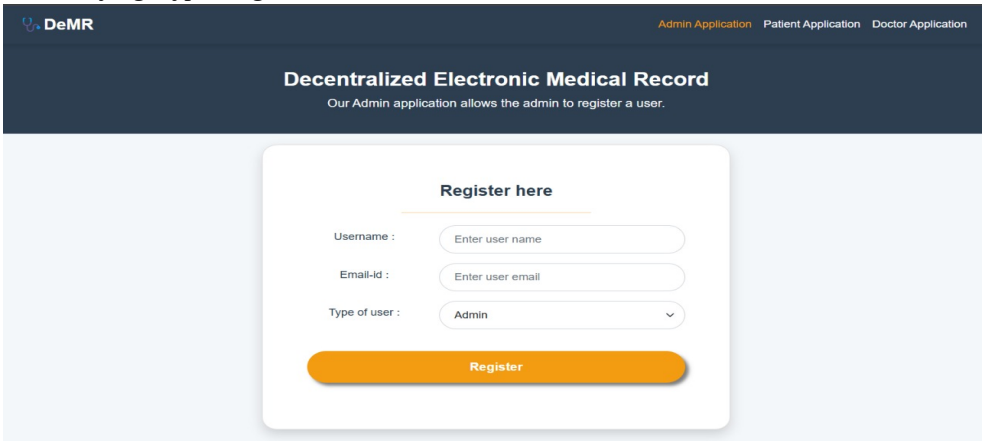


Fig. 9 Admin Portal – User Registration

This interface as described in the figure 9 allows the administrator to register a new user by specifying a username, email address, and user type (e.g., Admin, Doctor, Patient). Upon registration, a unique identity is issued and managed through the Membership Service Provider (MSP), reinforcing secure and permissioned access within the Hyperledger Fabric network [6], [13].

This web application also includes a dedicated notification functionality implemented using nodemailer. The important updates are sent via email to the concerned authorities. This helps them stay up-to-date with any change in record that might take place. Patients are notified promptly whenever a new EMR is added and the doctors are informed whenever they are granted access to add or view a specific EMR. This shall be illustrated further with the help of snapshots.

The DeMR (Decentralized Electronic Medical Records) platform supports secure and decentralized storage of medical records along with role-based access control for better privacy. A registration confirmation email as displayed in the figure 10 indicates the capability of the platform to provide easy sharing of data among authorized individuals. Registration assigns a unique identification number and role-based access, protecting data integrity and security.

