JNNCE Journal of Engineering & Management, Volume 6, No.1, Jan – June 2022 ISSN 2582-0079
This paper is presented at National Workshop on Cryptology NWC 2021, held at JNN College of Engineering, Shimoga during 18-20 Nov 2021

Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060111
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

# Survey on Robust Block-Chain Assisted Internet of Medical Things (IoMT) Infrastructure for Healthcare Sector

**Chandini A.G[1]*, P.I Basarkod[2]**

[1,2] REVA University, Bengaluru, Karnataka, India.

chandinimegu@gmail.com, basarkodpi@reva.edu.in

***Abstract***

*Security is the prime concern and also is a requirement for the increasing usage of the internet or public cloud for storing the data. To ensure advanced security and privacy preserving task, an opportunistic computing framework has been proposed, called Block-Chain technology. The technology of blockchain application is undergoing a conceptual evolution in the healthcare industry. Patients need to focus on the details of their own healthcare and restore management of their own medical information to preserve privacy. The rapid advancement of blockchain technology in healthcare sector promotes population healthcare, including patient-related data as well as medical records. The Blockchain technology provides patients with comprehensive, immutable records of data, and access to EHRs (Electronic Health Records) free from treatment website and service providers. The aim is to provide privacy thereby security, scalability, and interoperability in a distributed decentralised network, here privacy must be achieved in between the multiparty patients(nodes) to provide apt healthcare services in hospitals where health records are maintained in EHR/PHR (Electronic /Patient Health Records) using Block chain technology assisted with Internet of Medical Things (IoMT).*

Keywords: *Electronic Health Record/Patient Health Record (EHR/PHR); Block-Chain technology; Internet of Medical Things (IoMT).*

## 1. Introduction

Security is needed for preserving the integrity, confidentiality, availability of the information system resources.

In the last few years, the exponential rise in internet technologies and advanced software computing has broadened the horizon for the different socio-economic activities to enable knowledge-based decentralized computing and decision making. However, diversity in application demands and allied technologies often triggers academia-industries to achieve more effective solution(s). Despite of exponential rise in technologies and allied constructive purposes; the likelihood of operational challenges such as security, scalability, ease of access, personalized computing and resource access etc. have remained as challenge. Though, the development of advanced technologies such as Internet of things (IoTs), ,Big Data Analytics, Cloud computing, have gained wide-spread momentum service there is a mass contemporary socio-industrial demand. Amongst the major demands, healthcare sector being one of the most sough-after region alarming academia-industries to explore more advanced technologies to serve the at-hand purposes. Healthcare systems, which have the scopes of blockchain towards electronic healthcare records, telemedicine, require more effective role-based, permissioned access control with higher reliability, scalability, interoperability and resource efficiency.
The main aim is to design a highly robust blockchain architecture, a Distributed Ledger

Technology (DLT) and Smart Contracts with decentralized storage systems for higher scalability and interoperability of EHR/PHR (Electronic Heath Record/Patient Health Record) purposes and also to design and develop Anonymous lightweight encryption/hashing/homomorphic encryption with high privacy preserving to ensure seamless access control and attack-resilience.

## 2.Background Of Research

Providing a quality and reliable healthcare services with the advanced technology is the need for today's world. Moreover, the landscape of healthcare system is shifting towards a more patient-centric approach which focuses on two major elements namely to:

1. To always provide apt healthcare facilities and affordable treatment to patients.
2. Focusing on a good quality health care services means always ensuring patient health management at a high level [1].

