*Grenze International Journal of Engineering and Technology, January Issue*

# A Review of Hyperledger Fabric in Enhancing Electronic Health Records System

Mrs. Rohini Pise[1], Dr. Sonali Patil[2], Mr. Dhiren Ojha[3], Mr. Gaurav Kasliwal[4] and Mr. Atharva Nanavate[5]
[1-5] Department of Information Technology, Pimpri Chinchwad College of Engineering, Pune, India
Email: {rohini.pise, sonali.patil}@pccoepune.org, {ojhadhiren, gauravkasliwal70, atharvananavate}@gmail.com

***Abstract*—The digitization of healthcare has led to extensive use of Electronic Health Records (EHRs) for efficient patient data management. Hyperledger Fabric, a permissioned blockchain framework, holds significant promise in enhancing the security, privacy, and interoperability of EHR systems. This literature survey paper provides a comprehensive review of existing research on Hyperledger Fabric-based EHR management systems. The review focuses on crucial aspects including data privacy, security, access control, interoperability, and scalability. This paper provides insights into the latest developments in Hyperledger Fabric-based EHR management by putting together findings from multiple studies. It points out the challenges and limitations that current implementations face and suggests areas for future research aimed at improving the effectiveness and adoption of Hyperledger Fabric in EHR management [1]. By highlighting the potential benefits and challenges associated with leveraging Hyperledger Fabric for EHR management, stakeholders in healthcare and blockchain technology gain valuable perspectives. The paper concludes with recommendations for further research and development efforts, aiming to address existing gaps and propel advancements in this critical domain. Overall, this literature survey serves as a great resource for learners, policymakers, and researchers, interested in understanding the role of Hyperledger Fabric in revolutionizing EHR management, thereby contributing to the ongoing evolution of healthcare systems towards greater efficiency, security, and interoperability.**

***Index Terms*—Blockchain Technology, Hyperledger Fabric, Healthcare Management, Electronic Health Records (EHRs), Data Privacy, Security, Access Control, Interoperability, Scalability, Literature Survey, Research Directions.**

## I. INTRODUCTION

The digitization of healthcare has transformed the landscape of patient data management, with Electronic Health Records (EHR) emerging as a pivotal tool in modern health care systems. The efficient and secure management of EHRs is essential for ensuring high-quality patient care, facilitating medical research, and streamlining healthcare operations. However, traditional EHR systems are often plagued by challenges related to data security, privacy breaches, lack of interoperability, and centralized control. Blockchain technology has attracted a lot of interest recently as a possible solution for these issues [1]. Among various blockchain frameworks, Hyperledger Fabric stands out as a promising option for EHR management due to its permissioned architecture, robust security features, and support for complex data sharing and access control mechanisms. Hyperledger Fabric offers a decentralized and tamper-resistant platform that can potentially increase the security, interoperability, and privacy of HER systems while ensuring compliance with regulatory requirements. This

