Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 3
Open Access

Assessing the Security of Healthcare Information through Block-chain Solutions

Abhishek Sanjeev[1], Devraj Vishnu[2*], Ajay Kumar Phulre[3], Subhash Chandra Patel[4]

[1]School of Computer Science and Engineering, VIT Bhopal University, Sehore, Madhya Pradesh, 466114, India. Email: abhishek.sanjeev2020@vitbhopal.ac.in ORCiD: 0009-0004-2568-1583

[2] School of Computer Science and Engineering, VIT Bhopal University, Sehore, Madhya Pradesh, 466114, India. Email: devrajvishnu@vitbhopal.ac.in ORCiD: 0000-0002-3106-2939

[3]School of Computer Science and Engineering, VIT Bhopal University, Sehore, Madhya Pradesh, 466114, India. Email: ajaykumarphulre@vitbhopal.ac.in

[4] School of Computer Science and Engineering, VIT Bhopal University, Sehore, Madhya Pradesh, 466114, India. Email: subhash.patel@vitbhopal.ac.in

***Corresponding Author:**
Devraj Vishnu

School of Computer Science and Engineering, VIT Bhopal University,
Sehore, Madhya Pradesh, 466114, India
Email: devrajvishnu@vitbhopal.ac.in

Cite this paper as: Abhishek Sanjeev, Devraj Vishnu, Ajay Kumar Phulre, Subhash Chandra Patel (2024) Assessing the Security of Healthcare Information through Block-chain Solutions. *Frontiers in Health Informatics, 13* (3),7120-7131

Abstract-

Problem Statement-With the rise of Health 4.0, healthcare has experienced a digital transformation that enhances patient care but also increases risks to data security. Patient information is now more vulnerable to cyber threats, which can compromise privacy, impact treatment quality, and lead to significant financial and reputational losses for healthcare providers.

Objective- This study aims to evaluate the application of blockchain technology as a solution to these data security challenges, specifically in the areas of patient data privacy, secure data sharing, and interoperability across healthcare systems.

Methodology-The approach was a qualitative case study of blockchain technology deployment in healthcare data security during COVID-19 pandemic. Through real world applications it studies blockchain's potential and its capabilities and limitations in healthcare contexts.

Findings-The analysis shows that blockchain provides substantial improvements over current methods of securing healthcare data such as better data integrity, limiting unauthorized access, and better traceability in drug supply chain. Scalability and regulatory compliance are still the challenge, which is not allowing widespread adoption of blockchain solutions in healthcare.

Implications- As the first contribution, this study outlines a framework for blockchain implementation in healthcare, and highlights that technical and regulatory barriers must be overcome. The insights gained here provide a basis for further research, and suggest that healthcare organizations may select blockchain as a realistic option for protecting patient data.

Keywords- Blockchain in Healthcare, Data Security, Patient Data Privacy, Healthcare Interoperability, COVID-19 Case Study

I. INTRODUCTION

With the vulnerability of healthcare information to cybercriminals more than ever, and the latter now targeting patient data more frequently than ever, also protecting your data is more crucial than ever. Keeping this information secure, finding it complete, and making it available at the right time is vital to maintaining patient trust and a well running healthcare system. Major consequences brought by data breaches and unauthorised access include identity theft, financial loss, and interruption of patient treatment. In addition, the healthcare industry is subject to a very strict regulatory framework, for instance, HIPAA, in the United States, which imposes severe data protection rules. By definition, securing healthcare information is important (or even crucial) not only for regulatory reasons, but because it's a key component of patient safety and in building a health system we can trust.

As healthcare records continue to be digitized and telemedicine and mobile health apps grow, the case for more security only becomes more urgent. Getting healthcare information is clearly not as simple as checking off regulatory requirements but also involves matters pertaining to the quality of patient care and the efficiency of the provision of healthcare services. Take for example, disclosure of patient data, it results in wrong treatments, wrong diagnosis and other serious problems that could impact patient health. Also, data breaches can cause large monetary losses and kill a healthcare provider's reputation due to loss of patients trust which will also hinder the acceptance of cutting edge technologies.

