International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

Vol. IV, No. 09, pp. 13-22, September

Block Chain in Healthcare Ecosystems: From Electronic Health Records to Secure Data Sharing

Thirugnana Sambandham P[1], Hussain Sharif[2], Soundarya D.S Rajan[3]

[1]Assistant Professor, Department of Computer Science and Engineering, Sri Rangapoopathi College of Engineering, Alampoondi, Gingee, 604 151, India. Email: samutha85@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering (AIML), Marri Laxman Reddy Institute of Technology and Management, Hyderabad -500043, India. Email: sharif0206@mlritm.ac.in
[3]Assistant Professor, Department of Computer Science and Engineering (AIDS), Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai, Tamil Nadu 600117, India. Email: soundaryadsrajan@gmail.com

Corresponding Author E-mail: [1]samutha85@gmail.com

ABSTRACT: The healthcare sector increasingly relies on digital technologies for storing, accessing, and sharing sensitive medical data, yet challenges such as data privacy, interoperability, security, and trust persist. Traditional centralized systems for managing Electronic Health Records (EHRs) are vulnerable to cyberattacks, unauthorized access, and data fragmentation. Blockchain, with its decentralized, transparent, and tamper-resistant architecture, provides a transformative approach to overcome these limitations. By integrating blockchain with distributed storage and smart contracts, healthcare ecosystems ensure secure data exchange, patient-controlled access, and regulatory compliance while maintaining efficiency. This study highlights the role of blockchain in enhancing EHR management and enabling secure, seamless data sharing among hospitals, laboratories, insurers, and patients. Block chain techniques PoR, PoS, PoTE, PoW, PoCW are used to calculate the EHRs. Among the techniques PoR achieves the highest throughput of 98%. Furthermore, it explores scalability, interoperability, and ethical considerations that influence its adoption. Overall, blockchain holds the potential to create a patient-centric, trustworthy, and resilient healthcare data management framework.

Keywords: Blockchain, Electronic Health Records, Data sharing, Healthcare Ecosystems, Electronic Medical Record

1. Introduction

In recent years, block chain have emerged as a prominent slogan in the Information and Communication Technology (ICT) production [1]. Whereas, this rapidly advancing technology shows immense promise in overcoming challenges of data privacy, security, and integrity, blockchain first gained widespread recognition with the publication of Satoshi Nakamoto's Bitcoin white paper in 2008 [2]. The essential technology of Bitcoin demonstrated how financial transactions executed securely without the need for a centralized trusted authority [3]. Fundamentally, blockchain operates as a distributed peer-to-peer network (P2P) network, blockchain enables digital data to be shared either publicly or privately [4]. Moreover, conventional financial transactions, together the source as well as the destination must hang on a Trusted Third Party (TTP) to facilitate and validate the exchange [5]. In contrast, blockchain eliminates the reliance on a Trusted Third Party (TTP) by enabling direct

peer-to-peer transactions that are validated through consensus mechanisms. This decentralized validation process not only enhances transparency but also ensures that each transaction is immutable and verifiable by all participants in the network. As a result, blockchain technology addresses several limitations of conventional systems, such as vulnerability to single points of failure, high operational costs, and the risk of fraud or unauthorized alterations. As its source code is open-source, developers were able to modify and enhance it, leading to the evolution of blockchain technology through several phases in table 1 [6]:

Table 1: *Block chain phases*

Block chain version	Functions
Blockchain 1.0	Representing the initial and most notable application of Distributed Ledger Technology (DLT), this phase focused on cryptocurrencies. Blockchain 1.0 introduced a transparent mechanism for recording and verifying Bitcoin transactions on a shared ledger.
Blockchain 2.0	Marked by the introduction of legally binding Smart Contracts, generated from small computer programs, enabling automated and enforceable transactions. Ethereum emerged as the most prominent platform in this phase.
Blockchain 3.0	Centered on Decentralized Applications (DApps), eliminating reliance on centralized infrastructure. Unlike traditional applications, DApps utilize decentralized storage and servers. This phase aimed to extend blockchain adoption into conventional sectors such as government, healthcare, and education.
Blockchain 4.0	Designed to meet the diverse business requirements of Industry 4.0. It emphasizes heightened trust and privacy, making it suitable for complex enterprise environments.