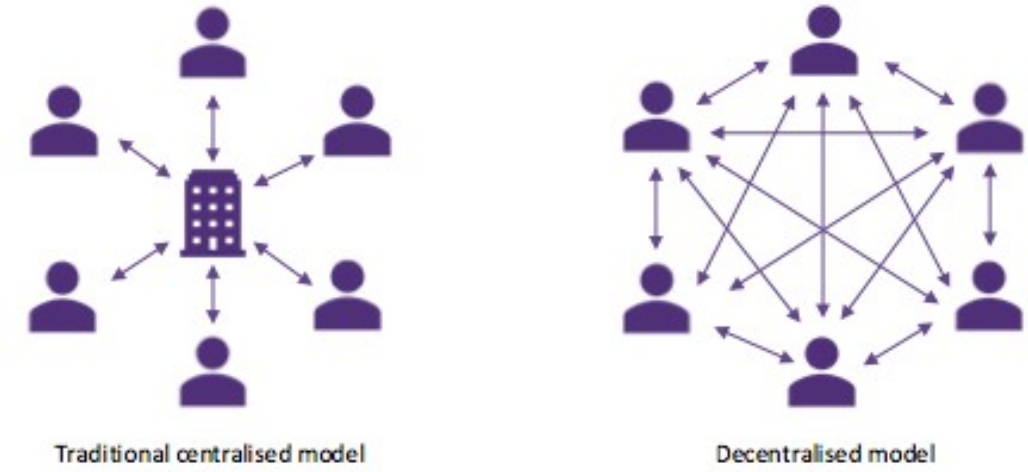
*Grenze ID: 01.GIJET.11.1.42*

paper presents a comprehensive literature survey on Hyperledger Fabric-based EHR management systems, aiming to explore the most recent developments, and identify the challenges and limitations, and propose future research directions [2]. The survey encompasses a wide range of studies and research articles focusing on key aspects such as data privacy, access control policies, security mechanisms, interoperability standards, and scalability issues in Hyperledger Fabric-based EHR implementations. By synthesizing findings from existing research, this paper aims to provide valuable insights for researchers, practitioners, and policymakers interested in leveraging Hyperledger Fabric for EHR management. Through a critical analysis of the literature, this survey seeks to shed light on the potential benefits and challenges associated with adopting Hyperledger Fabric in healthcare settings, thereby informing future research efforts and guiding the development of more effective and secure EHR management solutions.

## II. BACKGROUND

### *A. Existing Problems*

Tracking the sequential development of a patient's health status is difficult with the current EHR management systems. These outdated systems have left hospitals, labs, and pharmacies with a complex that is only partially digitalized, with paper records still being used on a variety of levels. The disjointed and unreliable electronic systems cause administration problems pertaining to interoperability, scalability, security, and integrity [3]. Cybercrime-related attacks that target the healthcare sector frequently involve the theft and modification of EHR, including names, addresses and social security numbers. This impacts the confidentiality, privacy, and data integrity of the EHR systems that are currently in place. In 2015, about 79 million patient records were stolen from the servers of the Anthem insurance firm due to security breaches. The 2017 attacks on the U.S. Department of Health impacted the data of about 2.6 million people. Furthermore, the global ransomware attack known as WannaCry in 2017 caused significant harm to 80 out of the 236 National Health Service (NHS) trusts. It is regarded as the largest ransomware attack in recorded history and affected more than 300,000 compromised server machines across more than 150 countries. FedEx was also affected. Electronic health record (EHR) theft is on the rise these days due to insufficient security measures, systems, and enforcement of regulations. This is a result of the records being kept in shared databases under the management and maintenance of service providers. By utilizing third-party service providers, a blockchain-enabled EHR management system promotes trust among industry players while providing security, transparency, and interoperability. It aids in the tracking and monitoring of all patient-related activities and events by providing specific information about transactions related to the patient, including diagnosis, medical records, tests, medications, and post-medical care. After that, this data is kept in a shared, unchangeable ledger. Through the use of Hyperledger Fabric, healthcare stakeholders can achieve security, interoperability, transparency, and trust without relying on outside service providers [4]. Hyperledger Fabric provides a comprehensive solution to the security, scalability, integrity, and interoperability problems inherent in traditional EHR management systems, thereby enabling a safer and more efficient health care ecosystem. Fig. 1 illustrates the difference between traditional centralised and decentralised model.




Traditional Centralised and Decentralised Model

*B. Hyperledger Fabric Network*

Hyperledger is an open source and free suite of technologies and applications that were introduced by the Linux Foundation in December 2015. The Hyperledger projects had entered an active development phase at the beginning of 2016, which involved the development of additional frameworks and tools. Among the Hyperledger frameworks / distributed ledger technology (DLT) are Sawtooth, Indy, Burrow, Iroha, and Fabric. Hyperledger continues to invest in the development of support tools. Blockchain access is made simple and efficient by a number of technologies [5]. Hyperledger Composer, Hyperledger Explorer, Hyperledger Cello, and Hyperledger Caliper are the most often used tools. Every Hyperledger tool provides a unique set of benefits for particular uses. On permissioned blockchains (such as Go, Java, and Node.js), distributed apps written in general-purpose programming languages are executed by a distributed operating system known as Hyperledger Fabric. It securely stores the execution history in an append-only replicated ledger data structure and does not come with any built-in cryptocurrency. Fabric departs from the conventional order-execute blockchain architecture by introducing the execute-order- validate architecture. Based on the technologies of permissioned blockchain, Hyperledger Fabric (HLF), developed by IBM, is used [6]. It is created to act as a foundation for blockchain applications in a variety of industries. Fig. 2 depicts the Hyperledger Fabric Network Architecture. The plug-and-play nature of HLF design allows for the flexibility of adding and removing components as needed. Docker container is provided to develop the application logic utilizing smart contracts, also known as chaincode. Transactions are only visible to nodes that have been assigned to a certain channel by use of a channel isolation technique. As a result, the network is able to keep transaction secrecy. Table I. has comparative analysis of different platforms based on various parameters and showcases how Hyperledger Fabric is superior to other platforms