With patient data sensitive, today's digital age requires healthcare information security as fraudsters target patient data regularly. Maintaining patient's trust and flow of healthcare services depends on healthcare information confidentiality, integrity and availability. The consequences of data breaches and unauthorised access can be very serious, including identity theft and financial loss, and compromised patient care. Besides, the healthcare industry is under strict legal bondage (such as HIPAA in the US) to maintain a high level of data privacy. Protecting healthcare information is not only a regulatory duty, it is key to safe care, and to the assurance of secure care, upon which patients trust in a safe system is built [1].

It only becomes more important as telemedicine proliferates and more and more telemedicine and mobile health applications are consumed, and as such, the digitization of healthcare increasingly demands strong security measures to protect patient data from breaches and unauthorized access. Making sure healthcare information is secured is no longer just for the sake of keeping up with industry mandated regulations it is also about providing high quality of patient care and timely exchange of healthcare information. For example, compromised patient data can be used to administer incorrect medical treatments, delay diagnosis, or result in some other adverse outcome to the detriment of the patient's health. Additionally, continuing trend of financial and reputation damage mandates healthcare providers when breaches occur, while challenging patient's trust with their provider, which stands in the way of new technology adoption [2].

The purpose of this research is to determine the potential of Blockchain technology to eliminate data security breaches in the healthcare sector and to ensure that medical records are secure and reliable. Additionally, the research aims to evaluate how Blockchain enhances the security of drug supply chains and to identify the technical, regulatory, and operational challenges associated with implementing Blockchain solutions in healthcare.

Interoperability and data sharing, which are the main barriers faced in healthcare information security enable a secure exchange of patient data across different health systems or providers. Coordination of care - Part of providing effective, high-quality patient care involves ensuring that systems can interact with and share data between them. The challenge is achieving interoperability although still maintaining the security and privacy of data. Hannah et al. (2022) also reveals that deep learning service based on blockchain for IoT-enabled healthcare showed how the interoperability and secure data sharing were facilitated via a single, unified framework providing true potential of expanding use cases for prediction identifying demand load. Absence of standardized protocols & framework for data sharing and Lack of standardization adds complexities in making different system compatible with each other.

The most common challenge faced by healthcare organizations is the poor integration of their systems with one another, which results in fragmented and isolated pools of data that can impact both patient care and operational efficiency. According to Abbas et al. (2020), the authors argue blockchain technology can alleviate such concerns by providing a decentralized and secure data transmission platform based on which all parties concerned have access to up-to-date, accurate information. By being transparent and open source, Blockchain technology can be used to solve this interoperability issue by offering a secure means to share patient data between healthcare institutions on an immutable ledger.

TABLE II. **CHALLENGES IN HEALTHCARE INFORMATION SECURITY**

Challenge	**Description**	**Impact**
Data Breaches and Cyber Threats	Increasing incidents of unauthorized access to patient records and confidential data due to cyber attacks.	Threats to patient privacy, data integrity, and healthcare system security.
Regulatory and Compliance Issues	Complex regulatory landscape (e.g., HIPAA, GDPR) requiring healthcare organizations to implement strict security measures.	Resource-intensive compliance, risk of non-compliance penalties.
Interoperability and Data Sharing	Challenges in securely sharing patient information across different healthcare systems while ensuring data privacy and security.	Fragmented data, hindrance to coordinated patient care.

TABLE III. **SOLUTIONS AND TECHNIQUES FOR ENHANCING HEALTHCARE INFORMATION SECURITY**

Solution/Technology	**Description**	**References**
Blockchain Technology	A decentralized platform that enhances data integrity, security, and transparency for healthcare information systems.	Abbas et al. (2020), Bhattacharya et al. (2019)
Deep Learning and AI	Advanced technologies that can bolster security measures and compliance, particularly through homomorphic encryption and secure data analysis.	Ali et al. (2022), Gul et al. (2020)
Secure Data Exchange	Blockchain can facilitate secure data sharing and	Hannah et al. (2022),

Framework	interoperability, allowing disparate systems to communicate efficiently.	Abbas et al. (2020)

TABLE IIII. **KEY REGULATORY FRAMEWORKS IMPACTING HEALTHCARE INFORMATION SECURITY**

Regulation	**Region**	**Key Focus**	**Compliance Requirements**
Health Insurance Portability and Accountability Act (HIPAA)	United States	Protecting patient privacy and ensuring secure handling of healthcare information.	Implement security measures, conduct audits.
General Data Protection Regulation (GDPR)	European Union	Protecting personal data and privacy of EU citizens.	Data protection impact assessments, clear consent mechanisms.

