International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 12 Issue 4, July.-August, 2024, Impact Factor: 8.376

Comprehensive Survey of Access Control Schemes and Techniques in Blockchain for Enabling Secure Communication in Healthcare Systems

Mrs. Sanketi Raut[1], Dr. Rahul Thour[2]

[1]Ph.D. (CSE) Scholar, Desh Bhagat University, Mandi Gobindgarh, Punjab
[2]Assistant Professor, Department of CSE, Desh Bhagat University, Mandi Gobindgarh, Punjab

ABSTRACT

Recent advancements in mobile device development and the quick expansion of wireless communication technologies have greatly aided in the automation of remote patient monitoring and diagnosis in healthcare systems. Providing a guarantee for network security is crucial right now. The security of electronic health records has received more attention, which is significant since patient medical records shared via distant healthcare systems are vulnerable to security breaches that may compromise patient diagnosis accuracy. In order to prevent security breaches, access control methods that would restrict access to patient medical data were designed. Blockchain, a multifunctional technology that has attracted a lot of interest recently, can help with these issues. Nevertheless, in order to examine the whole history of transactions, each peer in the blockchain network keeps the ledger in the same state, which causes scalability problems. However, this technology has various issues related to scalability, security, and privacy. The security measures in the healthcare systems and various access control strategies will be investigated. The history of several approaches, together with their benefits, drawbacks, and potential implications, will be presented in order to highlight the weaknesses found in each method.

Keywords: Access control schemes, Block chain based healthcare system, Performance Improvement and Efficiency Models, Privacy and security in EHR system and Security and Privacy Enhancement Models.

INTRODUCTION

Although it is now harder for patients to get primary care doctors or practitioners, many nations are currently dealing with a significant rise in healthcare challenges. When one considers the term "blockchain," it is becoming more and clearer that this kind of technology is needed in the World Wide Web era, in addition to being extremely significant [1]. Blockchains are commonly regarded as distributed ledgers or decentralized record databases that contain all of the electronic transactions and exchanges that have occurred between the parties involved in a transaction. Every transaction that has ever been made is included in a blockchain's precise and verifiable record [2], [3]. Blockchain technology allows for the decentralized execution of transactions. As a result, blockchain can both significantly save costs and improve performance [4]. The Internet of Things (IoT) is a specific type of computing and communication environment made up of various computer devices, electromechanical devices, people, or animals with uniquely identifiable identities. By virtue of Internet Protocol addresses, these objects and devices are able to transfer data over a network without the need for human intervention [5], [6]. Massive volumes of data are generated by the Internet of Things' communication environment. To manage and analyze the data and draw meaningful conclusions from it, we therefore require a strong procedure. Artificial intelligence (AI) can facilitate the efficient execution of these tasks. When AI and IoT are combined, the result is the Internet of Intelligent Things (IoIT), an intelligent computing and communication ecosystem [7-8].

However, because IoIT-based communications are susceptible to many kinds of attacks, robust security measures are required.In addition, data integrity and privacy pose serious problems for the current industrial healthcare systems. It is our opinion that data privacy is the main factor connecting Active Data Privacy Attacks (ADPA) and Passive Data Privacy Attacks (PDPA) [8]. When an attacker attempts to alter, modify, or infer private information while it is being transported between two cooperating organizations, it is referred to as a data poisoning attack, or ADPA attack [9]. The

goal of these attacks is to change patients' real-time health data. Furthermore, it might have a negative effect on the effectiveness of data analytics powered by artificial intelligence (AI) or intrusion detection system (IDS) attack detection [10]. However, the attacker uses PDPA to either use data inference attacks to extract particular fundamental statistical traits or sniff (private) data from the training dataset [11]. An unauthenticated medical sensor can be easily utilized as a surveillance tool to follow and/or monitor private health information without the patient's knowledge in another scenario pertaining to privacy breaches and authentication [12]. Therefore, in order to prevent privacy breaches connected to authentication, an effective authentication method that controls participating IoT devices is also needed [13].