1) *The Ledger:* The ledger, that stores vital information about business objects such as the present value of the objects' characteristics and the course of the transactions that led to those values, is a fundamental component of Hyperledger Fabric. It is divided into two sections: a blockchain and a world state. The former is a database holding the most recent values of a collection of ledger states [6]. A program can easily retrieve the current value of a state by using the global state, which eliminates the need to calculate it by walking through the entire transaction log. Blockchain is a digital record of every transaction that brought about the current condition of the world. Transactions are gathered into blocks that are added to the blockchain to track the evolution of changes that have resulted in this value over time.
2) *Membership Service Provider (MSP):* The standards used to authenticate and validate IDs are known as MSP. Members can access a blockchain network through the membership service provider (MSP). It controls user identity and verifies clients attempting to connect to the network. In order for these clients to propose transactions, credentials must be given to them [7]. The MSP uses a certificate authority (CA), which is essentially a plug-and-play interface, to approve or reject the user certificate based on the verified identity.
3) *Client:* The program, referred to as the client system, generates a transaction proposal. To comply with the endorsement policy, the client simultaneously sends the request for transaction to several peers in order to get proposal responses from endorsements [7]. After that, the transaction is sent to a number of orderer nodes so that it may be included in a block. This block is then subsequently shared with all peers for commitment and verification.
4) *Peers:* Chaincode is the name of the software that represents smart contracts and keeps track of the ledger within a file system, and it is executed by peer nodes. Since the ledger protocols are fully specified, Chaincode has access to the shared world state [8]. A transaction is endorsed by the endorsing peer using chaincode logic; the committing peer does not have chaincode logic. All peers maintain the ledger despite this disparity.
5) *Channel:* A channel that acts as a private communication mechanism is utilized to connect to the larger network. Every channel has a different ledger that is available to peers and participating organizations alike [8]. In situations where competing companies are involved, the capacity to maintain confidential communication between the firms alone via the same channel could prove advantageous.
6) *Ordering Service:* Orderer nodes are used by HLF to achieve consensus. An orderer node's main responsibilities include grouping transactions into a block and sending that block to all peers for confirmation. HLF uses three different ordering service implementations: Raft, kafka, and Solo. The consensus approach used by the ordering service is adaptable and modular. The ordering node in a solo-based system is the only one. Solo is therefore unsuitable for production because it still presents a single point of failure. It can be used, nevertheless, for testing and scholarly investigations. The ideas of a leader

and a follower are applied in Kafka [8]. The leader orderer is responsible for sending transactions to the mentioned nodes. As long as other nodes are operational, the decision on who should lead is made dynamically.

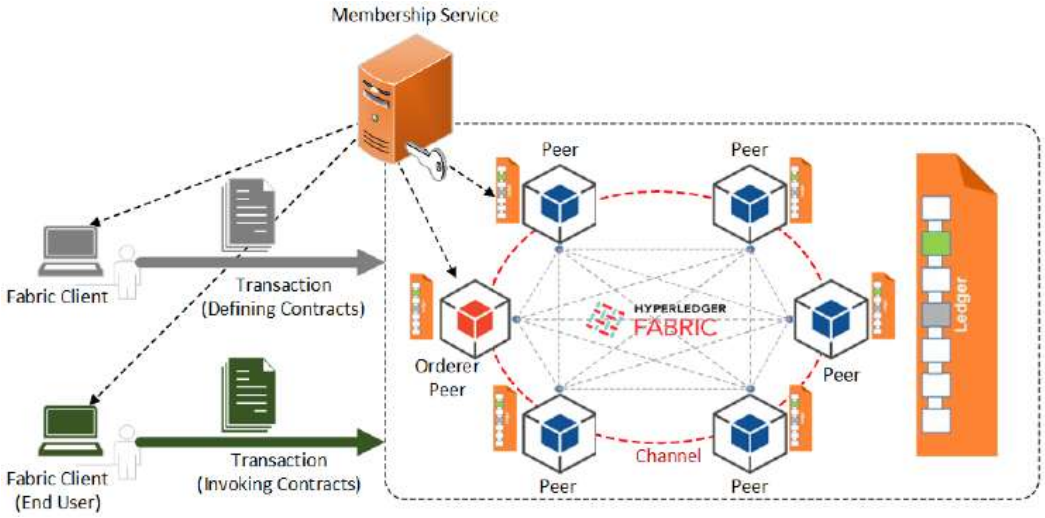



Fig 2. Hyperledger Fabric Network Architecture [9]