II. BLOCKCHAIN IN HEALTHCARE

As shown in the above Fig. 1, all the data which is available at server which further transfers using the transaction and each node involves in the transaction is known as block. With each new block verification is perform which means each node checks for the previous hash values and verifies the content of the block. After verifying the block, new block creates its own hash value and transfer to the next block for the execution.

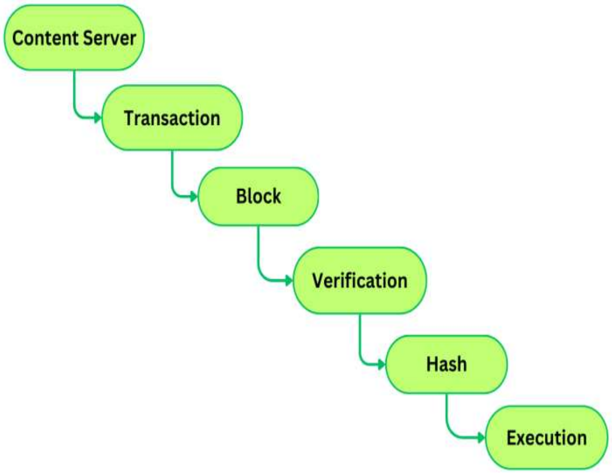

Fig. 1. Working steps of Blockchain

Each transaction (e.g., medical records) is stored in an immutable block. Altering a block would require changing all subsequent blocks, which is computationally infeasible. As well as data is not stored in a single central database, reducing the risk of large-scale data breaches. For passing data from one block to another block/new block index of new block, timestamp, transaction, proof and previous hash details are also sored which make it nearest to impossible for any data breaches.

As the Blockchain technology can provides a decentralized and immutable ledger, which significantly enhances data security by preventing unauthorized access and tampering. By storing data in a distributed manner, blockchain reduces the risk of single points of failure, making data breaches less likely [1, 2].

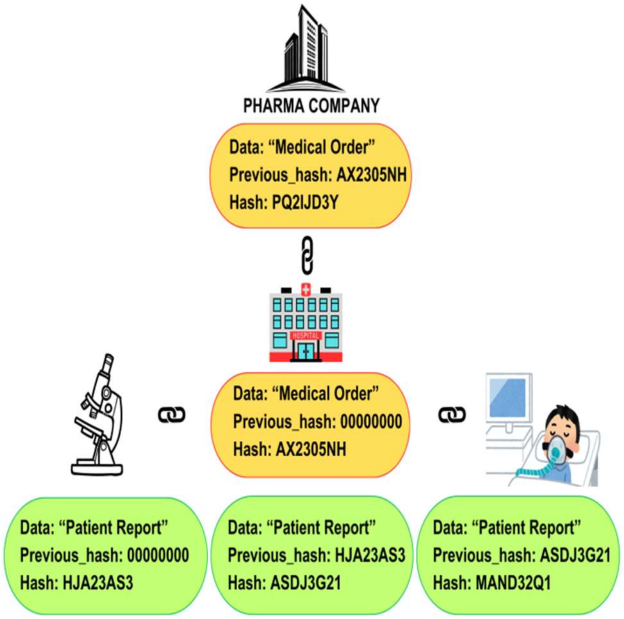

Fig 2. Illustration of how block-chain and hash value works

A. Data Integrity and Transparency

All transactions are visible on the blockchain, providing a transparent history of medical records. The hash of each blocks ensuring that data cannot be tampered with. Any changes in blocks would be immediately apparent. To maintain integrity in the data, block chain use hash code for each block and data. If any alteration in data is occurred by any node, then it becomes easy to identify that data has been changed during the transfer from the hash value. It is almost impossible for anyone to regenerate or identify the logic behind the hash values which is automatically created by blocks. This hash value provides integrity and transparency of records as it stores the previous hash values. This hash value looks like following record.