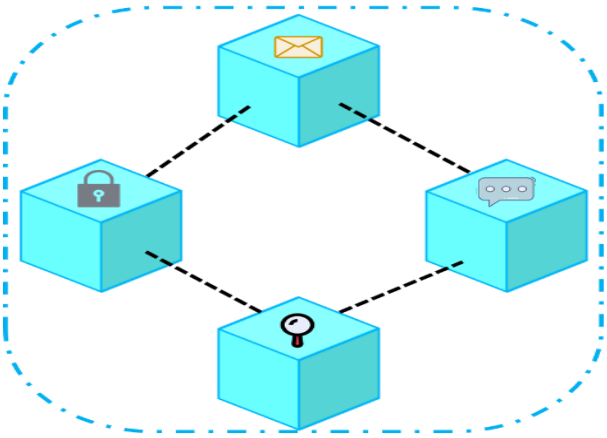

Figure 1: *Structure of block chain*

1.1 Types of blockchain

A Blockchain network in figure 1 is classified based on factors such as network size, application domain, and the type of consensus algorithm employed. Broadly, three main categories are recognized [7]:

- Public
- Private
- Consortium (Hybrid)

1.1.1 Public Blockchain

In a public blockchain, participation is open to anyone, allowing unrestricted access to block data. It operates on a public Distributed Ledger Technology (DLT) framework, enabling any internet-connected individual to join the network and act as an authorized miner. While the network is publicly accessible, user identities are represented by pseudo-anonymous hash-generated addresses, ensuring a degree of privacy [8].

1.1.2 Private Blockchain

A private blockchain shares operational and algorithmic similarities with a public blockchain but differs in its purpose and accessibility. It is a permissioned or restricted network, governed by predefined contact mechanism guidelines. Operating within a secure environment, it remains circulated in structure yet centralized in authority, with participation limited to approve entities [9].

1.1.3 Consensus algorithms for blockchain

A consensus algorithm is a coordination mechanism that allows nodes within a blockchain network to collectively agree on the validity of transactions. It agreement that all participating nodes uphold a consistent, accurate, and secure ledger, as shown in Table 2 [10].

Table 2: *Types of Consensus algorithm*

Types of Consensus algorithm	Function
Proof-of-Work (PoW)	PoW is the earliest and most widely adopted consensus mechanism, recognized for its robustness and reliability.
Proof-of-Stake (PoS)	PoS select a miner based on their wealth (stake) through a pseudorandom process.
Delegated Proof-of-Stake (DPoS)	In DPoS, token holders select delegates to validate blocks on their behalf.
Proof-of-Authority (PoA)	PoA combines elements of PoW as well as PoS, prioritizing the reputation of validators rather than their stake
Proof-of-Vote (PoV)	PoV is designed for consortium blockchains.
Practical Byzantine Fault Tolerance (PBFT)	PBFT developed to handle Byzantine faults, allowing consensus even if some nodes are malicious.
Proof-of-Importance (PoI)	PoI selects miners based on productivity rather than computational power or stake.

1.2 Electronic health records

EHR store patient medical analytical reports in digital formats such as JPEG or PDF. An Electronic Medical Record (EMR) serves as one of the key data sources for EHRs, aggregating information from various medical organizations. In addition, EHRs incorporate individual health data composed from wearable devices such as, smart watches, fitness bands managed by patients themselves as shown in figure 2 [11].

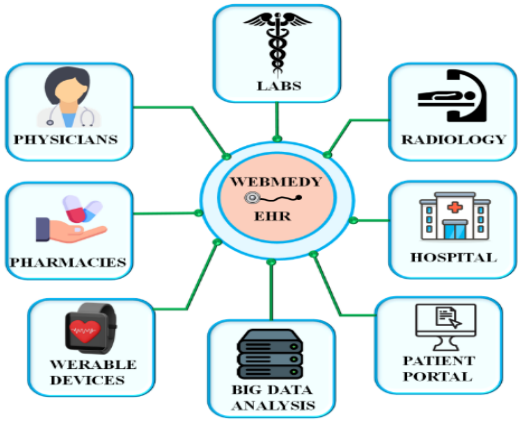

Figure 2: *Electronic Health Records*

1.3 Related work

Syed *et al* [12] (2025) have proposed a Blockchain Enabled Approach to Secure and Scalable Patient E-Health Data. A blockchain-enabled approach to secure and scalable patient e-health data offers significant benefits such as enhanced security, integrity, and privacy of medical records through decentralized and tamper-proof storage. However, smart contracts are utilized to manage and preserve critical information on the blockchain, ensuring data permanence and automated functionality.