However, Government federal rules and regulations are making processes lengthier and more tedious. Due to this, keeping such processes intact is not feasible in many cases to still provide effective care for patient's data. The major issue in providing quality healthcare services is the gap between payers and providers. In the healthcare sector, critical patient data and information remains hampered and scattered across different departments and systems [2]. Due to this, secure crucial data is not accessible and handily available in times of need. The existing healthcare ecosystem cannot be considered complete as multiple players in the system as they do not have a system in place for smooth process management. Moreover, it is also termed as inappropriate method for handling the information interchange and requires some major changes. The misuse of data available is preventing healthcare organizations from delivering appropriate patient care and highquality services for the sake of better health., These organizations are not able to fulfil the needs of patients, despite being efficient in terms of economy

Aforesaid factors have motivated academia-industries to exploit sustainable integration of IoT technologies (healthcare nodes to collect real-time data pertaining to the patient(s), processed data dissemination etc.) and cloud platform can enable different stakeholders to use real-time as well as logged information to make optimal diagnosis decisions as well as other management purposes. However, being centralized solution so far with multiple stakeholders, it often raises concerns towards data confidentiality, accessibility and reliability. Undeniably, considering providing cost-efficient patient care and high potential care, a large number of efforts have been made towards healthcare management of data. However, the classical cloud-based healthcare, client-server and data management systems are suffering from single point of failure, centralized data stewardship, data privacy, and system vulnerability issues. Electronic Healthcare Records (EHR) and PHR are used to record the diagnosis data of patient, such as thedoctor's notes on scan report of radiology images [3]. So, they include secure information regarding patient's privacy and identity. Thereby, development of pure decentralized Healthcare Information Systems (HIS) is a great challenging task in terms of technical structure and architecture of the systems. Designing a reliable and robust heath care system employing EHR/ PHR, that represent the base of many other hospital services, depends on keen finding the balance in a natural trade-off between many factors, such as level of decentralization, privacy, security, scalability and data throughput.

Undeniably, in the contemporary world of healthcare, EHR or PHR are entirely controlled by hospitals instead of patients, which complicates seeking medical advice from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. Convergence of physical and digital

identity and integration of various individual records, such as patient data (say, PHR or EHR), into a united repository remains a serious challenge [4]. On contrary, the development of a transparent, robust, and E-healthcare interoperable infrastructure has been a hard task due to many rules and legislatures like GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). Healthcare service providers prefer to store data about their patients in locked up ledgers, behind often layers of firewalls and security [5]. Such an approach limits the ability to get a real holistic view of the medical data history of a patient result in data breaches. Right to control personal data and Self-Sovereign identity comes into question, because patients are not handling their data explicitly. Unlike classical centralized permission-less infrastructures serving EHR or HIS purposes, there is the inevitable need of decentralized technologies to enable higher interoperability, scalability, reliability, time-efficient etc. to ensure seamless (permissioned) data access and control. Unfortunately, today's PHR management systems fail to give a traceable, reliable, trustful, and secure control over their patient medical data, which poses some serious problems to their accuracy and authenticity. Moreover, most of the current approaches for managing PHR systems has leveraged that are centralized that not only make medical data sharing difficult but also pose a risk of traffic signaling or single point of failure problem. Moreover, telemedicine being one of the most sought healthcare technologies too is vulnerable due to high risks in the development and implementation, such as restricted access across medical fraternity, data breach, incorrect diagnosis of data and patient prescription, fraud, and abuse [6].

To meet above stated demands, a recently emerged technology named Blockchain has can be of great significance. Unlike classical cryptosystem based EHR security solution, blockchain technologies offers an encrypted ledger and distributed ledger designed to allow the creation of tamper-proof records and immutable records of data at different locations. While blockchain may enhance IoT with data integrity, innate security, and autonomous governance, IoT data management and allocation of IoT in blockchain still are remaining as an architectural concern, especially for healthcare sector, where there can be a large number of stakeholders with distinct and of course different roles and responsibilities [7].

However, as a distributed decentralized technology, Blockchain can be very beneficial, giving patients control over their own data and self-sovereign identity. To the extent of our knowledge, there is no literature covering the same concerns? Though, blockchain technology provides patients with comprehensive, immutable records, and access to EHRs; however, retaining patient's concerns and turning it as permissioned model, unlike permission-less model has remained challenge so far, due to commerce-centric institutional behave and lack of policies [8].