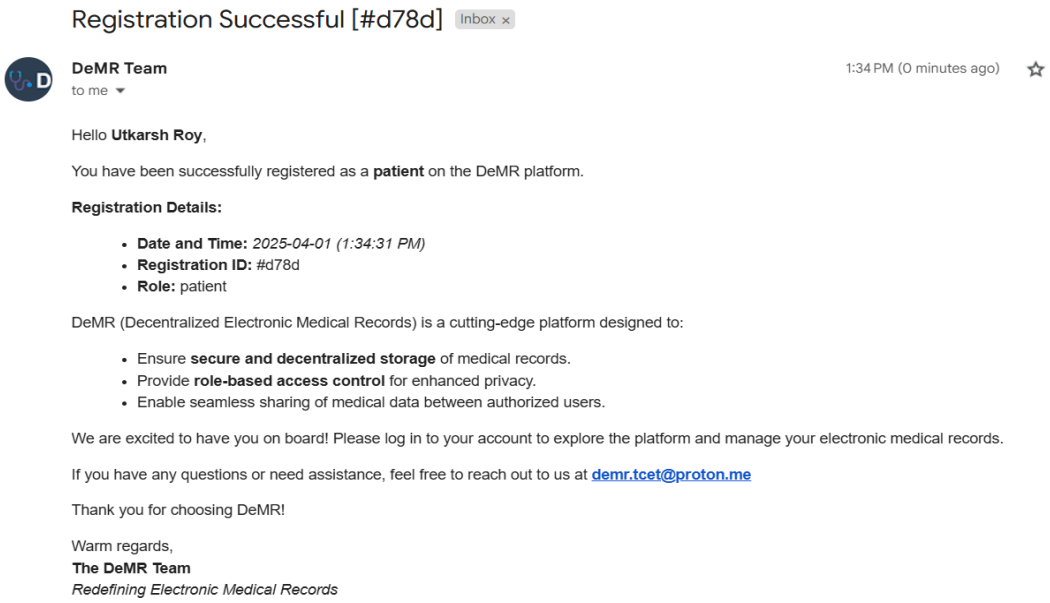


Fig. 10Registration email notification to the concerned authority

The email as displayed in figure 11 ensures that access has been provided to add Electronic Medical Records (EMRs) for a particular patient. It gives the access date and time, as well as the patient ID, so that authorized users can securely update medical records (EMRs). This controlled access mechanism is in line with Hyperledger Fabric's role-based access control.

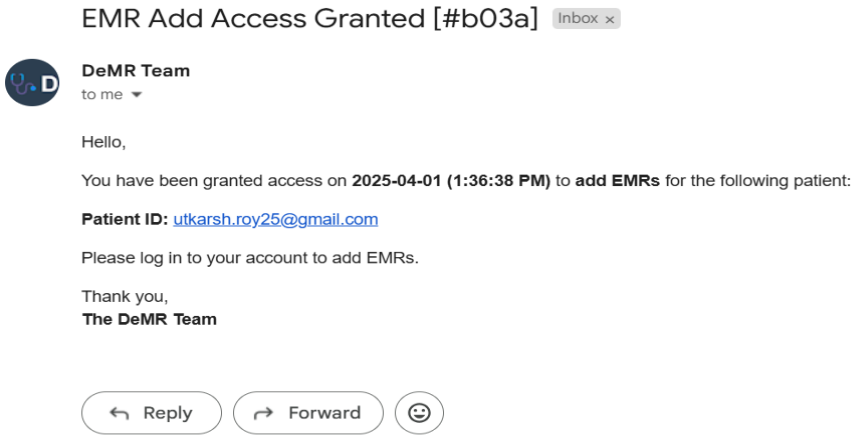


Fig. 11EMR Add access granted (email to Doctor side)

The figure 12 shows an automated email notification to the doctor, that they have been assignedview access to an Electronic Medical Record (EMR). It includes the EMR ID, specifying the exact record to which the user has access. The e-mail requests the recipient to log in to the account for more information making it secure by not directly providing sensitive medical information. This kind of notification system improves transparency and accountability in accessing medical records while maintaining conformity to data protection laws.

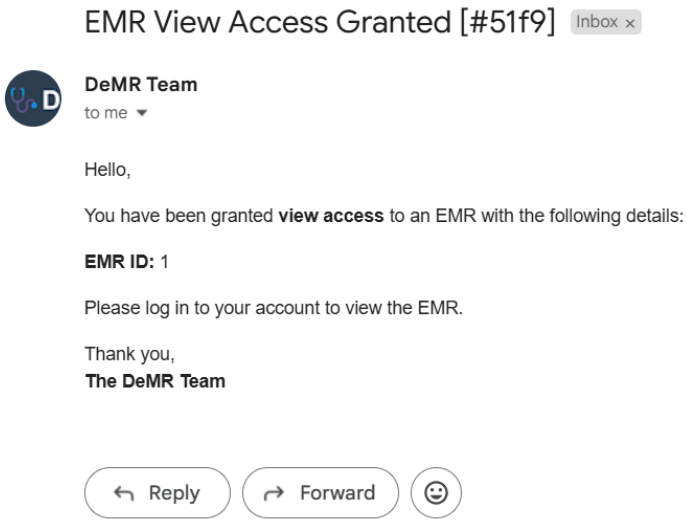


Fig. 12 EMR view access granted (email to Doctor side)

The figure 13 depicts an email notification informing the patient, who is the recipient in this case, about the addition of a new Electronic Medical Record (EMR) to their account. The email includesdetails such as the EMR ID, type (medical), and timestamp of the update. This automated notification system ensures timely communication and accessibility of medical records for users.