"previous_hash": "5b60c8344d7e8e7e20c6dfbae8ff88fda62f9397a5b54fd848a5400b8fddc57d"

Blockchain ensures data integrity through its immutability feature. Once data is added to the blockchain, it cannot be changed without modifying all subsequent blocks, which requires agreement from the network. This ensures that medical records remain accurate and unaltered, providing a transparent and trustworthy history of patient data [3, 4].

B. Security Of Drug Supply Chains

Each transaction in the supply chain, such as drug shipments, is documented, creating a clear and traceable path from the manufacturer to the distributor. By monitoring the origin and movement of drugs through the blockchain, it becomes challenging for counterfeit products to infiltrate the supply chain without being noticed. In the blockchain, each record is typically formatted as JSON data.

As shown in the above data, each record contains all the necessary data including timestamp and hash which protects data and to improves the security of the data. Enhancing security in the drug supply chain is possible by utilizing the blockchain to provide transparent and tamper proof records of an entire supply chain. This can be used to trace the route of drugs from the manufacturer to the end consumers, limits the chances that parallel or unapproved pharmaceutical products can end up in the supply chain, and verify with certainty the duplication of pharmaceutical products [5, 6].

C. Technological and Regulatory Challenges

To integrate blockchain with healthcare systems, there will need to be a compliance with regulations such as HIPAA. While blockchain can be implemented in existing healthcare systems, there are integration challenges, training healthcare professionals and ensuring user adoption, which can be further explored through extended simulation and real world testing. To implement blockchain in healthcare, there are technical, regulatory and operational challenges to overcome. Scalability and interoperability challenges are technical challenges. Regulatory challenges include ensuring that healthcare regulations like HIPAA.

III. LITERATURE REVIEW

Interoperability and data sharing constitute the two main challenges of healthcare information security in the area of communicating smooth patient information exchange among various healthcare systems and providers. To coordinate and provide effective patient care, you need to make sure disparate systems can safely exchange data among themselves. The biggest obstacle to interoperability, though, is doing it in a way that's secure for data privacy and data security.

Hannah et al. (2022), utilized blockchain based deep learning in which blockchain is used to facilitate secure data sharing and interoperability through a unified and secure data exchange framework. The lack of standardized protocols or frameworks for sharing data makes interoperability efforts difficult. But healthcare organizations are often faced with the challenge of bringing systems together to use the data more effectively, leaving them with disconnected, siloed data that can have a negative impact on patient care and business operations.

Abbas et al. (2020), using blockchain technology, which ensures all parties have access to the most up to date and correct information through a decentralised and secure data transmission platform. Blockchain solutions may improve interoperability by setting up a transparent and immutable goods ledger, which will allow secure data sharing and supply better healthcare services quality.

The researchers, including Hu et al. (2023) and the researchers propose an intelligent system that integrates blockchain, IoT and machine learning to enhance vaccine supply chain management. The problem of tracking and authentication in vaccine distribution is tackled, especially during public health emergencies, using this approach. The system optimizes distribution routes and predicts demand through the use of machine learning, while using blockchain for secure data storage and IoT devices for real time monitoring. This complete solution seeks to improve vaccine accessibility and supply chain management efficiency.

Imran et al. (2021) study the combined capability of IoT, machine learning and Blockchain technologies in healthcare applications, for example in pandemic preparedness. Healthcare systems are shown to face challenges including data silos and inefficient communication, which the authors specify. Through the integration of these technologies, data sharing is improved, decision making is enhanced, and real time monitoring of health indicators are realized. Importantly, this requires an interdisciplinary approach towards building resilient healthcare infrastructures capable of responding to future health crises.

Kumar et al. (2023) introduce a blockchain based deep learning architecture to ensure safe data transmission in IoT enabled healthcare systems, while highlighting the need for data protection in environments that produce and share patient data on an ongoing basis..

Mantey et al. (2022) looks at the application of blockchain and deep learning in a recommender system that works with electronic health records (EHRs). EHRs are full of sensitive data and protecting it is of paramount importance, say the authors. Protecting data is done using blockchain, and insights from EHRs are mined using deep learning algorithms. It provides a better handle to clinical decisions with more informed clinical decisions and better patient care.