## 3.Data Block Structure

Data Block Structure is shown in figure 1.

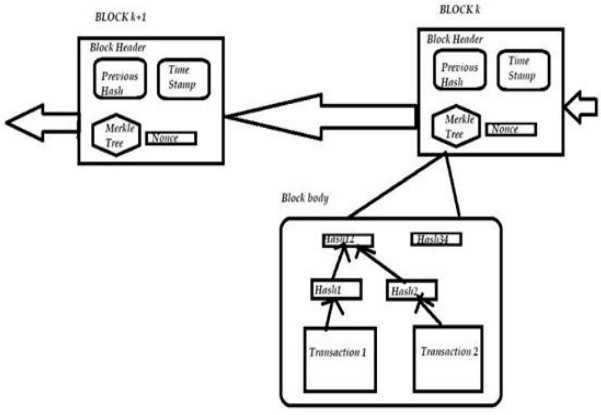


Figure 1: Data Block Structure

Block header: The header of Block contains the below listed data attributes required to verify the data block.

• Hash: The hash value can be formulated as

Hash12 = Hash (Hash1 + Hash2) = Hash [(Tx1.Hash) + (Tx2.Hash)]. The SHA256 hash of the block

• Previous hash: Previous block hash is considered which is used for block validation.

• Merkle Root: A Merkle tree root hash is a structure used to store a group of transactions present in each block.

• Nonce: It is a random number. It refers to a unique number that is generated by proof of work operation on miner nodes, in order to produce a hash value below a target difficulty level.

• Timestamp: It is the timestamp of the transaction in the block, and it also refers to the time of when the data received in the block.

## 4.Critical Review Of Literatures And Identification Of Research Gaps

Blockchain As Holistic Security Model for Healthcare Sector: Exploring Pros and Cons of the Existing Systems.

One of the most disruptive technologies is Blockchain, that has taken the world by storm nowadays. A blockchain is defined as a distributed ledger that keeps record storage of transactions and activities happening throughout the IoT network [9]. Once a piece of information or data is added to the distributed ledger, no one can change/ alter is the most unique factor of a blockchain. The information stored on a blockchain is secure. However, unlike classical bitcoin-based approaches, healthcare sector requires blockchain to have more decentralized permissioned role-based access control, which makes it more complex than the classical architectures. Healthcare systems, which have the scopes of blockchain towards electronic healthcare records, telemedicine, supply chain management etc., require more effective role-based, permissioned access control with higher reliability, scalability, interoperability and resource efficiency [10].

Looking into the past works or literatures pertaining to the Blockchain based EHR solutions, it can be found that the majority of the classical Blockchain based EHR solutions have applied, like Hyperledger Fabric or Ethereum, that allow running smart contracts, that specify business logic in critical cooperative applications. Applications like EHR or PHR being multiple stakeholder scenario demands Smart-contract type of verification module to ensure optimal block encryption followed by chaining. Despite of the high significance, any presence of software defects in these smart contracts can cause failures, including severe high security problems [11]. Unfortunately, no literature, especially pertaining to blockchain based EHR focus on fault-condition of the aforesaid middleware, which could adversely affect overall performance. And therefore, designing a smart-contract assisted blockchain model requires ensuring bug-free logics at the middleware as well as the cloud platform. It also requires formal verification and runtime protection mechanisms to ensure seamless EHR access and allied control over multipart infrastructure. Formal verification and runtime protections have to complement built-in platform checks to guarantee proper dependability of blockchain systems. To achieve it, strengthening smart contracts verification and robust encryption or hashing can be a key research scope [12].