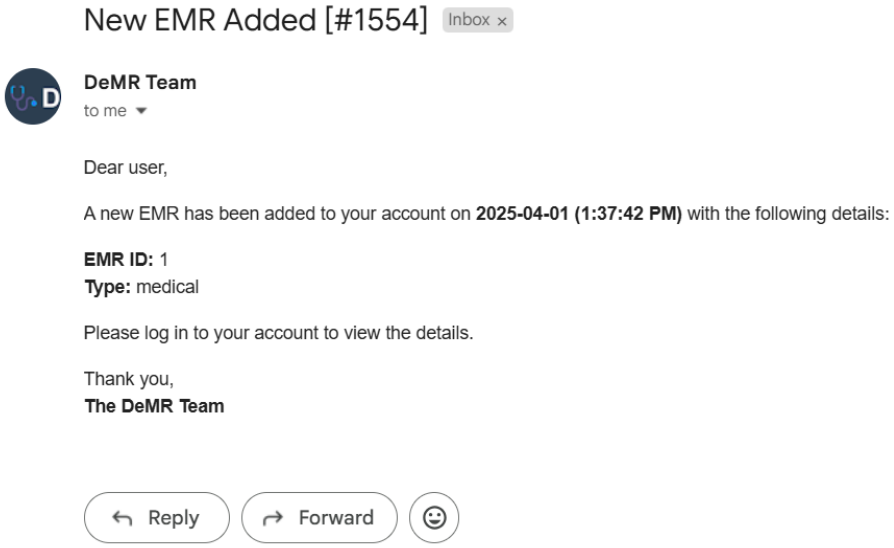


Fig. 13New EMR added (email to Patient side)

The figure 14 showcases anemail alert notifying the patientthat their EMR has been accessed. The email contains details such as the EMR ID, the accessing doctor's email ID, and the exact date and time of access. Such notifications promote transparency and security by keeping users informed about activities related to their medical data and prevent any unauthorized access without the patient's consent.

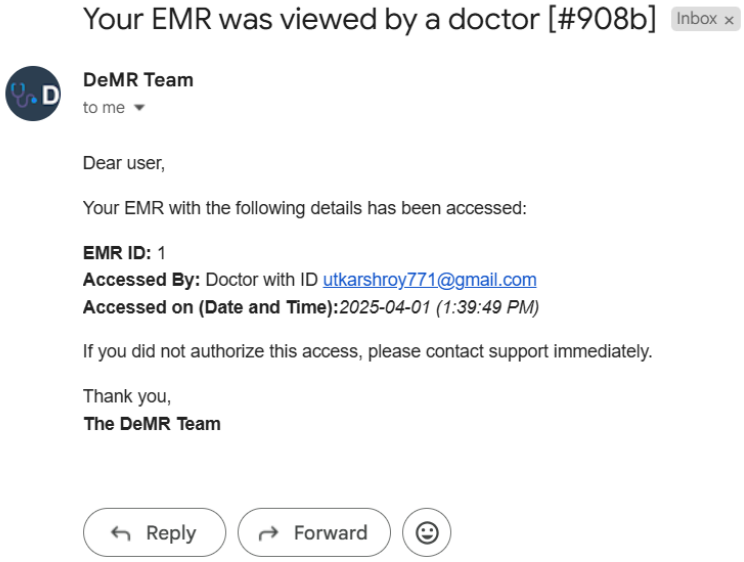


Fig. 14 EMR viewed by doctor (email to Patient side)

V. CONCLUSION

This work shows the robustness of Hyperledger Fabric (HLF) for managing Electronic Health Records (EHR) on blockchain in a decentralized healthcare ecosystem. With HLF features including customizable policies, smart contracts (chaincode), and secure identity management through Certificate Authorities (CAs) and Membership Service Providers (MSPs), it is assuredly and meticulously secured the patient records. HLF provides hospitals' facilities with transparency and seamless interoperability among various hospital organizations without the need for any central oversight. By creating this interoperability, healthcare providers can easily access comprehensive patient histories improving decision making and improving patient care outcomes. In addition, not having to keep physical medical records saves patients from having to physically carry around records. Based on this, we can argue that Hyperledger Fabric comes with an efficient and secure solution to managing medical records on the downside of traditional EHR systems in terms of security, privacy and interoperation. This research shows the potential of HLF to replace current practices for healthcare record management with an improved, more efficient, more secure system, enabling a more patient centric healthcare environment.