The purpose of this survey is to determine which blockchain access control mechanisms and techniques are used in various evaluation metrics, datasets, and research needs. This study also examines some limitations, such as inadequate data security, privacy, and security. About twenty-five research publications were analyzed in this study, with a focus on the challenges faced, the strategies used, the results obtained, and the parameters that were used. The study's objectives were to provide an overview of current practices and the advantages of block chain-based healthcare systems, as well as security and privacy in EHR approaches, integration of cutting-edge technologies, models for efficiency and performance improvement, models for enhancing security and privacy, and schemes and techniques for access control. The aspects listed below comprise the sections of this survey. The literature review's taxonomy of access control methods is expounded upon in Section 2. A concise overview of the techniques, datasets, metrics, results, and constraints is provided in Section 3, and the research gaps are covered in Section 4. Section 5 summarizes the conclusion.

TAXONOMY OF SCALABLE AND SECURE ACCESS CONTROL IN BLOCKCHAIN-ENABLED HEALTHCARE SYSTEM TECHNIQUE

Figure 1. depicts the taxonomy diagram Scalable and Secure Access Control in Blockchain-Enabled Healthcare Systems using a variety of methodologies, including integration of advanced technologies, privacy and security in EHR systems, access control schemes and techniques, security and privacy enhancement models, and block chain based healthcare systems.

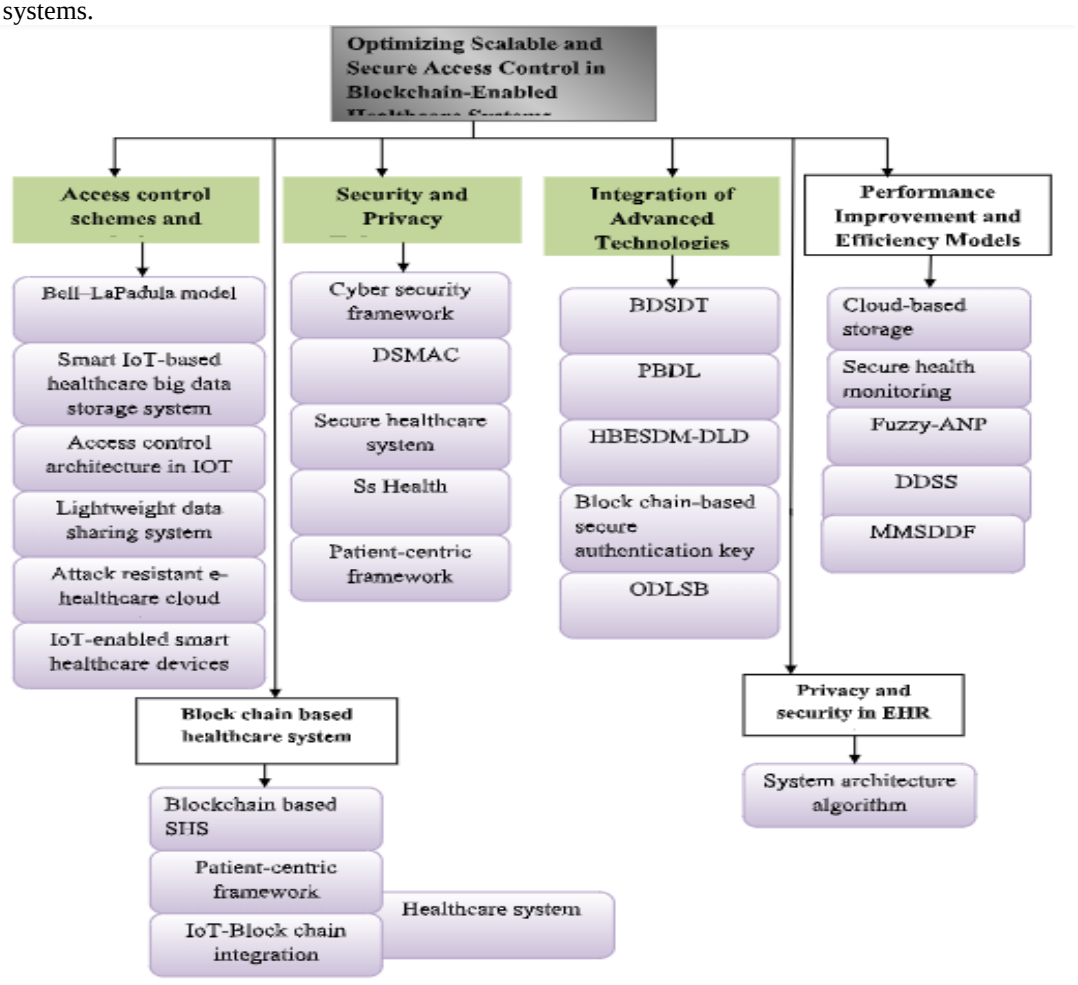

Figure 1. Depicts the taxonomy diagram Scalable and Secure Access Control in Blockchain-Enabled Healthcare Systems