Interestingly, most of the recent research works on blockchain in the healthcare domain have focused primarily on the permission-less Bitcoin Blockchain network that are suffering the from drawbacks such as limited scalability, high energy consumption and low throughput in transaction. Consequently, there is a need for a fault-tolerant, scalable, secure, traceable, and private blockchain to suit the healthcare domain requirements[13]. Additionally, major classical Blockchain based approaches, especially interfaced with IoT and cloud are found suffering from higher interoperability and scalability problem with increased cost. It requires optimization specially in terms of

permissioned smart-contracts, block-size, storage and lightweight encryption [14]. To alleviate this problem fault-less, smart contracts (for multi-party authorization), and decentralized storage systems such as the Interplanetary File Systems (IPFS) with lightweight encryption including adaptive attribute-based encryption or signature, Diffie-Hellman or Homomorphic encryption can be of great significance, which can also be considered as the key requirement behind this study.

Undeniably, majority of the decentralized database in blockchain focuses on data security and privacy [15]. Also, the consensus mechanism (same as Smart Contracts for data validation and verification) in it makes sure that data is secured and legitimate. Still, it raises new security issues such as majority attack and double spending, which can't be suitable for a EHR solution [16]. Moreover, being patient-doctor dynamic scenario where more patients subscribe or unsubscribe various medical services frequently in the database or cloud, unlike other methods lightweight encryption and high privacy preserving is must [17]. It can also be designed to reduce the computation with anonymous authentication and privacy access control. The proposed research considers this fact as one of the motivations behind this study.

Thus, in sync with above stated discussions, in this research the key emphasis has been made on achieving the following:

Patient-centric role-based permissioned access control with fault-less smart-contracts module for verification and access control.
Anonymous lightweight encryption/hashing/homomorphic encryption with high privacy preserving to ensure seamless access control and attack-resilience.

Distributed Ledger Technology (DLT) and Smart-Contracts (multi-party authorization or multiple signatures based smart contract) assisted Blockchain (BC) technology with decentralized storage systems such as the Interplanetary File Systems (IPFS), Web3 (or Ethereum Swarm, native base layer service of the Ethereum Web3 stack)) for higher scalability and interoperability of EHR/PHR systems.
The above stated key-points can be considered as the key gaps behind this research.

Considering the significance of a robust Blockchain assisted EHR solution for healthcare solution, in this research the key intend is made on designing a highly robust blockchain architecture with better scalability, interoperability, reliability, lightweight computation and resource efficiency (say, storage efficiency), which are must towards HIS systems[18]. Realizing the key components of blockchain technologies including encryption or cryptosystem, Smart Contracts, distributed ledger, and storage, this proposed research intends to make enhancement at each layer of the blockchain architecture to ensure robustness of the proposed solution [19].

Undeniably, in the past a few researches have been made towards blockchain based EHR systems; however, the key issues such as fault or vulnerability in classical Ethereum or Hyperledger blockchain frameworks which have been found possessing vulnerability (Ref., vulnerability in Ethereum blockchain, Oyenet, 2018)[20]. Additionally, most of the existing approaches employs, even including Ethereum framework apply Smart Contracts, a module or logic dedicated towards user's verification and access control are found to be limited due to present vulnerability. This as a result can degrade the overall security aspects of the blockchain. To alleviate it, in this research a fault-less Smart Contract model is proposed to be implemented with Ethereum framework with multi-party authorization and access control. Here, the prime motive is to reduce any probability of vulnerability caused access-manipulation at the Smart Contract for

Ethereum based implementation (OYENET identified a number of vulnerabilities in classical Ethereum service smart contracts) [21]. Interestingly, a few existing approaches have applied consensus based Smart Contracts or blockchain architecture; however, fail to address the vulnerability caused due to as majority attack and double spending, which can be highly probable in multi-party scenario such as EHR or PHRs [22]. In this case, strengthening block-chain with role-based permission architecture is must. The proposed work intends to design a role based permissioned blockchain architecture with patient centric access control to have higher interoperability [23]. Additionally, to strengthen scalability (and decentralized access control and governance) of the proposed solution, unlike classical cloud-based architectures or chain-based (often called ON-CHAIN STORAGE) data storage, this research aims to employ Web3 technologies and decentralized storage of interplanetary file systems (IPFS)[24]. This as a result can not only avoid possible internal attacks due to higher decentralized architecture (primarily it happens on chain-based data storage) but can also enhance seamless or privacy preserved access control across the network [25].