Jiancheng *et al* [13] (2024) have developed a role of artificial intelligence for the application of integrating electronic health records and patient-generated data in clinical decision support. The integration of electronic health records (EHRs) and patient-generated data into clinical decision support (CDS) systems using artificial intelligence (AI) plays a vital role in enhancing healthcare delivery. It also enables real-time monitoring of patient health through wearable devices and remote sensors, facilitating proactive care and reducing hospital readmissions. However, there are notable drawbacks, including concerns over data privacy and security, algorithmic bias arising from poor-quality training data.

Antwi *et al* [14] (2021) have invented a blockchain-based framework Hyper ledger Fabric. It is employed to build two liberated private

blockchain consortiums designed for secure and proficient healthcare data sharing, wherever multiple health individuals participate in a P2P consortium network. However, it have some limitations, including a steep learning curve, complex deployment processes, and high resource requirements for managing nodes and chain code.

Faruk *et al* [15] (2022) have presented a Hyperledger fabric for teleradiology application for secure and efficient medical image sharing. Model have strong data privacy, fine-grained access control, scalability for handling large imaging datasets, and reduced risk of unauthorized data manipulation. However, disadvantages include the complexity of setup and maintenance, significant computational and storage overhead and potential latency issues during large-scale data exchanges.

The main contributions of this paper are as follows:

- A comprehensive analysis of leveraging blockchain technology for effective health record management.
- An in-depth examination of AI, IoMT enhances the management and utilization of health records.
- An updated exploration of privacy and security challenges associated with EHR management.

2. Reviews in blockchain in EHRs

2.1 Proof of Trust as well as Expertise (PoTE)

PoTE consensus mechanism leverages the dependability and domain-specific knowledge of operators within the network for EHR. It ensures secure and efficient transaction validation whereas meeting the critical requirements of healthcare data management. The PoTE model demonstrates strong performance, achieving an average block processing time, a throughput and a success rate even when operating across a large number of nodes. PoTE include high scalability, low latency, domain-driven trust validation, and strong alignment with healthcare compliance needs. However, it is potential bias in expertise-based validation, dependency on accurate trust scoring, and challenges in maintaining fairness and decentralization when expertise is unevenly distributed among participants [16].

2.2 Proof of Stake (PoS)

A lightweight hybrid security-driven explanation is designed for Healthcare Networking Systems, incorporating an optimized consensus algorithm specifically tailored to ensure secure and efficient EHR data management. Built within a blockchain framework, the model employs a robust security protocol to safeguard information transfer and prevent data theft. By combining the strengths of PoW and PoS, the algorithm achieves an effective balanced trade-off between computational productivity, security, and reorganization [17].