Access control schemes and techniques:

Rakesh Tripathi et al. [1] improved the Bell-LaPadula model and included a new classification scheme for peers and transactions based on different levels of clearance and security. The access restriction technique additionally exacerbates the scalability issue with the healthcare blockchain network. Nonetheless, a significant issue facing the healthcare company was data security. Xianghan Zhenget al. [2] presented a smart IoT-based healthcare large data storage system with a self-adaptive access control method that preserves privacy. Comprehensive comparisons and simulations show the effectiveness of this clever healthcare big data storage technology, which has been officially proven safe. Nevertheless, the decryption technique of this scheme has a large computing overhead.The access control architecture for limited healthcare resources in the Internet of Things was introduced by Shantanu Pal et al. [3]. It protects valuable resources against uninvited modification while providing granular access to services for authorized users. Compared to previous suggestions that use IoT capabilities for access control, this strategy involves the least amount of extra overhead. But maintaining system users, resource management and implementing suitable policies continue to be difficult and complex tasks.Yang Yang et al. [4] suggested a straightforward data interchange system with two access control options for the Internet of medical things. Authorized data users can access and decode patient medical records using attribute secret keys under attribute-based access mode. Furthermore, this architecture makes it possible for rescue or emergency medical staff to quickly access the data. However, this scheme's lack of a decryption technique could present security issues.Wei Zhang et al. [5] presented an e-healthcare cloud system with fine-grained access control that is safeguarded against inference attacks. This technique can be readily expanded to enable search functionality and reduce computing costs. Nevertheless, there were still two major issues with this paradigm. It was once restricted to supporting the policy of black or white access restriction. They also experience the deluge of inferences. Akanksha Saini et al. [6] created an access control architecture that offers acceptable security performance for IoT-enabled smart healthcare devices and the medical system using blockchain technology as a platform for storage by utilizing blockchain-based smart contracts, however, results in a greater storage overhead delay in the response to access requests.

Security and Privacy Enhancement Models:

In a distributed fog computing environment, Amandeep Singh Sohal et al. [7] created a thoroughly detailed cyber security technique for recognizing malicious edge devices. The framework is effective in recognizing the malicious device and lowering the false IDS warning rate, according to the results. Nonetheless, the largest problem facing cloud service providers was identifying the invaders in the scattered cloud environment.HafidaSayi et al. [9] presented a novel Decentralized Self-Management of data Access Control (DSMAC) system that uses a blockchain-based identity concept to safeguard patient privacy. Patients can self-grant access privileges to their medical records and obtain the resources they require to maintain privacy by using this system. By reducing latency, this methodology achieves a higher level of security. However the computational cost of this model was very high.An improved method of securing and protecting patient privacy through remote patient monitoring was introduced by KebiraAzbeg [10]. The security of healthcare systems has demonstrably improved due to the experimental system. Still, there are issues with this model's processing, memory, and energy use.AlaaAwadAbdellatif et al. presented a novel approach to secure and intelligent healthcare, known as ssHealth [11]. It uses blockchain and edge computing to facilitate rapid emergency response, remote monitoring, and epidemic detection. This paradigm achieves minimal latency, large data rates, and anytime, anywhere data accessibility. It was difficult to guarantee that medical data could be accessed remotely by various authorized bodies in order to implement personalized medicine and large-scale, affordable healthcare.A patient-centric paradigm for a blockchain-enabled healthcare system that successfully addresses the issues of data privacy, authentication, and immutability was presented by AkhilendraPratap Singh et al. [16]. They also presented a performance analysis and an extensive deployment and implementation strategy for the recommended scheme, however handling the complexity of data processing and transfer while satisfying a range of security and privacy requirements proved fairly challenging.