In most of the blockchain techniques, fulfilling timely computation and secure private key cryptography has remained a challenge [26]. For instance, SHA256 or MD5 which are the most used cryptography methods for the classical blockchain architecture are highly attack-prone towards collision attack, primage attack and attacks on wallet. Being in multi-part computation environment such attack probability can increase significantly [27]. Therefore, to avoid such problems, in this research a first of its kind adaptive lightweight attribute-based signature or encryption method is proposed. Though, the use of homomorphic encryption too can give higher level or attack-resilience. The use of above stated encryption model can make the proposed blockchain architecture more anonymous and privacy preserved and therefore would have higher node's security [28].

Summarily, the overall research goal can be stated as a Distributed Ledger Technology (DLT) and Smart-Contracts (multi-party authorization with multi-signature smart contracts) assisted Blockchain (BC) technology with decentralized storage systems such as the Interplanetary File Systems (IPFS), Web3 for higher scalability and interoperability of EHR/PHR purposes[29]. Thus, taking into consideration of above stated key research goals and allied scopes, in this research a few objectives have been identified. These are:

To design a role-based permissioned access control model for blockchain-IoT architecture to be used in EHR systems.
To design a state-of-art new fault-less Multi-Signature Smart Contract (MSSC) assisted blockchain architecture for nodes or user's verification and authorization for seamless access control and governance.
To design a lightweight encryption model such as attribute based signature or re-encryption (also called revocation attribute based lightweight signature) (and/or homomorphic encryption) for privacy preserved and anonymous block-encryption in blockchain architecture.
To implement the proposed blockchain architecture with decentralized ledger strategically interfaced with decentralized storage systems such as the Interplanetary

File Systems (IPFS), Web3 (Web3 (or Ethereum Swarm, Ethereum Web3 stack))for higher scalability and interoperability.
To implement overall proposed blockchain-based EHR/PHR solution with fault-less Smart Contract enabled Ethereum service or blockchain platform, and examine performance in terms of security, interoperability, scalability etc.

## 5.Objectives Of Research Work

In this research the key emphasis has been made on achieving the following objectives:

To design and develop a patient centric role-based permissioned access control model for blockchain-IoT architecture to be used in EHR systems.

To design and develop a lightweight encryption model such as attribute based signature or re-encryption (and/or homomorphic encryption) for privacy preserved and anonymous block-encryption in blockchain architecture.

To design and develop a Distributed Ledger Technology (DLT) and Smart-Contract blockchain-based EHR/PHR solution with fault-less Smart Contract enabled Ethereum service or blockchain platform, and examine performance in terms of security, interoperability, scalability etc.

## 6.Methodology or Approach Intended to be Adopted in the Execution of the Research

To simulate the overall proposed blockchain-IoT system with IoT signifying nodes or users with distinct roles and access-level. The Process flow is shown in figure 2.

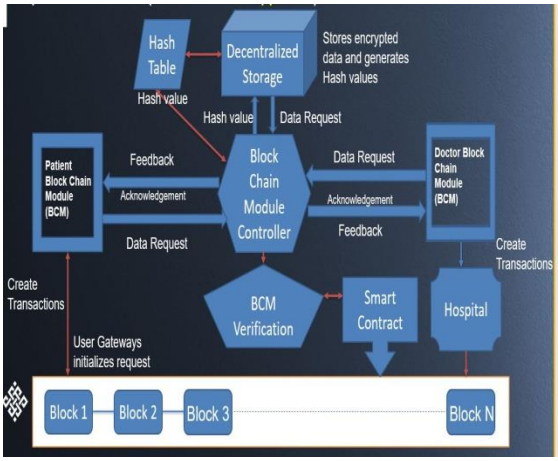


Figure 2: Process flow (Patient Centric Approach

Explanation of Steps in Proposed Methodology:

The user gateways initialize the request to create and upload a new transaction into Patient Block Chain Module (BCM).