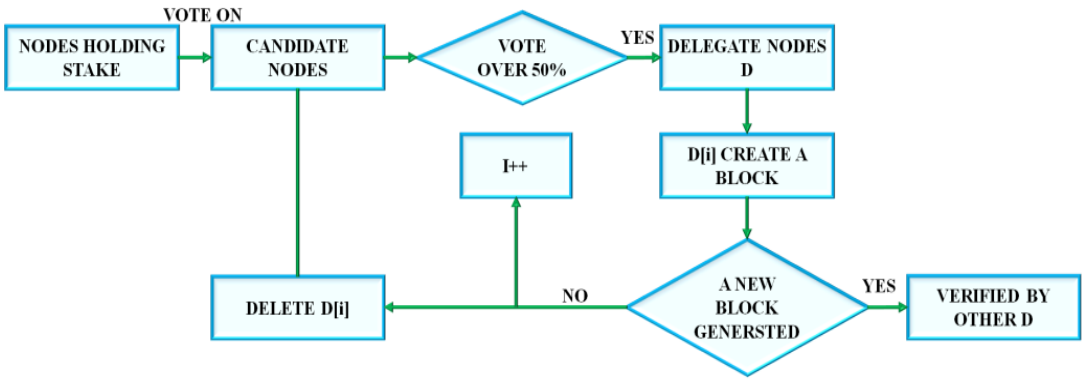

Figure 3: *Flow chart for POS*

2.3 Proof-of-Work (PoW):

For EHR by leveraging the unique structures of Hashgraph within the MedHash framework like the gossip protocol as well as virtual voting each node actively participates in the consensus process, eliminating the possibility of power centralization among limited nodes. As MedHash does not rely on mining, it significantly reduces energy consumption using PoW blockchains. In addition, it offers strong resilience against Sybil attacks and double-spending issues. When applied to healthcare, MedHash enhances privacy protections and strengthens data security by giving patients more authority and mechanism over their complex medical data [18]

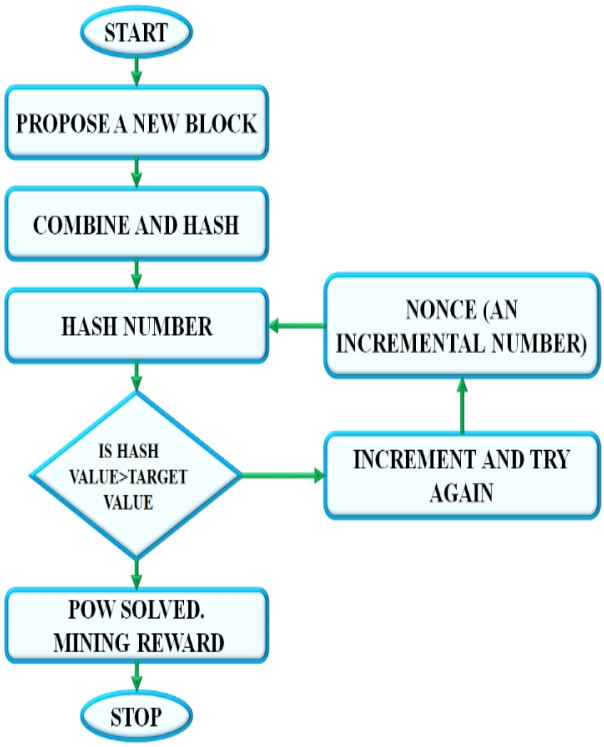

Figure 4: *Flow chart for PoW*

2.4 Practical Byzantine Fault Tolerance (PBFT)

The IPFS is integrated with a consortium blockchain to create hybrid storage architecture for EHRs, thereby enhancing data safety, confidentiality safety, besides effective productivity. The system incorporates unidirectional multi-hop restricted proxy re-encryption with distributed key generation, enabling safe EHR sharing whereas ensuring fine-grained access control. Additionally, all user operations on EHRs are logged, ensuring full traceability of data usage. To further improve performance, a dynamic Byzantine fault-tolerant (dBFT) algorithm centred arranged character as well as collecting introduced, the limitations of PBFT allowing nodes to achieve consensus with greater efficiency. Furthermore, the hybrid model mitigates single-point failures, strengthens resistance to insider threats, and ensures availability of critical health data even under network disruptions, making it a robust and reliable solution for real-world healthcare applications [19].

2.5 Proof-of-Authority (PoA)

In IoTChain-EHR framework, fine-grained access control is achieved using an Attribute-Based Access Control (A-BAC) plan, with the Ethereum blockchain serving as a transparent and auditable entrance control layer. Smart contracts are specifically designed this ideal, it integrates the Ethereum blockchain with IPFS to enable secure and decentralized storage of EHRs. Furthermore, conventional PoW mechanism is replaced with PoA to reduce transaction costs and enhance throughput. Experimental validation on the Ethereum Rinkeby test network confirms that the solution is both practical and cost-effective for efficient management and sharing of sensitive healthcare data. Moreover, the system offers strong accountability by recording all access events on the blockchain, while the combination of IPFS and Ethereum significantly reduces on-chain storage overhead. Collectively, these features position IoTChain-EHR as a secure, efficient, and sustainable approach for managing electronic health records in next-generation healthcare ecosystems [20].