Integration of Advanced Technologies:

Prabhat Kumar et al. [12] introduced a Blockchain-orchestrated Deep learning technique for Secure Data Transmission (BDSDT), a new secure data transmission application for IoT-enabled healthcare systems, by combining deep learning with blockchain technology. Tests conducted on two datasets show that this BDSDT model achieves accuracy near 99% using both datasets and surpasses current standards in blockchain and non-blockchain scenarios. However, this paradigm has trouble addressing data security concerns and data storage expenses.For industrial healthcare systems, Randhir Kumar [13] introduced a revolutionary architecture called Permissioned Blockchain and smart contract with Deep Learning (PBDL) to improve data safety and guarantee safe data sharing. The results show that the state-of-the-art, baseline, and classic BiLSTM techniques are outperformed in terms of detection rate and accuracy by the trials carried out on two datasets. Still, there are security concerns with this strategy.Deep learning (DL)-based diagnostics and a new hyper ledger blockchain-enabled secure medical data management platform called HBESDM-DLD were introduced by Naresh Sammeta and Latha Parthiban [19]. The idea being presented involves several stages of operation, including encryption, the best way to generate keys, secure data storage using a hyper-ledger blockchain, and diagnosis. This approach performed well in terms of scalable consensus technique, low latency, high throughput, and decentralization. Nonetheless, this approach still has issues with network node processing and storage limitations.

Mohammad Wazid et al. [20] provided a tutorial aimed at developing a universal blockchain-based safe authentication key management method for the IOT that combines high security and performance. Nonetheless, there are still issues with high computing, communication, and storage costs in this architecture. Adeep-learning-based secure blockchain (ODLSB) enabled IOT and healthcare diagnosis model was created by T. Veeramakali et al. [22]. The three primary processes of the proposed approach safe transaction, hash value encryption, and medical diagnosis achieve good accuracy performance. Nevertheless, there were still issues with this model's centralized architecture, privacy and security concerns, resource limitations, and a dearth of sufficient training data.

Performance Improvement and Efficiency Models:
Seyed Morteza Pournaghi et al. [8] presented a novel and safe method for efficiently exchanging medical data between patients, hospitals, and the entities consuming medical data.

Using cloud-based storage technology has several benefits, such as improved data sharing, quick data transmission, large store capacity, simple information access, and dynamic communication. Nevertheless, this approach came at a relatively high computational cost.An innovative and secure mechanism for effectively sharing medical data between patients, hospitals, and the entities consuming medical data was presented by Seyed Morteza Pournaghi et al. [8]. This makes it possible for medical professionals to monitor patients using medical sensors and respond appropriately on a frequent basis by accurately predicting illnesses in a faster, more cost-effective manner. Still, there are a number of security problems with this paradigm. Mohammad Zarour et al. [21] introduced an integrated Fuzzy Analytic Analytical Network Process (fuzzy-ANP) TOPSIS technique to evaluate the viability of blockchain technology models for safeguarding electronic health records.

This model achieved a high degree of precision and had a very high storage capacity. However, it was difficult to guarantee that medical data could be accessed remotely by many authorized bodies in order to achieve individualized therapy and large-scale, affordable healthcare. Bhaskara S. Egala et al. [23] developed the Distributed Data Storage System (DDSS) with blockchain technology to solve the issues with the blockchain-based cloud-centric IoMT healthcare system, such as high latency, high storage costs, and single points of failure. However, there are still several steps involved in utilizing blockchain technology to take advantage of distributed data storage systems and hybrid computing, including new standards, protocols, and methodologies. Rajakumar Arul et al. [24] presented the Multi-Modal Secure Data Dissemination Framework (MMSDDF) idea. It is utilized in IoMT to enable secure patient data access and control, and it is built on blockchain technology. When compared to other methods now in use, this model offers exceptional accuracy, prediction, minimal delay, latency, and response time. Even yet, there are still security issues, like the block chain's constrained storage region and the stored data's susceptibility to unwanted access.

Block chain based healthcare system:
A blockchain-based smart healthcare system (SHS) framework was presented by GautamiTripathi et al. [15] with the goal to achieve high scalability and high speed while maintaining inherent security and integrity of the system. However, there are a lot of difficulties and problems with this paradigm that pertain to user and data privacy, transparency, and security.A patient-centered architecture for a blockchain-enabled healthcare system was presented by Singh et al. [16]. It not only effectively responds to issues with immutability, authentication, and data privacy, but it also includes a performance study and a comprehensive deployment and implementation plan. It was extremely difficult to deal with the intricacy of data processing and transfer while meeting a variety of security and privacy criteria.In order to solve problems caused by a lack of IoT resources, Marah R. Bataineh et al. [17] developed architecture for combining IoT with Blockchain that combines a rich-thin client IoT strategy with an Ethereum Blockchain infrastructure.