Patient Blockchain module executes it and forwards the request to BCM controller.

BCM Controller in sync with Smart Contract Verifies and validates the request and sends back the acknowledgement for upload.

Once getting feedback, the user gateway selects the patient data collected through Wireless Area Network IoT. The data is first encrypted with public key and uploaded.

The decentralized storage stores the encrypted data with respect to the user node(Patient ID, Name) and applies SHA 256 hash algorithm, to generate Hash , which is kept in Decentralized storage and Decentralized Hash Table.

The user transactions (Multiple transactions) are grouped into data block. To append block chain Data blocks information is inserted into pool of transaction for confirmation.

The Uploaded transaction is updated to the gateway.

The user connects with Block chain network and prepares a transaction by sending request and signs it with private key for data access.

BCM Manager verifies the data using Smart Contract.

The Block chain Module Controller then decrypt the request and returns the data to user.

The data is updated to decentralized storage and Bundle hash in hash table is updated.

Doctor requests for data access through Smart Contract.

The patient then generates re-encryption key and sends to Smart Contract.

Smart Contract generates hash and re-encryption key to BCM verification unit.

BCM verification unit requests and retrieves the data bundle from storage.

Smart Contract selects re-encryption oracle on BCM verification unit and asks doctor for its choice.

BCM verification unit re-encrypts the bundle from patient key to doctor key and sends to doctor.

The doctor decrypts the bundle that makes data verifiable for him/her.

## 7. Conclusion

The overall research goal can be stated as a Distributed Ledger Technology (DLT) and Smart-Contracts (multi-party authorization with multi-signature smart contracts) assisted Blockchain (BC) technology with decentralized storage systems such as the Interplanetary File Systems (IPFS), Web3 for higher scalability and interoperability of EHR/PHR purposes. Thus, taking into consideration of above stated key research goals and allied scopes, in this research outcomes are:

To design a role-based permissioned access control model for blockchain-IoT architecture to be used in EHR systems.[34]

To design a state-of-art new fault-less Multi-Signature Smart Contract (MSSC) assisted blockchain architecture for node's or user's verification and authorization for seamless access control and governance.

To design a lightweight encryption model such as attribute based signature or re-encryption (also called revocation attribute based lightweight signature) (and/or homomorphic encryption) for privacy preserved and anonymous block-encryption in blockchain architecture.[37]

To implement the proposed blockchain architecture with decentralized ledger strategically interfaced with decentralized storage systems such as the Interplanetary File Systems (IPFS), Web3 (Web3 (or Ethereum Swarm, native base layer service of the Ethereum Web3 stack))) for higher scalability and interoperability.

To simulate the overall proposed blockchain-IoT system with IoT signifying nodes or users with distinct roles and access-level.[36]

Unlike classical Bitcoins based blockchain architectures, in the proposed work, the Smart-Contract model is supposed to be designed and implemented (with Ethereum blockchain) in such manner that it provides patient's control over its data in such way that it retains decentralized, immutable, transparent, traceable, trustful, and secure environment. Additionally, it proposes to design the architecture in such manner that a patient can retain access control right, without manipulation ability [31]. In other words, a patient can control other's access on its data across the multi-party computing environment; however, can't make changes or manipulation to its own data to preserve data purity. Additionally, the design is supposed to be made in such manner that it follows "SNOWBALL AFFECT", signifying that a small change in key or allied artifacts affects more change across the block to ensure higher security [32]. Noticeably, based on suitability and ease of implementation Ethereum and/or Consortium blockchain model can be taken into consideration [33].