Senthilmurugan and Chinnaiyan (2021) developed a peer to peer platform using IoT and machine learning to monitor crop growth and crop diseases and using blockchain to store data securely. The authors explain that traditional agricultural practices are inefficient because they are not transparent, they do not offer real time data access, and crop management is not possible. They run machine learning algorithms on environmental conditions to predict crop diseases, and help farmers share secure agricultural data on their platform. This can however be a great step in improving agricultural productivity and sustainability.

Shafay et al. (2023) investigate how blockchain technology can be integrated with deep learning in various sectors including healthcare. The authors highlight the challenges of scalability, interoperability and efficient consensus mechanisms. The combination of these technologies has the potential to greatly improve data security and privacy, but only if several hurdles can be overcome. This review will help direct future research into bridging the gap between blockchain applications and deep learning applications.

Li et al. (2023), hybrid framework to enable secure sharing of healthcare data through blockchain and machine learning technologies is presented by Li et al. (2023). Still, the authors argue that data sharing is essential to improving patient care and outcomes, but current systems are often not secure enough. They use blockchain to secure data transactions and use machine learning algorithms to analyze shared data to derive actionable insights. It not only improves data security, but also facilitates collaboration among healthcare providers, which ultimately benefits patient care.

IV. CASE STUDIES AND REAL WORLD APPLICATIONS

This paper describes how blockchain has been successfully deployed in healthcare, and what lessons can be learned for future deployments. One such successful story is Blockchain for secure data transmission in IoT enabled healthcare system. According to Kumar et al (2023), their deep learning approach, backed by blockchain, is efficient in keeping the transmission of the data safe and secure as the high level encryption and decentralized control can help trace and resolve security problems. This case study highlights the role of blockchain in protecting sensitive health data in an emerging connected healthcare environment.

Blockchain with AI has been useful to integrate in patient recommender systems. A blockchain secured recommender system is developed by Mantey et al. (2021) for patients with special needs and has shown improvement in the delivery of personalized care. We learned from this implementation that we require interoperability of blockchain with existing healthcare technologies and user friendly interfaces to encourage the adoption of blockchain by healthcare professionals and patients.

A. Comparative Analysis of Different Blockchain Solutions:

Different approaches and the results of different blockchain solutions in healthcare are presented in a comparative study. For instance, Li et al. (2021) do a bibliometric study of the applications of machine learning and blockchain in the smart healthcare industry. Results from this project indicate that blockchain solutions are adopted and deployed at different levels to address critical healthcare problems and that scalability, integration complexity and user acceptance are all factors in developing effective blockchain solutions.

The other comparison is between blockchain based vaccine supply systems and general health data management systems in general. Yong et al. (2020) create an intelligent, blockchain based system for safe vaccine supply and supervision, which is traceable and transparent for the process of vaccine distribution. This solution is unique compared to other health data management systems that aim to secure patient records and facilitate easier information transfer. Comparative analyses of similar nature permit the identification of the strengths along with weaknesses of assorted blockchain implementations, and moreover, they actually make it possible to direct next intended improvement and deployment strategies.

TABLE IIV. **BLOCKCHAIN IMPLEMENTATIONS IN HEALTHCARE**

Study	**Implementation**	**Key Findings**
Mantey et al. (2022)	Integration of blockchain with deep learning	Improved security and efficiency in managing electronic health records
Singh et al. (2022)	Federated Learning and blockchain framework	Enhanced privacy preservation for IoT healthcare data
Kumar et al. (2023)	Secure data transmission in IoT-enabled healthcare	Effective mitigation of security risks through robust encryption and decentralized control
Mantey et al. (2021)	Blockchain-secured recommender system	Significant improvements in personalized care delivery
Li et al. (2021)	Bibliometric analysis of ML and blockchain	Varied adoption and effectiveness across different healthcare settings
Yong et al. (2020)	Blockchain-based vaccine supply system	Ensured transparency and traceability in vaccine distribution

TABLE IV. **SECURITY AND PERFORMANCE EVALUATION METRICES**

Metric	**Description**	**Example Studies**
Transaction Validation Time	Time taken to validate a transaction	Bhattacharya et al. (2019)
Network Resilience	Ability to withstand attacks	Shafay et al. (2023)
Cryptographic Protocols	Effectiveness of encryption methods	Ali et al. (2022)
Computational Efficiency	Efficiency in data retrieval and analysis	Ali et al. (2022)

Scalability Techniques	Methods to handle large data volumes	Shafay et al. (2023)

TABLE IVI. EVALUATION OF BLOCKCHAIN

It provides a structured approach that includes comprehensive tables to support discussions and citations relevant to implementing and evaluating blockchain in healthcare with a detailed analysis.