TABLE I. COMPARATIVE ANALYSIS OF DIFFERENT PLATFORMS BASED ON VARIOUS PARAMETERS

| Platform / Methodology | Security | Privacy | Auditability | Scalability | Cost |
|---|---|---|---|---|---|
| Traditional Databases | Low | Medium | Low | High | Medium |
| Cloud-Based Solutions | High | High | High | High | High |
| Ethereum-based | High | Low | High | Medium | Very High |
| Hyperledger Fabric | Very High | Very High | Very High | High | Medium |

## III. LITERATURE SURVEY

### *A. Research Paper Selection Criteria*

The selection of research papers for this literature review was guided by their relevance to key sub-topics, ensuring a comprehensive exploration of Hyperledger Fabric-based Electronic Health Records (EHR) management. Each paper was carefully chosen based on its contribution to understanding privacy preservation mechanisms, data privacy challenges, and the applications of the Hyperledger Fabric platform in healthcare, with a focus on data security and privacy challenges. Table II. gives a summary of our literature survey.

### *B. Mechanism for preserving privacy on blockchain*

Among the selected papers, "Secure Data Transmission of Electronic Health Records Using Blockchain Technology" (2023, Electronics - MDPI) describes a blockchain-based framework with a new privacy preservation mechanism. The SPAKE protocol for password-protected smart contract-based control of access ensures record privacy, control of access, and confidentiality [10]. Despite the advantages, the study acknowledges the complexity in implementing SPAKE encryption, shedding light on the intricacies of privacy mechanisms within blockchain-based EHR systems.

### *C. Data Privacy Concerns Associated with Customer Data*

The literature highlights the larger data privacy problems related with data obtained from customers or users. Papers highlight concerns such as computational expenses, integration difficulties, and data privacy issues

associated with public blockchains. The selected paper, "Preserving the Privacy of Electronic Health Records using Blockchain," explores challenges in data migration and system integration, emphasizing the need for a nuanced approach to balancing privacy and accessibility [11].

*D. Hyperledger Fabric Platform Applications in Healthcare*

The Hyperledger Fabric platform's uses in the healthcare industry are thoroughly reviewed in the literature, with an emphasis on issues like security, access control, data privacy, scalability and interoperability [12]. Hyperledger Fabric is a promising solution for improving the security, privacy, and interoperability of EHR systems, as demonstrated by papers like "MedBloc: A Blockchain-based Secure EHR System for Sharing and Accessing Medical Data" (2019, IEEE) and "Blockchain-based Decentralized Platform for Electronic Health Records Management" (2023, IEEE). These uses include transparent and safe platforms for exchanging and storing PHI, preventing illegal activity, and using smart contracts to guarantee data integrity.

*E. Hyperledger Fabric Platform Applications in Healthcare*

A crucial component of the literature review is addressing issues with data security and privacy. The chosen papers demonstrate the benefits and drawbacks of integrating Hyperledger Fabric into EHR administration. As an illustration, the 2023 Hindawi publication "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract" highlights robust security measures but also notes scalability and data privacy issues related to public blockchains [13]. Similar to this, "Securing Blockchain based Electronic Health Record using Multilevel Authentication" (2019, IEEE) acknowledges vulnerabilities like mining pool attacks and high storage requirements and addresses them by introducing a multilevel authentication scheme [14].

*F. Data Security and Privacy Challenges*

One of the most important parts of the literature review is addressing issues with privacy and data security. The selected papers demonstrate the benefits and drawbacks of using Hyperledger Fabric for EHR management. In "Electronic Healthcare Data Record Security Using Blockchain and Smart Contract" (2023, Hindawi), for example, robust security measures are emphasized, but scalability and data privacy issues related to public blockchains are noted [15]. Comparably, "Securing Blockchain based Electronic Health Record using Multilevel Authentication" (2019, IEEE) acknowledges vulnerabilities like mining pool attacks and high storage requirements, but presents a multilevel authentication scheme to counter user wallet attacks.