High storagecapacity is achieved and the Blockchain mining approach can be implemented in IoT systems. However, this model had a very high computational cost. For the treatment of chronic illnesses, Ziyu Wang1 et al. [25] presented an IoT, Blockchain, and IPFS-based healthcare system.This solution offers daily data gathering, data exchange, and security as well as a number of other benefits for remote patient monitoring. Ensuring data integrity, controlling access to patient data, and protecting privacy are all achieved by the fully decentralized, high-security system that leverages IPFS, smart contracts, blockchain, and proxy re-encryption. Strong hybrid models are yet required in order to increase performance.

Privacy and security in EHR system:
An algorithm and system architecture for access control policies were provided by SudeepTanwar et al. [14] to assist users in achieving patient data security and privacy in the EHR system. In order to achieve superior results, this approach achieves high throughput, low latency, network security, and minimal communication time. But the computational cost of this model was very high.

SUMMARIZED ANALYSIS

Table 1.: An overview of the methods and scalable and secure access control in the blockchain-enabled healthcare system

Sr. No.	Model	Metrics	Research gaps
1	Bell–LaPadula model [1]	Execution time, validation time and access time	Data security
2	Smart IoT-based healthcare big data storage system [2]	Processing time	The decryption technique of this scheme has a large computing overhead.
3	access control architecture in IOT [3]	Time ms	Maintaining system users, resource management and implementing suitable policies continue to be difficult and complex tasks
4	Lightweight data sharing system [4]	Key size, master public key size, secret key size, cipher text size, user time, encryption time, and Dec time.	The lack of a decryption method in this scheme could pose security risks.
5	Attack resistant e-healthcare cloud system [5]	Time of registration, time of secret buffer, time of operation, time of revoking and time of computation.	Inference attack
6	IoT-enabled smart healthcare devices [6]	Average latency, transaction cost and time.	There is a larger delay of access request response owing to storage overhead.
7	Cyber security framework [7]	Response Time, number of request, number of queries processed	The largest problem facing cloud service providers was identifying the invaders in the scattered cloud environment
8	Cloud-based storage technology [8]	Key generation, encryption and decryption.	High computational cost
9	DSMAC [9]	Time, throughput, latency, encryption time and consumption rate	High computational cost
10	Secure healthcare system [10]	Processing time	Issues with this model's processing, memory, and energy use.
11	ssHealth [11]	Latency, security and cost	It was difficult to guarantee that medical data could be accessed remotely by various authorized bodies in order to implement personalized medicine and large-scale, affordable healthcare.
12	BDSDT [12]	FP, FN, TP, TN, Precision and F1 Score	However, this paradigm has trouble addressing data security concerns and data storage expenses
13	PBDL [13]	accuracy, precision, detection rate and F1-score	Still, there are security concerns with this strategy.
14	System architecture algorithm [14]	latency, throughput and Round Trip Time (RTT)	This model came at a very hefty computational cost
15	blockchain based SHS [15]	Time	There are a lot of difficulties and problems with this paradigm that pertain to user and data privacy, transparency, and security.
16	Patient-centric framework [16]	resource utilization, latency, and throughput,	It was extremely difficult to deal with the intricacy of data processing and transfer while meeting a variety of security and privacy criteria

17	IoT-Blockchain integration architecture [17]	Gas limit and used gas	But this model came at a very hefty computational cost.
18	Secure health monitoring system [18]	TP, TN, Positive Prediction Value & Negative Prediction Value	Still, there are a number of security problems with this paradigm.
19	HBESDM-DLD [19]	Accuracy F-Score Kappa	Nonetheless, this approach still has issues with network node processing and storage limitations.
20	Blockchain-based secure authentication key management [20]	Computational cost	Nonetheless, there are still issues with high computing, communication, and storage costs in this architecture

RESEARCH GAPS

Based on the extensive literature review provided, here are additional research gaps and challenges in the domain of access control schemes in Blockchain networks for healthcare systems.