REFERENCES

[1] Zhigang Xu, Rohit Shukla, Pratik Sushil Zambani, Arun Swaminathan, Md Majid Jahangir, Khadija Chowdhry, Rahul Lachhani, Nitesh Idnani, Michael Schumacher, Karl Aberer, Scott D. Stoller, Samuel Ryu, Alevtina Dubovitskaya, Furqan Baig, and Fusheng Wang, "ACTION-EHR: Patient- Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care," Journal of Medical Internet Research, vol. 22, no. 8, Aug. 2020, p. e13598. doi: 10.2196/13598.

[2] Roman Beck, "Beyond Bitcoin: The Rise of Blockchain World," Computer, vol. 51, no. 2, pp. 54–58, Feb. 2018. doi: 10.1109/MC.2018.1451660.

[3] Andrew Lippman, John D. Halamka, and Ariel Ekblaw, "The Potential for Blockchain to Transform Electronic Health Records," Harvard Business Review, 2017. [Online]. Available: https://hbr.org/2017/03/the-potential-for- blockchain-to- transform-electronichealth-records. [Accessed: Sept. 27, 2024].

[4] T. Kumar, A. Braeken, M. Liyanage, and M. Ylianttila, "Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment," in 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–7. doi: 10.1109/ICC.2017.7996966.

[5] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in 2018 IEEE 20th International Conference on eHealth Networking, Applications and Services (Healthcom), 2018, pp. 1–7. doi: 10.1109/HealthCom.2018.8531136.

[6] "Membership Service Provider (MSP)," Hyperledger Fabric Documentation. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release2.2/membership/membership.html. [Accessed: Sept. 27, 2024].

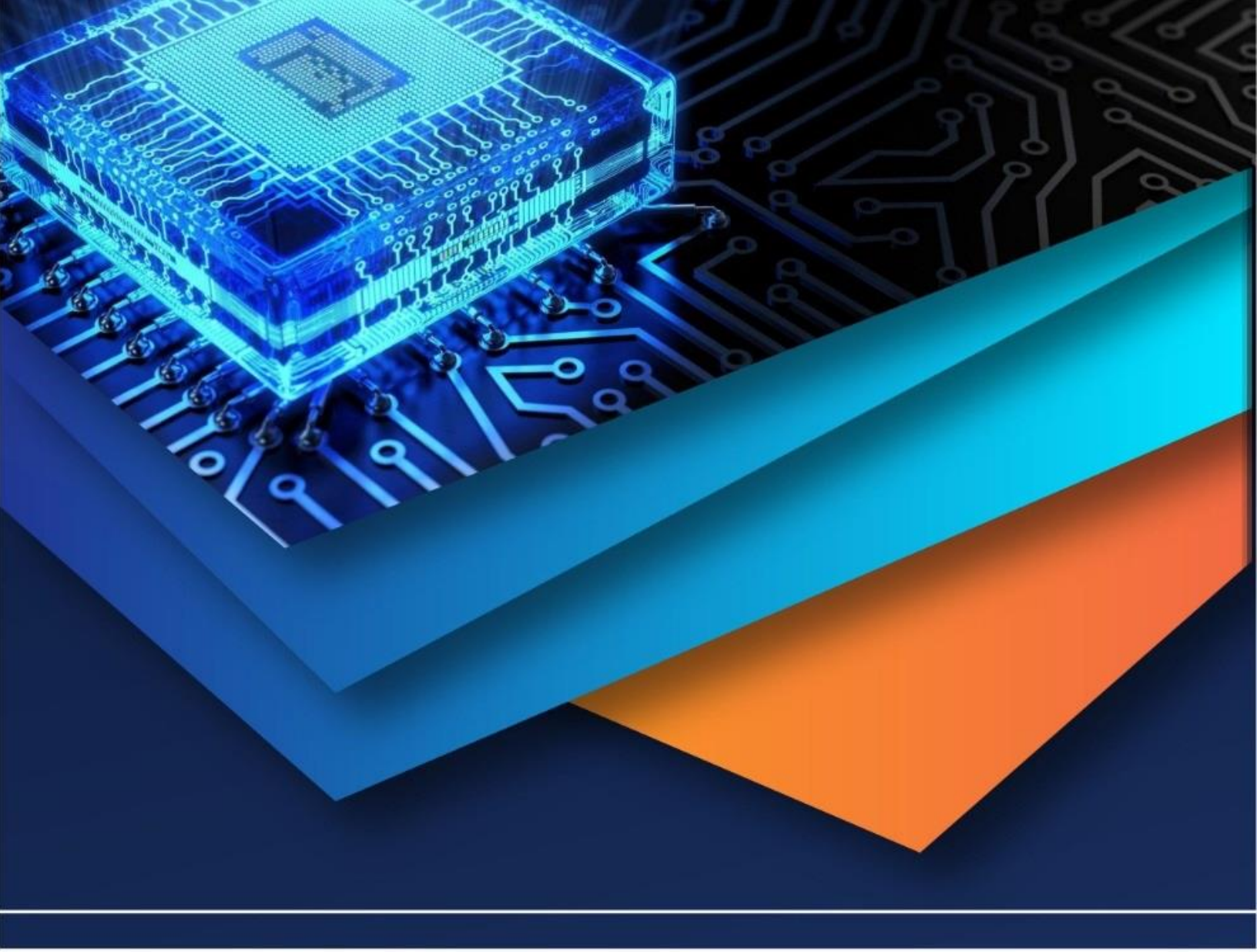
[7] Neeraj Kumar, Muhammad Khurram Khan, Shuyun Shi, Debiao He, and Kim-Kwang Raymond Choof, "Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey," Computers & Security, 2020. doi: 10.1016/j.cose.2020.101966

