Grenze International Journal of Engineering and Technology, January Issue

Secure Healthcare Data Systems with Blockchain

Deepika Walanjkar[1], Kalash Malage[2], Sujal Jagtap[3], Amit Laware[4] and Yash Kabade[5]
[1]Assistant Professor, International Institute of Information Technology, Pune, India
Email: deepikaw@isquareit.edu.in
[2-5]BE Student, IT department, International Institute of Information Technology, Pune, India
Email: kalashm_t22075@students.isquareit.edu.in, sujalj_t22034@students.isquareit.edu.in,
amitl_t22015@students.isquareit.edu.in, yashk_t22152@students.isquareit.edu.in

***Abstract*— The digitization of the healthcare sector has led to the widespread use of Electronic Health Records (EHRs), which have the potential to transform patient care and advance medicine. However, traditional centralized EHRs face challenges such as data security, confidentiality, patient empowerment, and interoperability. This literature review explores the use of blockchain technology as a decentralized approach to address these issues. Key characteristics of blockchain include immutability, transparency, and cryptographic security. The review also explores patient-centric models, data integrity preservation strategies, and interoperability improvements.**

I. Introduction

A. Importance of Electronic Health Records (EHRs)

In the digital age, EHRs have become pivotal for healthcare, transforming practices into information-based approaches [2], [20]. EHRs store essential medical information such as health history, diagnoses, medications, allergies, and treatment plans [27]. They enhance patient care quality and decrease operational costs, providing detailed patient histories that facilitate accurate disease exploration, qualitative diagnoses, and informed clinical decisions [28]. The effectiveness of EHR sharing is crucial for expediting care delivery, especially within multi-provider healthcare systems [21].

B. Challenges in Current EHR Systems

Despite their potential, traditional centralized EHR systems face significant challenges [10], [21]. One major issue is data silification, where patient histories are fragmented across various health organizations' databases, leading to communication bottlenecks, unnecessary data exchanges, and treatment delays [5]. Security concerns arise as centralized databases are prime targets for cyberattacks and breaches, risking patient confidentiality and trust [7], [8]. Current frameworks struggle with patient-centric management and limit patients' control over their health information, hampering safe data exchange [9], [25].

C. The Role of Decentralized Technologies

To counter the drawbacks of centralized models, researchers are exploring decentralized technologies, particularly blockchain [10], [13], [21]. Blockchain offers a distributed and immutable ledger ideal for secure medical data management and sharing [19], [25]. Its decentralization, data immutability, traceability, and transparency foster a trustworthy environment for data sharing among healthcare members [35].

Grenze ID: 01.GIJET.12.1.319_1

By removing single points of control, blockchain mitigates risks of data tampering and privacy breaches while enhancing interoperability andempowering patients over their medical information, thereby reimagining healthcare data management [37], [46].

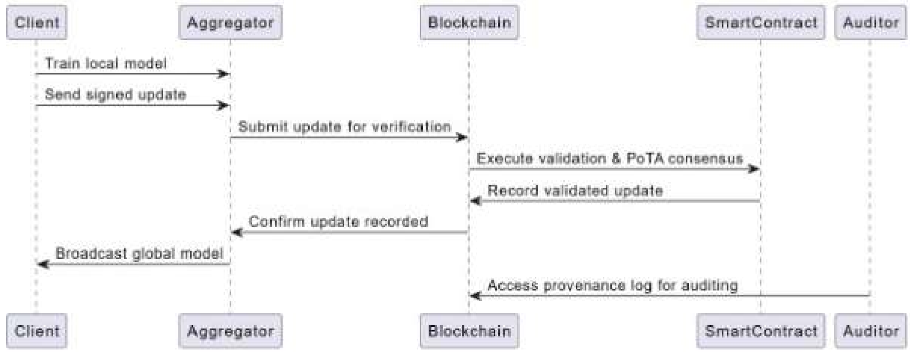


Fig 1. Sequence Diagram

II. BLOCKCHAIN THEORY OF HEALTHCARE FOUNDATIONS

Blockchain technology is a decentralized, peer-to-peer database system that effectively holds a continuously increasing list of transactions in a ledger format [10], [13]. Each block within the blockchain is cryptographically connected to its prior block, ensuring data integrity since transactions, once recorded, cannot be altered or deleted without consensus [19], [42]. Blockchains can be categorized into public, private, and consortium types, with consortium chains being particularly suited for the healthcare sector due to their controlled access and high transaction throughput[11],[25].