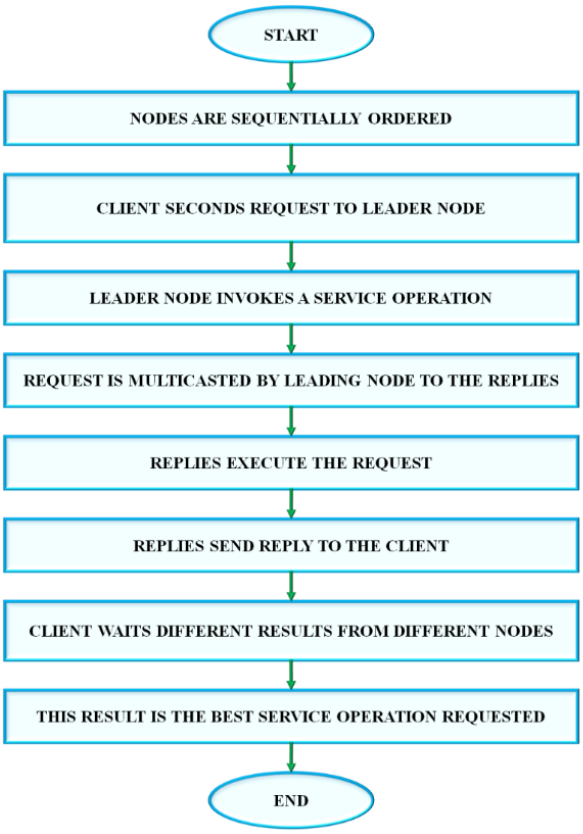

Figure 5: *Flow chart for PoA*

2.6 Proof of Continuous Work (PoCW)

PoCW consensus algorithm-based blockchain structure is for securing EHRs, referred to as PoCW-BC-EHR. The framework consists of three key processes: healthcare institution enrolment, blockchain-enabled secure data storage, and blockchain-enabled secure data sharing. During the enrolment phase, new healthcare providers join the blockchain network by generating their public and private keys. BC-enabled secure data storage relies on the PoCW algorithm to ensure tamper-proof management of patient health records, In the secure data sharing process, medical records are exchanged among hospitals, clinics, and research entities with blockchain verification, ensuring authenticity and traceability. Furthermore, a consistency check protocol is applied to safeguard stored data, providing maximum security, integrity, and reliability in managing sensitive healthcare information [21].

2.7 Proof-of-Reputation (PoR)

A BlockChain-based User Authentication and Data Sharing (BC-UADS) structure designed to enhance the security and reliability of EHRs. In BC-UADS, multiple hospital servers collaborate within a consortium blockchain network, ensuring photo, immutability, as well as reality of patient medical data. The framework enables authorized doctors to securely share or retrieve patient EHR metadata through the blockchain, where storing metadata enhances trustworthiness and provides stronger protection for real-time healthcare applications. To manage secure and efficient data sharing, the BC-UADS framework employs a PoR consensus algorithm, which validates transactions based on the credibility of participating nodes. This design ensures trusted collaboration among healthcare entities whereas maintaining patient privacy and data integrity. Moreover, the BC-UADS framework integrates fine-grained access control policies to ensure that only authorized users with predefined attributes can access specific medical records. By employing smart contracts, the system automates authentication, access verification, and secure sharing processes without the need for third-party intermediaries, thereby reducing delays and operational overhead [22].

Table 3: *Reviews for blockchain techniques, AI & IoMT*

Author & year	Methods & it's functions	Benefits	Limitations
Johari et al (2022) & Almaiah et al (2022)	For securing medical patient data using blockchain technology a PoW algorithm is used.	Resistant to tampering and double-spending, ensuring integrity of patient data.	Limited transaction throughput and high latency so it is unsuitable for EHR access [23&24]