Criteria	**Proposed Blockchain Model**	**Traditional Centralized System**	**Existing Blockchain Models**
Data Security	High (Decentralized, Immutable)	Low (Single Point of Failure)	High
Data Integrity	High (Tamper-proof, Transparent)	Medium (Prone to Unauthorized Changes)	High
Transparency	High (All Transactions are Public)	Low (Limited Access)	High
Scalability	Medium (Depends on Blockchain Type)	High (Centralized Control)	Medium (Same as Proposed Model)
Interoperability	High (Standard Protocols)	Low (Proprietary Systems)	Medium
Compliance with Regulations	High (Compliant with Data Privacy Laws)	Medium (Depends on Implementation)	Medium
Operational Efficiency	Medium (Requires Consensus)	High (Central Control, Fast Transactions)	Medium (Similar Challenges)
Traceability of Medical Records	High (Full History Available)	Low (Records can be Altered)	High
Supply Chain Security	High (End-to-End Tracking)	Low (Prone to Counterfeits)	High
Implementation Challenges	Medium (Technical and Regulatory Hurdles)	Low (Established Systems)	Medium

V. CONCLUSION AND FUTURE WORK

In summary, incorporating blockchain technology into the health care ecosystem enables potential use as a means to improve data security in the evolving Health 4.0 environment. With the healthcare field adapting to advanced technologies, the volume and sensitivity of data is likely to increase significantly, which makes strong security incredibly important. In this study we highlight the important role blockchain can play in solving problems with data protection, privacy and verification of access. We can then analyze the key factors such as data types, access timing and security methods to understand how blockchain can be used to increase healthcare data security.

A case study of blockchain use in the COVID-19 pandemic shows how blockchain can secure health information and facilitate collaboration among different stakeholders. But enacting blockchain has plenty of challenges, such as technological limitations and regulatory hurdles. Future research should focus on the creation of strategies to overcome these challenges, innovative ways to incorporate blockchain into current systems, and the long term effects of blockchain on healthcare data security. Through blockchain in healthcare, we can advance our knowledge and application of blockchain in a way that can help us build a safer and more secure future for managing patient information.

For this experimental model, we used the built in modules of Python to make blocks and to do the hashing. In the future we will use custom hashing algorithm to increase security. Medical parcels could be barcoded or QR coded for fast processing if more hardware was available.

AUTHOR'S CONTRIBUTION

All authors contributed to the literature review, design, data collection and analysis, drafting the manuscript, read and approved the final manuscript.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest regarding the publication of this study.

FINANCIAL DISCLOSURE

No financial interests related to the material of this manuscript have been declared.

REFERENCES

[1] H. P. A, M. Senthilmurugan, P. R. K and R. Chinnaiyan, "IoT and Machine Learning based Peer to Peer Platform for Crop Growth and Disease Monitoring System using Blockchain," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 2021.

[2] K. Abbas, M. Afaq, T. Ahmed Khan and W.-C. Song, "A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry," *Electronics,* vol. 9, p. 852, May 2020.

[3] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham and M. Omar, "The role of blockchain technology in telehealth and telemedicine," *International Journal of Medical Informatics,* vol. 148, p. 104399, April 2021.

[4] A. Ali, M. F. Pasha, J. Ali, O. H. Fang, M. Masud, A. D. Jurcut and M. A. Alzain, "Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography," *Sensors,* vol. 22, p. 528, January 2022.

[5] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi and N. Kumar, "BinDaaS: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications," *IEEE Transactions on Network Science and Engineering,* vol. 8, p. 1242–1255, April 2021.

[6] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *Journal of Medical Systems,* vol. 42, p. 136, August 2018.

[7] A. Ghadge, M. Bourlakis, S. Kamble and S. Seuring, "Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework," *International Journal of Production Research,* vol. 61, p. 6633–6651, October 2023.