In healthcare, key blockchain features address various challenges. Decentralization allows data distribution across different nodes, reducing failure points and enhancing system resilience [31]. The unalterable ledger structure ensures permanence and authenticity of medical records through verifiable timelines or data provenance, which is crucial for medical documentation integrity [22], [24]. Smart contracts automate agreements and policies within the healthcare system, facilitating secure interactions between patients and medical institutions while minimizing administrative burdens [46], [47].

In contrast to traditional centralized electronic health record (EHR) systems that create data silos and interoperability issues, blockchain systems decentralize data control among network participants, fostering a patient-centric model driven by collective trust rather than a single authority [21], [25]. This allows for secure and real-time sharing of data among authorized institutions, promoting collaboration and streamlining healthcare operations [37].

III. PATIENT-CENTRIC MODEL SYSTEMS FOR EHR MANAGEMENT

A. Definition and Importance of Patient-Centric Approaches

Patient-centric healthcare prioritizes the individual, granting them control over their healthcare information, which is crucial for establishing trust between patients and providers [9], [25]. It encourages patients to manage, monitor, and securely share their information, leading to a more integrated and personalized healthcare model [21], [37]. Such approaches are driven by patients' desires for increased involvement in their healthcare management and clinical research participation, as well as potential financial gains from data usage [35].

B. Existing Models and Case Studies of Implementations

Notable work in this field includes MedRec, a decentralized record management system from MIT that employs Ethereum-based blockchain technology for interoperability and data permission management [46]. This system showcased the use of smart contracts for access control and provided an auditable log of data interactions [43]. Recent advancements, such as the framework by Sun et al., implement a blockchain system with provenance awareness, meticulously tracking medical records through a Directed Acyclic Graph (DAG) structure [22], [24]. This framework offers dynamic access control based on data provenance, thereby enhancing efficiency and security through a three-layer architecture focused on data collection, authorization, and auditing, ensuring transparency and accountability [25], [48].

IV. Data Integrity and Healthcare Privacy

Blockchain technology ensures data integrity by guaranteeing that once information is written, it cannot be altered, corrupted, or deleted unnoticed [10], [19]. This is achieved through mechanisms such as crypto-hashing, where each transaction is hashed and grouped into blocks, with each new block containing the hash of the previous one [42]. This creates a secure, chronological chain; any alteration in past transactions changes their hashes, invalidating subsequent blocks and exposing tampering to the entire network [13], [31]. This property of immutability is vital in healthcare, especially for safeguarding patient information and audit trails for regulatory compliance [35], [37].

While blockchain enhances data integrity, storing sensitive Electronic Health Records (EHRs) directly on-chain poses significant privacy risks due to the ledger's replication among participants [44]. To address this, off-chain storage solutions are used, where actual EHR files are securely stored in encrypted form on decentralized systems like IPFS, while only the encrypted file's unique hash is recorded on the blockchain [22], [25]. This maintains data integrity while keeping sensitive information off the ledger [48]. Advanced cryptographic methods further enhance confidentiality, including encryption using the patient's public key, allowing only the patient to decrypt the data [24]. Techniques such as Proxy Re-encryption facilitate secure data exchange with healthcare professionals without disclosing the patient's private key [44], and zero-knowledge proofs enable validation of data characteristics without exposing the data itself, thereby augmenting confidentiality protections [5], [48].

TABLE I

System Focus	Primary Security Technology	Key Mechanism	Privacy Goal
Federated Learning	PQC (Dilithium, Falcon), ECDSA	Signature Verification (On-chain PQC check)	Prevent quantum attacks; verify model update origin.
Provenance / EHR Sharing	Proxy Re-encryption (NuCypher), Asymmetric Encryption (RSA, EC-DSA)	Provenance DAG for dynamic access; Key Agreement (KA) protocol for secure credential exchange.	Patient control over EHR access; secure off-chain data retrieval.
System Integrity	Smart Contracts, Consensus (PoTA, PoA)	Nash Equilibrium Auditing; Verification Condition for detecting malicious updates.	Ensure auditor honesty; protect the global model from poisoning attacks.
Data Synchronization	Write Ahead Log (WAL) via Blockchain	Timely data synchronization to prevent query inconsistency in off-site insurance.	Ensure data consistency and availability across regional databases.