- Even though Elimination approach of Blockchain guarantees data integrity and non-angularity, the selection of consensus algorithms demonstrate a notable impact on scalability and the volume of transactions. An emerging area of future work is to investigate the most efficient consensus algorithms for IoT-Health that consumes less energy while processing the health records' transactions.
- Mainstream authorization models are not very dynamic in the sense that access rights cannot be changed from time to time depending on the conditions (e. g. patient's status, roles of healthcare providers). Research could also be dedicated to flexible and context-dependent access control, which allows the timely availability of the data while providing maximum security [3][4].
- Implementation of Blockchain in healthcare should strictly follow legal guidelines (for example GDPR and HIPAA). Existent literature is limited in proposing Blockchain-based access control systems that inherently obey privacy laws and regulations of various regions [13][19].
- Blockchain is known to have compatibility issues, especially when implementing it in the current and evolving healthcare IT architectures. Business research should start by identifying standards and requirements for working with the existing IT systems to maintain data coherence and ensure the functionality of systems that will be integrated into the project [27].
- The healthcare industry is exposed to cyber attacks more frequently. Thus, inherent security of block chain comes from decentralization, however, many smart contracts and nodes' securities remain to be studied [7][25].
- Contemporary Blockchain-based access control has high costs during the first phases of its deployment, mainly tied to infrastructure, maintenance and energy. There are some limitations on the methods of finding viable cost-efficient frameworks that would actualize and sustain the investment [6][17].
- When it comes to patients' record, blockchain-based systems have created some ethical issues in terms of ownership, consent, and data utilization. For these ethical considerations, there is a need for the further research to discover how such frameworks that support patients' autonomy but also promote ethical use of data, could be implemented [15].

Addressing the Research Gaps:

To advance the field and address these research gaps, future studies could focus on the following:

- Investigate new consensus algorithms that are specific to healthcare experienced while keeping security, scale, and efficiency into consideration.
- Construct wise adaptive access control mechanisms that involve the use of real time data in decision making and also have an understanding of the environment.
- Ensure that Blockchain systems are initially designed to have privacy in their design that complies with all world-wide regulations.
- Develop standards and guidelines that would ensure that Blockchain can be integrated with current healthcare information technology systems.
- Utilize proper and stronger cyberspace security measures including authentication and anomaly detection for well protection of health care systems that rely on Blockchain.
- Further examine the best practices for the deployment of Blockchain in the area of health and factors that would make it economical for organizations to use it while still being sustainable.
- Ethical standards and code for the use of Patient data in Blockchain-based Healthcare ecosystem and Consent Management.

In this manner, researchers can help fill these gaps and create better security, efficiency and ethical Blockchain-based access control systems for healthcare to facilitate milestone advancement in the patient's care and data management system.

CONCLUSION

In conclusion, literature review on access control schemes in Blockchain networks for healthcare system highlights many opportunities but many challenges as well. Blockchain integration will bring improved security, openness, and effectiveness for handling the primary medical data that is significant for modern medication digitalization. However, some challenges of adopting this technology include; Scalability due to consensus mechanisms, complex computation of algorithms when expanding the network, and mainly the necessity of maintaining privacy. Solving such problems necessitates radical solutions such as improved consensus to optimize bandwidth usage, new cryptography methods to enhance privacy-preserving mechanisms, and integration with the current healthcare systems. Furthermore, issues of patients' data ownership and consent demonstrate that the best ethical frameworks should put patient's self-determination and trust in focus. While researchers and practitioners strive to achieve these objectives, interdisciplinary cooperation will be critical to unlocking Blockchain's capability in reforming access control in healthcare, ultimately achieving safe and patient-centered services in the current technologically advanced world.

REFERENCES

[1]. Kumar, Randhir, and Rakesh Tripathi. "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model." Journal of Ambient Intelligence and Humanized Computing 12 (2021): 2321-2338.

[2]. Yang, Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, and Victor Chang. "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system." Information Sciences 479 (2019): 567-592.

[3]. Pal, Shantanu, Michael Hitchens, Vijay Varadharajan, and TahiryRabehaja. "Policy-based access control for constrained healthcare resources in the context of the Internet of Things." Journal of Network and Computer Applications 139 (2019): 57-74.

[4]. Yang, Yang, Ximeng Liu, and Robert H. Deng. "Lightweight break-glass access control system for healthcare Internet-of-Things." IEEE Transactions on Industrial Informatics 14, no. 8 (2017): 3610-3617.

[5]. Zhang, Wei, Yaping Lin, Jie Wu, and Ting Zhou. "Inference attack-resistant e-healthcare cloud system with fine-grained access control." IEEE Transactions on Services Computing 14, no. 1 (2018): 167-178.

[6]. Saini, Akanksha, Qingyi Zhu, Navneet Singh, Yong Xiang, Longxiang Gao, and Yushu Zhang. "A smart-contract-based access control framework for cloud smart healthcare system." IEEE Internet of Things Journal 8, no. 7 (2020): 5914-5925.