Zou et al (2021)	An SPChain technique for secure EHR using the PoR algorithm	Reduces risks of malicious nodes since reputation is tied to past behaviour	Requires robust mechanisms to evaluate, update, and audit reputations across healthcare entities [25].
Bodur et al (2024)	To stock, contact, then segment medical data wanting risking security vulnerabilities and attacks PoA and PoS algorithm is utilized.	Low latency and high throughput, ideal for real-time EHR access	Requires careful staking and slashing mechanisms to ensure fairness [26].
Chi et al (2020)	To ensure the security of data sharing for HER a blockchain and a community detection algorithm is used.	Identifies hidden structures in large, complex networks	Algorithms struggle to detect nodes belonging to multiple communities [27].
Dhinakaran et al (2025)	Adaptive Feature-Centric Polynomial Data Security Model (AFPDSM) capable of efficiently enforcing security measures on diverse datasets	Uses polynomial-based encryption to protect sensitive patient data from unauthorized access.	Requires careful handling of multiple encryption keys for different features, increasing system complexity [28].
Lakshmanan, M., and G. S. Anandha Mala (2024)	To enhance the security of EHRs, a novel Iteration-Based Firefly Reptile Search Algorithm (IFRSA) is employed.	Identify the most significant features in EHR datasets, reducing dimensionality whereas preserving accuracy.	Performance depends on fine-tuning multiple parameters [29].
Ray et al (2021)	The data sharing on a blockchain using PoA is intended to be secure EHR.	Handle a high volume of medical record transactions and large-scale healthcare networks effectively.	If multiple validators collude, they potentially manipulate EHR data [30].

Comparison for the review techniques

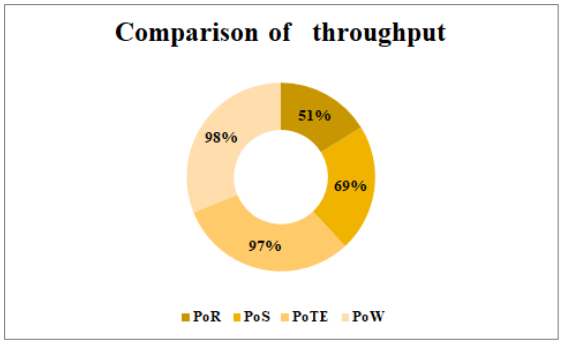

Figure 6: *Comparison of throughput*

Figure 6 shows the Comparison of Throughput illustrates the performance of four different blockchain consensus mechanisms in terms of throughput efficiency. Among the approaches compared, Proof of Reputation (PoR) [25] demonstrates the highest throughput with 98%, followed closely by Proof of Stake (PoS) [17] at 97%, indicating their effectiveness in handling large volumes of transactions efficiently. Proof of Trusted Execution (PoTE) [16] achieves a moderate throughput of 69%, while Proof of Work (PoW) [28] records the lowest throughput at 51%, reflecting the limitations of computationally intensive mechanisms. Overall, the comparison highlights that consensus models such as PoR and PoS provide superior scalability and transaction-handling capacity, making them more suitable for modern, data-intensive blockchain applications compared to PoW and PoTE.

Table 4: *Comparison of block processing time*

Method	Time
PoTE [16]	0.25sec
PoS [17]	0.61 sec

Table 4 presents a comparison of execution time between two blockchain consensus mechanisms, namely PoTE [16] and PoS [17]. According to the results, PoTE demonstrates a significantly lower execution time of 0.25 seconds, highlighting its efficiency in processing transactions rapidly. In contrast, PoS records a higher execution time of 0.61 seconds, which, although slightly slower, still

reflects a reasonably efficient mechanism compared to more traditional approaches such as Proof of Work. Overall, the comparison indicates that PoTE outperforms PoS in terms of speed, making it more suitable for applications that require fast transaction validation and real-time processing.

3. Conclusion

In this paper, a blockchain technology offers a transformative solution for healthcare ecosystems by enabling secure, transparent, and tamper-resistant management of EHRs. Through decentralized storage, smart contracts, and patient-controlled access, it enhances data sharing among hospitals, laboratories, and insurers while safeguarding privacy and trust. Block chain techniques PoR, PoS, PoTE, PoW, PoCW are used to calculate the EHRs. Among the techniques PoR achieves the highest throughput of 98%. Although challenges related to scalability, standardization, and ethical governance remain, the integration of blockchain with distributed storage and smart contracts paves the way for a resilient, efficient, and patient-centric healthcare ecosystem. In future research, efforts should be directed toward designing lightweight consensus algorithms tailored for healthcare applications, developing standardized frameworks for interoperability across diverse medical platforms, and integrating artificial intelligence with blockchain to enhance predictive healthcare services.