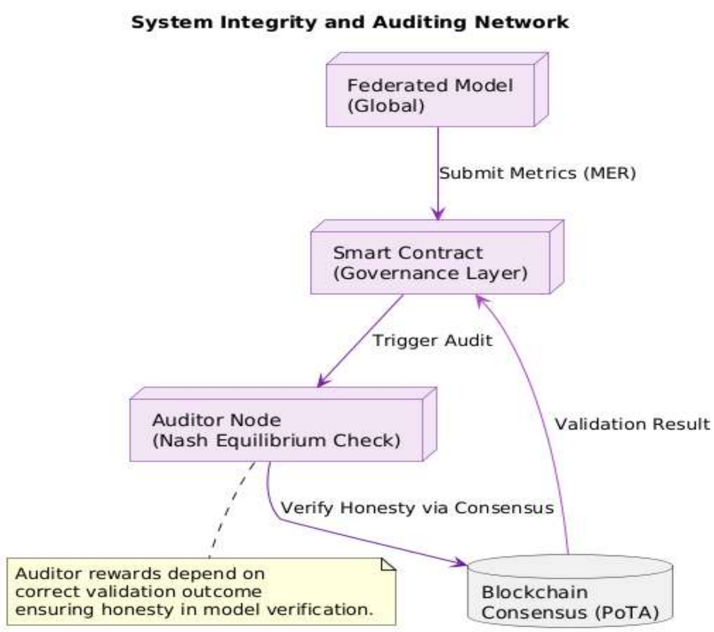


Fig 2. System Integrity and Auditing Network.

V. INTEROPERABILITY CHALLENGES AND SOLUTIONS.

A. Existing Status of Interoperability within EHR Systems

This section highlights the challenges of data exchange within healthcare due to the proprietary nature of systems like Epic and Cerner, as well as a lack of standardization, which results in low interoperability among institutions [2], [20]. This fragmentation hampers collaborative care and presents significant obstacles to achieving effective interoperability, despite the introduction of government-mandated standards such as Fast Healthcare Interoperability Resources (FHIR) [5], [27].

B. How Blockchain Enhances Interoperability

Reference [10] explains how blockchain technology can overcome these interoperability issues by providing a secure and universal infrastructure for data exchange. It serves as a trusted shared ledger that allows different systems to connect and share data without requiring direct integration of proprietary databases [21], [25]. By utilizing pointers to off-chain data and managing access through smart contracts, blockchain enables an auditable and standardized approach to health data exchange [37], [43]. This helps to dismantle data silos and allows healthcare practitioners to access patient records securely with the patient's consent [46], [47].

VI. FUTURE DIRECTIONS AND RECENT ADVANCES

Innovations in the healthcare sector are increasingly integrating Blockchain technology with Federated Learning (FL) to enhance data security and confidentiality [1], [6], [40]. This approach enables collaborative development of AI models across multiple healthcare parties without sharing raw patient data; hospitals train models locally and share only anonymized updates [22], [24]. Blockchain serves as a transparent ledger that records these updates, bolstering trust and auditability in the process [10], [25]. The Federated Averaging algorithm, which computes global model parameters based on local model updates weighted by dataset size, plays a crucial role in this collaborative learning framework[40]. Two emerging trends are anticipated to influence secure healthcare systems. The first is the shift towards Post-Quantum Cryptography (PQC) to protect healthcare data against future quantum computing threats [17]. Current cryptographic methods like ECDSA are at risk, making a transition to quantum-resistant algorithms, such as ML-DSA-65, essential for long-term data security within blockchain healthcare systems [10], [13], [17].