[8] M. J. J. Gul, A. Paul, S. Rho and M. Kim, "Blockchain based healthcare system with Artificial Intelligence," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2020.

[9] S. Hannah, A. J. Deepa, V. S. Chooralil, S. BrillySangeetha, N. Yuvaraj, R. Arshath Raja, C. Suresh, R. Vignesh, YasirAbdullahR, K. Srihari and A. Alene, "Blockchain-Based Deep Learning to Process IoT Data Acquisition in Cognitive Data," *BioMed Research International,* vol. 2022, p. 1–7, February 2022.

[10] H. Hasanova, M. Tufail, U.-J. Baek, J.-T. Park and M.-S. Kim, "A novel blockchain-enabled heart disease prediction mechanism using machine learning," *Computers and Electrical Engineering,* vol. 101, p. 108086, July 2022.

[11] H. Hu, J. Xu, M. Liu and M. K. Lim, "Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning," *Journal of Business Research,* vol. 156, p. 113480, February 2023.

[12] M. Imran, U. Zaman, Imran, J. Imtiaz, M. Fayaz and J. Gwak, "Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions," *Electronics,* vol. 10, p. 2501, October 2021.

[13] W. Javed, F. Aabid, M. Danish, H. Tahir and R. Zainab, "Role of Blockchain Technology in Healthcare: A Systematic Review," in *2021 International Conference on Innovative Computing (ICIC)*, Lahore, 2021.

[14] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei and A. K. M. Najmul Islam, "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system," *Journal of Parallel and Distributed Computing,* vol. 172, p. 69–83, February 2023.

[15] Y. Li, B. Shan, B. Li, X. Liu and Y. Pu, "Literature Review on the Applications of Machine Learning and Blockchain Technology in Smart Healthcare Industry: A Bibliometric Analysis," *Journal of Healthcare Engineering,* vol. 2021, p. 1–11, August 2021.

[16] E. A. Mantey, C. Zhou, J. H. Anajemba, I. M. Okpalaoguchi and O. D.-M. Chiadika, "Blockchain-Secured Recommender System for Special Need Patients Using Deep Learning," *Frontiers in Public Health,* vol. 9, p. 737269, September 2021.

[17] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain and B. Sundaravadivazhagan, "Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System," *Frontiers in Public Health,* vol. 10, p. 905265, May 2022.

[18] A. H. Mayer, C. A. Da Costa and R. D. R. Righi, "Electronic health records in a Blockchain: A systematic review," *Health Informatics Journal,* vol. 26, p. 1273–1288, June 2020.

[19] K. J. Peterson, R. Deeduvanu, P. Kanjamala and K. Mayo, "A Blockchain-Based Approach to Health Information Exchange Networks," 2016.

[20] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, W. A. Bukhari and M. I. A. Khan, "Blockchain technology in healthcare: A systematic review," *PLOS ONE,* vol. 17, p. e0266462, April 2022.

[21] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, W. A. Bukhari and M. I. A. Khan, "Blockchain technology in healthcare: A systematic review," *PLOS ONE,* vol. 17, p. e0266462, April 2022.

[22] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Computing,* vol. 26, p. 197–221, February 2023.

[23] S. Singh, S. Rathore, O. Alfarraj, A. Tolba and B. Yoon, "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology," *Future Generation Computer Systems,* vol. 129, p. 380–388, April 2022.

[24] S. Soner, R. Litoriya and P. Pandey, "Combining blockchain and machine learning in healthcare and health informatics: An exploratory study," in *Blockchain Applications for Healthcare Informatics*, Elsevier, 2022, p. 117–135.

[25] S. Vyas, M. Shabaz, P. Pandit, L. R. Parvathy and I. Ofori, "Integration of Artificial Intelligence and Blockchain Technology in Healthcare and Agriculture," *Journal of Food Quality,* vol. 2022, p. 1–11, May 2022.

[26] B. Yong, J. Shen, X. Liu, F. Li, H. Chen and Q. Zhou, "An intelligent blockchain-based system for safe vaccine supply and supervision," *International Journal of Information Management,* vol. 52, p. 102024, June 2020.

[27] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu and J. J. P. C. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," *Future Generation Computer Systems,* vol. 130, p. 140–154, May 2022.