TABLE II : LITERATURE SURVEY SUMMARY

| Sr No. | Title | Study Context | Advantages | Disadvantages |
|---|---|---|---|---|
| 1. | Blockchain-based Decentralized Platform for EHR (2023, IEEE) | Secure PHI exchange, integration challenges | Secure and Transparent PHI Exchange | Computationally Expensive, Difficult Integration with Existing Systems |
| 2. | Electronic Healthcare Data Record Security (2023, Hindawi) | Scalability issues, data privacy concerns | Strong Security Mechanisms | Not Easily Scalable, Data Privacy Concerns with Public Blockchain |
| 3. | Secure Data Transmission of EHR (2023, Electronics - MDPI) | SPAKE protocol, Password-safe access control | SPAKE Protocol for Confidentiality and Access Control | Complex Implementation of SPAKE Encryption |
| 4. | Preserving Privacy of EHR using Blockchain (2020, ELSEVIER) | Permissioned private blockchain | Permissioned Private Blockchain | Difficult to Scale, Data Migration and System Integration Challenges |
| 5. | Securing Blockchain-based EHR using Multilevel Authentication (2019, IEEE) | Multilevel authentication, QR login | Multilevel Authentication Scheme | Prone to Mining Pool Attacks, High Storage Requirements |
| 6. | MedBloc: Blockchain-based Secure EHR System (2019, IEEE) | Smart contracts, User consent control | Smart Contracts for Data Integrity and User Consent Control | Potential Scalability Issues as System Expands |

## IV. FUTURE RESEARCH SCOPE

In this section, we delve into the future research trends shaping the landscape of Hyperledger Fabric-based Electronic Health Records (EHR) management. Drawing upon insights garnered from our comprehensive

literature review and the synthesized findings presented in the summarized studies, we navigate the evolving frontier of EHR systems with a keen focus on innovation, scalability, interoperability, and security [16]. By identifying emerging trends and potential areas of exploration, we aim to provide a roadmap for advancing the efficacy and adoption of Hyperledger Fabric in healthcare settings.

### *A. Scalability Solutions*

Addressing scalability concerns is imperative for the widespread adoption of Hyperledger Fabric in large-scale healthcare networks. Research efforts should focus on developing novel consensus algorithms, partitioning strategies, and network optimization techniques to facilitate efficient transaction processing and accommodate growing volumes of EHR data.

### *B. Data Security Enhancement*

Continual advancements in data security measures are essential to mitigate evolving cyber threats and safeguard sensitive healthcare information. Research endeavours should explore novel approaches for enhancing data security within Hyperledger Fabric-based EHR systems, including robust access control mechanisms, threat detection algorithms, and anomaly detection techniques [17].

### *C. Interoperability Standards*

Establishing interoperability standards is crucial for seamless data exchange and integration across heterogeneous healthcare systems. Future research should prioritize the development of interoperability frameworks, data exchange protocols, and standardization initiatives to foster interoperability among disparate EHR platforms and healthcare stakeholders [18].

### *D. User-Centric Design*

Emphasizing user-centric design principles is paramount for enhancing user experience and fostering user acceptance of Hyperledger Fabric-based EHR systems. Future research should prioritize usability studies, user feedback mechanisms, and user interface optimization strategies to ensure intuitive and seamless interaction with EHR platforms by healthcare professionals, patients, and other stakeholders [19].

## V. CONCLUSION

In conclusion, the literature review underscores Hyperledger Fabric's transformative potential in Electronic Health Records (EHR) management, despite encountering significant challenges. The analysis reveals that while the platform offers robust solutions for enhancing security, privacy, and interoperability through decentralized applications (DApps), smart contracts, and innovative encryption protocols like SPAKE, scalability issues, and integration difficulties remain prominent hurdles. However, leveraging Hyperledger Fabric's permissioned blockchain framework can address these challenges by providing enhanced data privacy and control, mitigating concerns surrounding public blockchains. Additionally, the platform's modular architecture facilitates seamless integration with existing healthcare systems, resolving interoperability issues. Furthermore, its consensus mechanisms and smart contracts ensure data integrity and security, safeguarding against unauthorized access. Looking ahead, collaborative efforts among stakeholders are essential to further develop and refine Hyperledger Fabric for EHR management. Future research should prioritize innovations in scalability solutions, interoperability standards, and user-friendly interfaces to maximize its benefits in healthcare [20]. Hyperledger Fabric can indeed revolutionize EHR management, paving the way for secure, efficient, and interoperable healthcare systems in the digital age.

## REFERENCES


[1] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads and Y. -C. 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 Computing And Communications pp. 594-601, doi: 10.1109/TrustCom/BigDataSE.2019.00085.

[2] B. L. Radhakrishnan, A. S. Joseph and S. Sudhakar, "Securing Blockchain based Electronic Health Record using Multilevel Authentication," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 699-703, doi: 10.1109/ICACCS.2019.8728483.