VII. UNRESOLVED QUESTIONS AND CHALLENGES

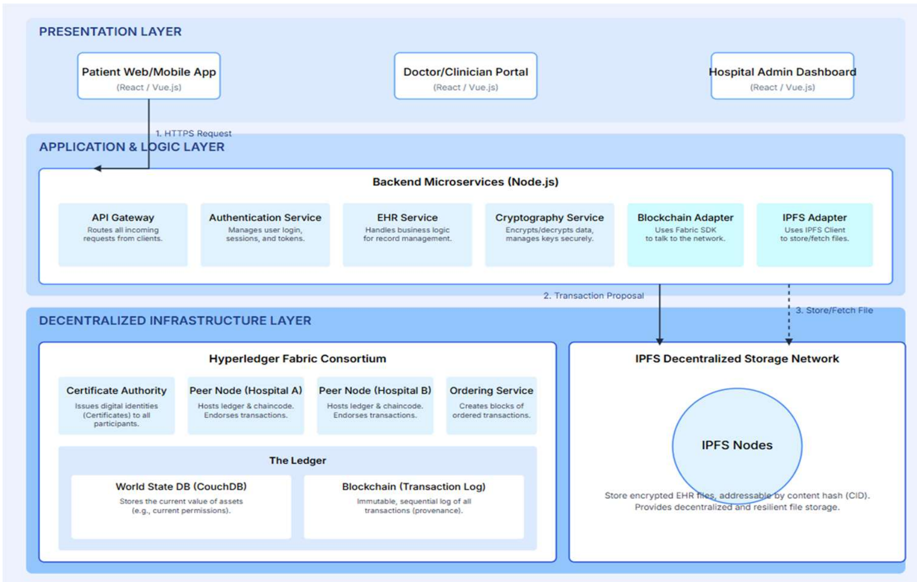
Despite significant progress, several challenges in blockchain technology for healthcare remain [10], [35]. Scalability issues arise as the user base and transactions increase, leading to high costs and processing delays, particularly with complex smart contracts [13], [42]. The absence of standardization poses another barrier, necessitating certified compliance with international data formats and security protocols to ensure interoperability [11], [31], [37]. Additionally, non-technical factors like organizational culture and risk management in healthcare institutions are crucial for technology adoption, as skepticism and misconceptions [4], [36].

Future research should prioritize enhancing the efficiency and scalability of blockchain systems tailored to healthcare, including the optimization of consensus algorithms and hybrid models that combine on-chain and off-chain processing [10], [13], [37]. The integration of advanced AI tools for better analytics while ensuring privacy protection is noted as a promising direction [1], [6], [40]. Lastly, addressing the knowledge gap among healthcare professionals and establishing robust governance frameworks is necessary to facilitate ethical data usage in a decentralized environment involving various stakeholders [4], [35], [36].

VIII. PROPOSED WORK

Proposed work outlines a decentralized and secure healthcare information system utilizing blockchain and distributed storage to enhance Electronic Health Record (EHR) management [10], [21], [25]. Its architecture comprises three levels: presentation, application, and decentralized infrastructure, focusing on data protection [37]. Patients access their health data via web or mobile applications, while doctors and administrators use dedicated portals for secure interaction and management [46]. The application layer, built on Node.js microservices, includes an API gateway and authentication service, with an EHR service for record handling supported by a cryptography service [22], [24]. The decentralized infrastructure combines Hyperledger Fabric and IPFS, ensuring trust and immutability [25], [37], [48]. When generating EHRs, data is encrypted and stored in IPFS, with the content identifier recorded on the blockchain, allowing patients control over their data [44]. This system promotes patient-centric control, security through cryptography, and improved inter-institutional communication, fostering a secure and transparent healthcare ecosystem [5], [10], [25].

IX. Architecture Diagram



References

[1] Z. Abbas, S. F. Ahmad, M. H. Syed, A. Anjum, and S. Rehman, "Exploring deep federated learning for the Internet of Things: A GDPR-compliant architecture."

[2] W. Abdelrahman and A. Abdelmageed, "Medical record keeping: Clarity, accuracy, and timeliness are essential," Brit. Med. J., vol. 348, p. 17716, Jan. 2014.

[3] K. Abbas, M. Afaq, T. A. 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, no. 5, 2020, Art. no. 852.

[4] A. Abdullah, S. Rogerson, N. B. Fairweather, and M. Prior, "The motivations for change towards e-government adoption: Case studies from Saudi Arabia," in Proc. E-Government Workshop, 2006, vol. 6, no. 1, pp. 1–21.

[5] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," Proc. Comput. Sci., vol. 113, pp. 73–80, Jan. 2017.