## References

1. Tandon, A. Dhir, A.K.M, N. Islam, M. Mäntymäki, Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda, Computers in Industry 122 (2020) 103290, 2020.

2. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences—A scoping review, International Journal of Medical Informatics 134 (2020) 104040, 2020.

3. Abugabah, N. Nizamuddin and A. A. Alzubi, Decentralized Telemedicine Framework for a Smart Healthcare Ecosystem, in IEEE Access, Vol. 8, 2020, pp. 166575-166588. doi: 10.1109/ACCESS.2020.3021823.

4. Bhawiyuga, A. Wardhana, K. Amron and A. P. Kirana, Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network, 2019 6th NAFOSTED Conference on Information and Computer

Science (NICS), Hanoi, Vietnam, 2019, pp. 55-60. doi: 10.1109/NICS48868.2019.9023797.

5. E. B. Tomaz, J. C. D. Nascimento, A. S. Hafid and J. N. De Souza, Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain, in IEEE Access, vol. 8, pp. 204441-204458, 2020,
doi: 10.1109/ACCESS.2020.3036811.

6. Manzoor, M. Samarin, D. Mason and M. Ylianttila, Scavenger Hunt: Utilization of Blockchain and IoT for a Location-Based Game, in IEEE Access, Vol. 8, pp. 204863-204879, 2020,
doi: 10.1109/ACCESS.2020.3037182.

7. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid and M. F. Yusof, Scalability Challenges in Healthcare Blockchain System—A Systematic Review, in IEEE Access, vol. 8, pp. 23663-23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

8. S.Koushik, B. Jain, N. Menon, D. Lohia, S. Chaudhari and V. K. B.P, Performance Analysis of BlockChain-based Medical Records Management System, 2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2019, pp. 985-989.
doi: 10.1109/RTEICT46194.2019.9016812.

9. Shahnaz, U. Qamar and A. Khalid, Using Blockchain for Electronic Health Records, in IEEE Access, Vol. 7, 2019, pp. 147782-147795. doi: 10.1109/ACCESS.2019.2946373

10. Houtan, A. S. Hafid and D. Makrakis, A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare, in IEEE Access, Vol. 8, pp. 90478-90494, 2020,
doi: 10.1109/ACCESS.2020.2994090.

11. Buzachis, A. Celesti, M. Fazio and M. Villari, On the Design of a Blockchain-as-a-Service-Based Health Information Exchange (BaaS-HIE) System for Patient Monitoring, 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 2019, pp. 1-6.
doi: 10.1109/ISCC47284.2019.8969718

12. Parameswari and V. Mandadi, Healthcare Data Protection Based on Blockchain using Solidity, 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, United Kingdom, 2020, pp. 577-580.
doi: 10.1109/WorldS450073.2020.9210296.

13. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. Song, A. K. Bashir and A. A. A. El-Latif, DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems, in IEEE Access, vol. 8, pp. 111223-111238, 2020.
doi: 10.1109/ACCESS.2020.2999468.

14. F. Anjum et al., Mapping Research Trends of Blockchain Technology in Healthcare, in IEEE Access, vol. 8, pp. 174244-174254, 2020, doi: 10.1109/ACCESS.2020.3025011.

15. Jin, Y. Luo, P. Li and J. Mathew, A Review of Secure and Privacy-Preserving Medical Data Sharing, in IEEE Access, Vol. 7, pp. 61656-61669. 2019.
doi: 10.1109/ACCESS.2019.2916503.

16. Kim, S. Kim, J. Y. Hwang and C. Seo, Efficient Privacy-Preserving Machine Learning for Blockchain Network, in IEEE Access, vol. 7, pp. 136481-136495, 2019.
doi: 10.1109/ACCESS.2019.2940052.

17. Yang, H. Cha and Y. Song, Secure Identifier Management Based on Blockchain Technology in NDN Environment, in IEEE Access, Vol. 7, 2019, pp. 6262-6268.
doi: 10.1109/ACCESS.2018.2885037.