[3] S. Ballal, Y. Chandre, R. Pise, B. Sonare and S. Patil, "Blockchain-Based Decentralized Platform for Electronic Health Records Management," 2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), New Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICBDS58040.2023.10346392.

[4] Sanjeev Kumar Dwivedi, Ruhul Amin, Jegatha Deborah Lazarus, Vijayakumar Pandi, "Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment", Security and Communication Networks, vol. 2022, Article ID 4645585, 10 pages, 2022. https://doi.org/10.1155/2022/4645585
[5] Yogesh Sharma, B. Balamurugan,Preserving the Privacy of Electronic Health Records using Blockchain, Procedia Computer Science, Volume 173, 2020, Pages 171-180, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.06.021
[6] Sonkamble, R.G.; Bongale,A.M.; Phansalkar, S.; Sharma, A.; Rajput, S. Secure Data Transmission of Electronic Health Records Using Blockchain Technology. Electronics 2023, 12, 1015. https://doi.org/10.3390/electronics12041015
[7] Reegu, F.A.; Abas, H.;Gulzar, Y.; Xin, Q.; Alwan, A.A.; Jabbari, A.; Sonkamble, R.G.; Dziyauddin, R.A. Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System, Sustainability 2023, 15, 6337. https://doi.org/10.3390/su15086337
[8] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
[9] Honar Pajooh H, Rashid MA, Alam F, Demidenko S. Experimental Performance Analysis of a Scalable Distributed Hyperledger Fabric for a Large-Scale IoT Testbed. Sensors. 2022; 22(13):4868. https://doi.org/10.3390/s22134868
[10] Nishi, Farjana & Shams-E-Mofiz, Mahizebin & Khan, Mohammad & Alsufyani, Abdulmajeed & Bourouis, Sami & Gupta, Punit & Saini, Dinesh. (2022). Electronic Healthcare Data Record Security Using Blockchain and Smart Contract. Journal of Sensors. 2022. 1-22. 10.1155/2022/7299185.
[11] Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE 15(12): e0243043. https://doi.org/10.1371/journal.pone.0243043
[12] Veeramakali, T., Siva, R., Sivakumar, B. et al. An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. J Supercomput 77, 9576–9596 (2021). https://doi.org/10.1007/s11227-021-03637-3
[13] Makwana Bhavin, Sudeep Tanwar, Navneet Sharma, Sudhanshu Tyagi, Neeraj Kumar, Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications, Journal of Information Security and Applications, Volume 56,2021,102673, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2020.102673
[14] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos and J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems," 2021 IEEE International Mediterranean Conference on Communications and Networking (MeditCom), Athens, Greece, 2021, pp. 186-190, doi: 10.1109/MeditCom49071.2021.9647521
[15] Guipeng Zhang, Zhenguo Yang, Wenyin Liu, Blockchain-based privacy preserving e-health system for healthcare data in cloud, Computer Networks, Volume 203, 2022, 108586, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2021.108586
[16] Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE 15(12): e0243043. https://doi.org/10.1371/journal.pone.0243043
[17] Xi, Peng, Xinglong Zhang, Lian Wang, Wenjuan Liu, and Shaoliang Peng. 2022. "A Review of Blockchain-Based Secure Sharing of Healthcare Data" Applied Sciences 12, no. 15: 7912. https://doi.org/10.3390/app12157912
[18] Hashim, Faiza, Khaled Shuaib, and Farag Sallabi. 2022. "Connected Blockchain Federations for Sharing Electronic Health Records" Cryptography 6, no. 3: 47. https://doi.org/10.3390/cryptography6030047.
[19] McSeth Antwi, Asma Adnane, Farhan Ahmad, Rasheed Hussain, Muhammad Habib ur Rehman, Chaker Abdelaziz Kerrache, The case of HyperLedger Fabric as a blockchain solution for healthcare applications, Blockchain: Research and Applications, Volume 2, Issue 1, 2021, 100012, ISSN 2096-7209, https://doi.org/10.1016/j.bcra.2021.100012
[20] Sammeta, N., Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. Complex Intell. Syst. 8, 625–640 (2022). https://doi.org/10.1007/s40747-021-00549
[21] Mayer, André & André da Costa, Cristiano & Righi, Rodrigo. (2019). Electronic health records in a Blockchain: A systematic review. Health Informatics Journal. 26. 146045821986635. 10.1177/1460458219866350.