References

1. Atul B Kathole; Sonali D. Patil; Savita Kumbhare; Kapil Vhatkar; Aniruddha P. Kshirsagar; Vinod V. Kimbahune, Year: 2024, “Electronic health records protection strategy by using blockchain approach”, Multimedia Tools and Applications, Vol: 83, No: 39, pp. 86883-86894.

2. Hemant Ghayvat; Sharnil Pandya; Pronaya Bhattacharya; Mohd Zuhair; Mamoon Rashid; Saqib Hakak; Kapal Dev, Year: 2021, “CP-BDHCA: Blockchain-based Confidentiality-Privacy preserving Big Data scheme for healthcare clouds and applications”, IEEE Journal of Biomedical and Health Informatics, Vol: 26, No: 5, pp. 1937-1948.

3.Abinaya Inbamani; N. Divya; RR Rubia Gandhi; M. Karthik; M Sivaram Kumar, Year: 2024, “Cyber Security for Intelligent Systems The Fusion of Artificial Intelligence and Soft Computing Techniques for Cybersecurity”, pp. 133-150, Apple Academic Press.

4. ATR Krishna Priya; R. Anuja, Year: 2023, “Novel and Secure Blockchain Framework for Internet of Things Health Applications”, International Journal of Advanced Trends in Engineering and Management (IJATEM), Vol: 2, No. 03, pp. 10-18.

5. RR Rubia Gandhi; Abinaya Inbamani; N. Divya; M. Karthik; Ramya, Year: 2024, “E;Soft Computing Techniques for Cyber-Physical Systems”, The Fusion of Artificial Intelligence and Soft Computing Techniques for Cybersecurity, pp. 169-193, Apple Academic Press.

6. Anil Kumar Mishra; Yogomaya Mohapatra, Year: 2024, “Hybrid blockchain based medical data sharing with the optimized CP-ABE for e-Health systems”, International Journal of Information Technology, Vol: 16, No: 1, pp. 121-130.

7. Saeed Alzahrani; Tugrul Daim; Kim-Kwang Raymond Choo, Year: 2022, “Assessment of the blockchain technology adoption for the management of the electronic health record systems”, IEEE Transactions on Engineering Management, Vol: 70, No: 8, pp. 2846-2863.

8. Abinaya Inbamani; A. Siva Sakthi, Year: 2022, “Internet of Things Embedded in Healthcare Applications”, 6th International Conference on Computing Methodologies and Communication (ICCMC), pp. 382-389, IEEE.

9. S. Chidambaranathan; R. Geetha, Year: 2024, “Deep learning enabled blockchain based electronic heathcare data attack detection for smart health systems”, Measurement: Sensors, Vol: 31, pp. 100959.

10. H. Vidhya; Abinaya Inbamani; S. Lingeswaran; R. Abishek; R. Harish; K. Kishor, Year: 2021, “Internet of medical things applications for healthcare industry”, IEEE international conference on mobile networks and wireless communications (ICMNWC), IEEE.

11. Faiza Hashim; Khaled Shuaib; Farag Sallabi, Year: 2022, “Connected blockchain federations for sharing electronic health records”, Cryptography, Vol. 6, no. 3, pp. 47.

12. SA Syed, Year: 2025, “Blockchain Enabled Approach to Secure and Scalable Patient E-Health Data”.

13. Jiancheng Ye; Donna Woods; Neil Jordan; Justin Starren, Year: 2024, “The role of artificial intelligence for the application of integrating electronic health records and patient-generated data in clinical decision support”, AMIA Summits on Translational Science Proceedings 2024, pp. 459.

14. McSeth Antwi; Asma Adnane; Farhan Ahmad; Rasheed Hussain; Muhammad Habib ur Rehman; Chaker Abdelaziz Kerrache, Year: 2021, “The case of HyperLedger Fabric as a blockchain solution for healthcare applications”, Blockchain: Research and Applications, Vol: 2, No: 1, pp. 100012.

15. H. Vidhya, Abinaya Inbamani; S. Lingeswaran; R Abishek; R Harish; K Kishor, Year: 2021, “Internet of medical things applications for healthcare industry”, IEEE international conference on mobile networks and wireless communications (ICMNWC), IEEE.