18. Fan et al., Blockchain-Based Secure Time Protection Scheme in IoT, in IEEE Internet of

Things Journal, Vol. 6, No. 3, pp. 4671-4679. June 2019, doi: 10.1109/JIOT.2018.2874222.

19. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla, Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection, 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 2019, pp. 1-7.
doi: 10.1109/CAMAD.2019.8858469.

20. Wazid, A. K. Das, S. Shetty and M. Jo, A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things, in IEEE Access, Vol. 8, pp. 88700-88716, 2020. doi: 10.1109/ACCESS.2020.2992467.

21. Kumar, C. Parangjothi, S. Guru and M. Kiran, "Peer Consonance in Blockchain based Healthcare Application using AI-based Consensus Mechanism," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-7, doi: 10.1109/ICCCNT49239.2020.9225550.

22. Li et al., "ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains," in IEEE Systems Journal, Vol. 14, no. 2, pp. 2042-2053, June 2020, doi: 10.1109/JSYST.2019.2937930.

23. Akkaoui, X. Hei and W. Cheng, EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange, in IEEE Access, Vol. 8, pp. 113467-113486, 2020, doi: 10.1109/ACCESS.2020.3003575.

24. Lee, M. G. Kim and I. K. Kim, SHAREChain: Healthcare data sharing framework using Blockchain-registry and FHIR, 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), San Diego, CA, USA, 2019, pp. 1087-1090, doi: 10.1109/BIBM47256.2019.8983415.

25. Alexaki, G. Alexandris, V. Katos and N. E. Petroulakis, Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions, 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, 2018, pp. 1-6, doi: 10.1109/CAMAD.2018.8514954.

26. Chakraborty, S. Aich and H. Kim, A Secure Healthcare System Design Framework using Blockchain Technology, 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 260-264, doi: 10.23919/ICACT.2019.8701983.

27. Son, J. Lee, M. Kim, S. Yu, A. K. Das and Y. Park, Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain, in IEEE Access, Vol. 8, pp. 192177-192191, 2020, doi: 10.1109/ACCESS.2020.3032680.

28. Tanwar, Q. Bhatia, P. Patel, A. Kumari, P. K. Singh and W. Hong, Machine Learning Adoption in Blockchain-Based Smart Applications: The Challenges, and a Way Forward, in IEEE Access, Vol. 8, pp. 474-488, 2020, doi: 10.1109/ACCESS.2019.2961372.

29. Wang et al., "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," in IEEE Transactions on Computational Social Systems, Vol. 5, no. 4, pp. 942-950, Dec. 2018, doi: 10.1109/TCSS.2018.2865526.

30. Jaiman and V. Urovi, A Consent Model for Blockchain-Based Health Data Sharing Platforms, in IEEE Access, Vol. 8, pp. 143734-143745, 2020,
doi: 10.1109/ACCESS.2020.3014565.

31. Ni, X. Huang, J. Zhang and R. Yu, HealChain: A Decentralized Data Management System for Mobile Healthcare Using

Consortium Blockchain, 2019 Chinese Control Conference (CCC), Guangzhou, China, 2019, pp. 6333-6338,
doi: 10.23919/ChiCC.2019.8865388.

32. Yánez, R. Mahmud, R. Bahsoon, Y. Zhang and R. Buyya, Data Allocation Mechanism for Internet-of-Things Systems With Blockchain, in IEEE Internet of Things Journal, Vol. 7, no. 4, pp. 3509-3522, April 2020,
doi: 10.1109/JIOT.2020.2972776

33. Zheng, R. R. Mukkamala, R. Vatrapu and J. Ordieres-Mere, Blockchain-based Personal Health Data Sharing System Using Cloud Storage, 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-6,
doi: 10.1109/HealthCom.2018.8531125.