[8] Sudeep Tanwar, Karan Parekh, and Richard Evans, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," Journal of Information Security and Applications, vol. 50, Feb. 2020, p. 102407. doi: 10.1016/j.jisa.2019.102407.

[9] Dara Tith, Joong-Sun Lee, Hiroyuki Suzuki, W. M. A. B. Wijesundara, Naoko Taira, Takashi Obi, and Nagaaki Ohyama, "Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability," Healthcare Informatics Research, vol. 26, no. 1, 2020, p. 3. doi: 10.4258/hir.2020

[10] Azaria, Asaph &Ekblaw, Ariel & Vieira, Thiago & Lippman, Andrew. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 25-30. doi: 10.1109/OBD.2016.11.
[11] Alex Roehrs, Cristiano André da Costa, Rodrigo da Rosa Righi, Valter Ferreira da Silva, José Roberto Goldim, Douglas C. Schmidt, Analyzing the performance of a blockchain-based personal health record implementation, Journal of Biomedical Informatics, Volume 92, 2019,103140, ISSN 1532-0464, doi: 10.1016/j.jbi.2019.103140.
[12] Wang, Shuo. (2019). Performance Evaluation of Hyperledger Fabric with Malicious Behavior. doi: 10.1007/978-3-030- 23404-1_15.
[13] Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One. 2020 Dec 9;15(12):e0243043. doi: 10.1371/journal.pone.0243043. PMID: 33296379; PMCID: PMC7725426.
[14] Uddin, Mueen & Memon, M. & Memon, Irfana &Halepoto, Imtiaz & Memon, Jamshed & Abdelhaq, Maha &Alsaqour, Raed. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. Computers, Materials & Continua. 68. 2377-2397. doi: 10.32604/cmc.2021.015354.
[15] Liu, Weihua & Liu, Xinyu & Shi, Xiaoran& Hou, Jiahe & Shi, Victor & Dong, Jingxin. (2022). Collaborative adoption of blockchain technology: A supply chain contract perspective. Frontiers of Engineering Management. doi: 10. 10.1007/s42524- 022-0239-8.
[16] Huang, Guangjian&Foysal, Abdullah Al. (2021). Blockchain in Healthcare. Technology and Investment. 12. 168-181. doi: 10.4236/ti.2021.123010.
[17] https://www.investopedia.com/terms/h/hyperledger-fabric.asp
[18] https://www.lfdecentralizedtrust.org/blog/2020/01/29/fivehealthcare-projects-powered-by-hyperledger-you-may-not-know-about
[19] https://medium.com/@spydra/unlocking-the-future-of-healthcare-how-hyperledger-fabric-ensures-data-privacy-and-empowers-516b3a55fbf6
[20] M. Liyanage, and M. Ylianttila, “Identity Privacy Preserving Biometric Based Authentication Scheme for Naked Healthcare Environment,” in 2017 IEEE International Conference on Communications (ICC), 2017, pp. 1–7. doi: 10.1109/ICC.2017.7996966.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)