[7]. Sohal, Amandeep Singh, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang. "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." Computers & Security 74 (2018): 340-354.

[8]. Pournaghi, SeyedMorteza, Majid Bayat, and YaghoubFarjami. "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption." Journal of Ambient Intelligence and Humanized Computing 11, no. 11 (2020): 4613-4641.

[9]. Saidi, Hafida, Nabila Labraoui, Ado Adamou Abba Ari, Leandros A. Maglaras, and Joel HerveMboussamEmati. "DSMAC: Privacy-aware Decentralized Self-Management of data Access Control based on blockchain for health data." IEEE Access 10 (2022): 101011-101028.

[10]. Azbeg, Kebira, OuailOuchetto, and Said Jai Andaloussi. "Access control and privacy-preserving blockchain-based system for diseases management." IEEE Transactions on Computational Social Systems (2022).

[11]. Abdellatif, AlaaAwad, Abeer Z. Al-Marridi, Amr Mohamed, AimanErbad, Carla FabianaChiasserini, and Ahmed Refaey. "ssHealth: toward secure, blockchain-enabled healthcare systems." IEEE Network 34, no. 4 (2020): 312-319.

[12]. Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, AlirezaJolfaei, and AKM Najmul Islam. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." Journal of Parallel and Distributed Computing 172 (2023): 69-83.

[13]. Kumar, Randhir, Prabhat Kumar, Rakesh Tripathi, Govind P. Gupta, AKM Najmul Islam, and Mohammad Shorfuzzaman. "Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems." IEEE Transactions on Industrial Informatics 18, no. 11 (2022): 8065-8073.

[14]. Tanwar, Sudeep, Karan Parekh, and Richard Evans. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." Journal of Information Security and Applications 50 (2020): 102407.

[15]. Tripathi, Gautami, Mohd Abdul Ahad, and Sara Paiva. "S2HS-A blockchain based approach for smart healthcare system." In Healthcare, vol. 8, no. 1, p. 100391. Elsevier, 2020.

[16]. Singh, AkhilendraPratap, NiharRanjan Pradhan, Ashish K. Luhach, SivansuAgnihotri, Noor Zaman Jhanjhi, SahilVerma, Uttam Ghosh, and Diptendu Sinha Roy. "A novel patient-centric architectural framework for

blockchain-enabled healthcare applications." IEEE Transactions on Industrial Informatics 17, no. 8 (2020): 5779-5789.

[17]. Bataineh, Marah R., Wail Mardini, Yaser M. Khamayseh, and MuneerMasadehBaniYassein. "Novel and secure blockchain framework for health applications in IoT." IEEE Access 10 (2022): 14914-14926.

[18]. Rehman, Abdur, Sagheer Abbas, M. A. Khan, Taher M. Ghazal, Khan Muhammad Adnan, and Amir Mosavi. "A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique." Computers in Biology and Medicine 150 (2022): 106019.

[19]. Sammeta, Naresh, and LathaParthiban. "Hyperledgerblockchain enabled secure medical record management with deep learning-based diagnosis model." Complex & Intelligent Systems 8, no. 1 (2022): 625-640.

[20]. Wazid, Mohammad, Ashok Kumar Das, Sachin Shetty, and Minho Jo. "A tutorial and future research for building a blockchain-based secure communication scheme for internet of intelligent things." IEEE Access 8 (2020): 88700-88716.

[21]. Zarour, Mohammad, MdTarique Jamal Ansari, MamdouhAlenezi, Amal Krishna Sarkar, MohdFaizan, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records." IEEE Access 8 (2020): 157959-157973.

[22]. Veeramakali, T., Rathinavelayutham Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj. "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model." The Journal of Supercomputing 77, no. 9 (2021): 9576-9596.

[23]. Egala, Bhaskara S., Ashok K. Pradhan, VenkataramanaBadarla, and Saraju P. Mohanty. "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control." IEEE Internet of Things Journal 8, no. 14 (2021): 11717-11731.

[24]. Arul, Rajakumar, Yasser D. Al-Otaibi, Waleed S. Alnumay, Usman Tariq, Umar Shoaib, and MD JalilPiran. "Multi-modal secure healthcare data dissemination framework using blockchain in IoMT." Personal and Ubiquitous Computing (2021): 1-13.

[25]. Azbeg, Kebira, OuailOuchetto, and Said Jai Andaloussi. "BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security." Egyptian informatics journal 23, no. 2 (2022): 329-343.