[6] S. Abimannan, E.-S. M. El-Alfy, S. Hussain, Y.-S. Chang, S. Shukla, D. Satheesh, and J. G. Breslin, "Towards federated learning and multi-access edge computing for air quality monitoring: Literature review and assessment," Sustainability, vol. 15, no. 18, p. 13951, 2023.

[7] Accenture, "The impact of healthcare cybersecurity on Saudi Arabian consumers," 2017. [Online]. Available: https://www.accenture.com/_acnmedia/pdf-59/accenture-health-consumer-survey-cybersecurity-ksa.pdf

[8] N. R. Adam and J. C. Worthmann, "Security-control methods for statistical databases: A comparative study," ACM Comput. Surv., vol. 21, no. 4, pp. 515–556, Dec. 1989.

[9] S. J. Adams, R. Tang, and P. Babyn, "Patient perspectives and priorities regarding artificial intelligence in radiology: Opportunities for patient-centered radiology," J. Am. Coll. Radiol., vol. 17, no. 8, pp. 1034–1036, Aug. 2020.

[10] C. C. Agbo, Q. H. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare, vol. 7, no. 2, p. 56, Apr. 2019.

[11] C. C. Agbo and Q. H. Mahmoud, "Comparison of blockchain frameworks for healthcare applications," Internet Technol. Lett., vol. 2, no. 5, 2019, Art. no. e122.

[12] C. C. Aggarwal and S. Y. Philip, Privacy-Preserving Data Mining: Models and Algorithms. Springer, 2008.

[13] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in Proc. IEEE Technol. Eng. Manage. Conf. (TEMSCON), Jun. 2017, pp. 137–141.

[14] F. Ahmed, A. H. Khan, J. Mehmood, N. Sarwar, A. Ali, M. Mehboob, and A. Waqas, "Wireless mesh network: IEEE 802.11s," Int. J. Comput. Sci. Inf. Secur., vol. 14, no. 12, p. 803, 2016.