16. Jeya Bright Pankiraj; Govindaraj Vishnuvarthanan; Yudong Zhang; Murugan Pallikonda Rajasekaran; Milton Anisha, Year: 2022, “Development of scalable coding for the encryption and decryption of images using Modified Diagonal Min Max Block Truncation Code”, Multimedia Tools and Application, Vol. 82, No. 8, pp. 12263-12277.

17. Murari Kumar Singh; Sanjeev Kumar Pippal; Vishnu Sharma, Year: 2025, “Lightweight blockchain mechanism for secure data transmission in healthcare system”, Biomedical Signal Processing and Control, Vol: 102, pp. 107411.

18. Poonam Verma; Vikas Tripathi; Bhaskar Pant, Year: 2024, “Secure Hashgraph for healthcare: Strengthening privacy and data security in patient records”, IEEE Transactions on Consumer Electronics, Vol: 70, No: 1, pp. 1205-1213.

19. Guangfu Wu; Haiping Wang; Zi Yang; Daojing He; Sammy Chan, Year: 2024, “Electronic health records sharing based on consortium blockchain”, Journal of Medical Systems, Vol: 48, No: 1, pp. 106.

20. Tao Tang; Zhuoyang Han; Zhen Cai; Shuo Yu; Xiaokang Zhou; Taiwo Oseni; Sajal K. Das, Year: 2024, “Personalized federated graph learning on non-iid electronic health records”, IEEE Transactions on Neural Networks and Learning Systems, Vol: 35, No. 9, pp. 11843-11856.

21. P. Sheela Rani; S. Baghavathi Priya, Year: 2023, “A block chain-based approach using proof of continuous work consensus algorithm to secure the educational records”, Peer-to-Peer Networking and Applications, Vol: 16, No: 5, pp. 2456-2473.

22. Preeti Soni; SK Hafizul Islam; Arup Kumar Pal; Nimish Mishra; Debabrata Samanta, Year: 2024, Year: 2024, “Blockchain-based user authentication and data-sharing framework for healthcare industries”, IEEE Transactions on Network Science and Engineering, Vol: 11, No. 4, pp. 3623-3638.

23. Rahul Johari; Vivek Kumar; Kalpana Gupta; Deo Prakash Vidyarthi, 2022, “BLOSOM: BLOckchain

technology for Security of Medical records", Ict Express, Vol: 8, No. 1, pp. 56-60.

24. Mohammed Amin Almaiah; Aitizaz Ali; Fahima Hajjej; Muhammad Fermi Pasha; Manal Abdullah Alohali, Year: 2022, "A lightweight hybrid deep learning privacy preserving model for FC-based industrial internet of medical things", Sensors, Vol: 22, No: 6, pp. 2112.

25. Renpeng Zou; Xixiang Lv; Jingsong Zhao, Year: 2021, "SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system", Information Processing & Management, Vol: 58, No: 4, pp. 102604.

26. Hüseyin Bodur; Imad Fakhri Taha Al Yaseen, Year: 2024, "An Improved blockchain-based secure medical record sharing scheme", Cluster Computing, Vol: 27, No. 6, pp. 7981-8000.

27. Jiancheng Chi; Yu Li; Jing Huang, Jing Liu; Yingwei Jin; Chen Chen; Tie Qiu, Year: 2020, "A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things", Journal of Network and Computer Applications, Vol: 167, pp. 102710.

28. D. Dhinakaran; R. Ramani; S. Edwin Raja; D. Selvaraj, Year: 2025, "Enhancing security in electronic health records using an adaptive feature-centric polynomial data security model with blockchain integration", Peer-to-Peer Networking and Applications, Vol: 18, No: 2, pp. 7.

29. M. Lakshmanan; G. S. Anandha Mala, Year: 2024, "Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm", Knowledge and information systems, Vol: 66, No: 1, pp. 481-509.

30. Partha Pratim Ray; Biky Chowhan; Neeraj Kumar; Ahmad Almogren, Year: 2021, "BIoTHR: Electronic health record servicing scheme in IoT-blockchain ecosystem", IEEE Internet of Things Journal, Vol: 8, no. 13, pp. 10857-10872.