[15] R. Akkaoui, "Blockchain for the management of Internet of Things devices in the medical industry," IEEE Trans. Eng. Manag., vol. 70, pp. 2707–2718, 2023.
[16] K. Alabi, "Digital blockchain networks appear to be following Metcalfe's law," Electron. Commerce Res. Appl., vol. 24, pp. 23–29, 2017.
[17] G. Alagic et al., "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST IR 8413, Gaithersburg, MD, USA, 2022.
[18] M. G. R. Alam, M. S. Munir, M. Z. Uddin, and M. S. Alam, "Edge-of-things computing framework for cost-effective provisioning of healthcare data," J. Parallel Distrib. Comput., vol. 123, pp. 54–60, Jan. 2019.
[19] V. Alcazar, "Data you can trust: Blockchain technology," Air Space Power J., vol. 31, no. 2, pp. 91–102, 2017.
[20] B. Aldosari, "Rates, levels, and determinants of electronic health record system adoption: A study of hospitals in Riyadh, Saudi Arabia," Int. J. Med. Inform., vol. 83, no. 5, pp. 330–342, May 2014.
[21] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedila, and K. Shuaib, "Introducing blockchains for healthcare," in Proc. Int. Conf. Electr. Comput. Technol. Appl. (ICECTA), Nov. 2017, pp. 1–4.
[22] A. Ali et al., "An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural networks," Sensors, vol. 22, no. 2, p. 572, 2022.
[23] B. S. Ali et al., "ICS-IDS: Application of big data analysis in AI-based intrusion detection systems to identify cyberattacks in ICS networks," J. Supercomput., vol. 80, no. 6, pp. 7876–7905, 2024.
[24] A. Ali et al., "Deep learning-based homomorphic secure searchable encryption for keyword search in blockchain healthcare systems: A novel approach to cryptography," Sensors, vol. 22, no. 2, p. 528, 2022.
[25] A. Ali et al., "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," Appl. Sci., vol. 11, no. 21, p. 9999, 2021.
[26] M. A. Almaiah et al., "A lightweight hybrid deep learning privacy-preserving model for FC-based industrial Internet of Medical Things," Sensors, vol. 22, no. 6, p. 2112, 2022.
[27] M. Almalki, G. FitzGerald, and M. Clark, "Health care system in Saudi Arabia: An overview," East. Mediterr. Health J., vol. 17, no. 10, pp. 784–793, 2011.
[28] A. Aljarullah, R. Crowder, and G. Wills, "A framework for the adoption of EHRs by primary healthcare physicians in the Kingdom of Saudi Arabia," in Proc. Int. Conf. Inf. Soc. (i-Society), Jul. 2017, pp. 49–54.
[29] N. R. Al Khater, "A model of a private sector organisation's intention to adopt cloud computing in the Kingdom of Saudi Arabia," Ph.D. dissertation, Univ. Southampton, 2017.
[30] A. Alkhodre et al., "A blockchain-based value added tax (VAT) system: Saudi Arabia as a use-case," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 5, pp. 708–716, 2019.
[31] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in Proc. 15th Learn. Technol. Conf. (L&T), Feb. 2018, pp. 112–119.
[32] A. Al Omar et al., "Medibchain: A blockchain-based privacy-preserving platform for healthcare data," in Proc. Int. Conf. Security, Privacy and Anonymity in Computation, Communication and Storage, Springer, Cham, 2017.
[33] I. Al Ridhawi et al., "A continuous diversified vehicular cloud service availability framework for smart cities," Comput. Netw., vol. 145, pp. 207–218, Nov. 2018.
[34] L. Al Ridhawi et al., "A collaborative mobile edge computing and user solution for service composition in 5G systems," Trans. Emerg. Telecommun. Technol., vol. 29, no. 11, p. e3446, Nov. 2018.
[35] W. Al-Saqaf and N. Seidler, "Blockchain technology for social impact: Opportunities and challenges ahead," J. Cyber Policy, vol. 2, no. 3, pp. 338–354, 2017.
[36] M. Altuwaijri, "Health information technology strategic planning alignment in Saudi hospitals: A historical perspective," J. Health Inform. Dev. Ctries., vol. 5, no. 2, pp. 338–355, 2012.
[37] A. G. M. Alzahrani et al., "A framework for data sharing between healthcare providers using blockchain," in Proc. 5th Int. Conf. Internet Things, Big Data Secur. (IOTBDS), vol. 1, 2020, pp. 349–358.
[38] S. Aminizadeh et al., "The applications of machine learning techniques in medical data processing based on distributed computing and the Internet of Things," Comput. Methods Programs Biomed., p. 107745, 2023.
[39] G. J. Annas, "HIPAA regulations: A new era of medical-record privacy?," N. Engl. J. Med., vol. 348, pp. 1486–1488, 2003.
[40] R. N. Asif et al., "Detecting electrocardiogram arrhythmia empowered with weighted federated learning," IEEE Access, vol. 12, pp. 1909–1926, 2024.
[41] N. Aslam et al., "Sentiment analysis and emotion detection on cryptocurrency-related tweets using ensemble LSTM-GRU model," IEEE Access, vol. 10, pp. 39313–39324, 2022.
[42] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," Computer, vol. 50, no. 9, pp. 18–28, Jan. 2017.
[43] S. Attili et al., "Blockchain: The chain of trust and its potential to transform healthcare—Our point of view," in Proc. ONC/NIST Blockchain Healthcare Res. Workshop, Gaithersburg, MD, USA, 2016, pp. 1–9.
[44] M. H. Au et al., "A general framework for secure sharing of personal health records in cloud systems," J. Comput. Syst. Sci., vol. 90, pp. 46–62, Dec. 2017.
[45] R. Azad et al., "Advances in medical image analysis with vision transformers: A comprehensive review," Med. Image Anal., vol. 91, p. 103000, 2024.

[46] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in Proc. 2nd Int. Conf. Open Big Data (OBD), Vienna, Austria, Aug. 2016, pp. 25–30.
[47] K. Azbeg et al., "A taxonomic review of the use of IoT and blockchain in healthcare applications," IRBM, vol. 43, no. 5, pp. 511–519, 2022.
[48] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, "Access control and privacy-preserving blockchain-based system for diseases management," IEEE Trans. Comput. Soc. Syst., 2022.
[49] M. Bader, R. Jayaraman, and A. Sleptchenko, "Optimizing supplier selection and order allocation for medical supplies: A mixed integer linear approach," in Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM), 2023, pp. 153–157.
[50] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," J. Softw. Eng. Appl., vol. 9, no. 10, pp. 533–546, 2016.