MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1974 -1978

Blockchain-Based Secure Data Sharing Framework for Healthcare Systems

Satyavolu Rama Vijaya Kumar[1], Prof K Venkata Subbaiah[2]
[1]Research Scholar, Department of Mechanical Engineering, Andhra University, Visakhapatnam, India. Email: VijayIEM@outlook.com
[2]Professor of Mechanical Engineering, Andhra University, Visakhapatnam, India. Email: profkvsau@andhrauniversity.edu.in

Abstract: **The safe exchange of healthcare information is a burning issue because of a growing number of cyber threats, divided information platforms, and insufficient control over sensitive medical records by patients. The proposed research is a framework of Blockchain-Based Secure Data Sharing in Healthcare Systems that provides data confidentiality, integrity, transparency, and scalability in a decentralized system that can be used to distribution of Menstrual Products to women under Menstrual Health Management (MHM). The model combines a permissioned blockchain with off-chain encrypted storage, cryptographic hash checking, and access control via smart contracts in order to support patient-centric data sharing in healthcare among stakeholders. Also, a smart anomaly detection system is included to track the behavior of access to the system and detect possible threats to security in a real-time mode. There was a simulation of a multi-stakeholder healthcare setting with 10,000 synthetic electronic health records the subject of extensive experimentation. The findings illustrate 100 percent accuracy of the verification of integrity of data, the latency of encryption and decryption of AES for 50 MB records is less than 40 ms, and ACS is 98.3 percent. The detection accuracy at the anomaly detection model was 96 percent with low false positives whereas the permissioned blockchain performed in a stable way with a throughput of 125 transactions per second at 100 nodes. The fact that the proposed framework has better security, transparency, and efficiency and acceptable computational overhead proves to be more effective than the recent related works through comparative analysis. Altogether, the research confirms that blockchain is a potential and an effective tool in secure, scalable, and patient-centered healthcare data sharing, which should be implemented in the next generation smart healthcare ecosystem.**

Keywords: Blockchain, Healthcare Data Sharing, MHM Smart Contracts, Data Security, Privacy Preservation

I. INTRODUCTION

There is a fast-growing digitalization of the healthcare sector due to the popularity of Electronic Health Records (EHRs), telemedicine platforms, wearable health devices, Menstrual Health Management products and health information exchange systems. Although these innovations improve clinical effectiveness, and patient outcome, some serious challenges are also brought up by the innovations on the topic of data security, preservation of privacy, interoperability, and trust between the parties [1]. Healthcare data is valuable and sensitive information, and it is a reliable object of cyberattacks, data breaches, and unauthorized access. Traditional data-sharing models are frequently characterized by single points of failure, low transparency and insufficient control over their personal health data by the patients [2]. In this respect, blockchain technology has become a prospective framework of facilitating secure and reliable healthcare data sharing. Blockchain was first created as a means to store cryptocurrencies, but it functions as an immutable distributed registry maintained in a decentralized fashion, by which transactions are recorded transparently and in an irreversible way. Blockchain can provide data integrity, accountability, and traceability without the aids of a central authority by using cryptographic mechanisms and consensus protocols. The latter features render it especially appropriate in healthcare settings that deal with multiple, distrustful parties to each other, including hospitals, laboratories, insurers, and researchers [3]. A persistent limitation to this field is that A Blockchain-Based Secure Data Sharing Framework in Healthcare Systems suggests ways to solve the current constraints by combining patient-centric control over data ownership, providing fine-grained access control, and interoperability in heterogeneous healthcare systems. Rather than having giant medical files stored directly on the blockchain, the framework will normally combine off-chain storage with on-chain hash verification and smart contracts to govern the permissions to use access dynamically. This will improve scalability and has high security levels guaranteed. On the whole, it is possible that blockchain-based data-sharing models can greatly enhance the levels of trust, data confidentiality, and efficiency of healthcare systems. This initiative promises to be a groundbreaking technology to address healthcare information management in the next generation by enabling patients to have greater control over it and allowing others to access its profile and provide safe, auditable, methodical access when needed.

II. RELATED WORKS

The current literature has widely discussed the use of blockchain, artificial intelligence (AI), Internet of things (IoT), and advanced cryptography tools to prolong security and privacy issues of healthcare data dissemination. Proposed by Habib and Manik [15], ShaEr is a blockchain-powered framework that can be used to share medical data safely and monetise it. The work highlighted the patient control over healthcare information and implemented smart contracts to control access to information and income earned. Although ShaEr enhances trust and transparency, it is mostly used in data monetisation and does not have intelligent threat detection efficiency. Haojie et al. [16] introduced a trusted data management framework using blockchain with privacy protection of secure IoT systems. They combine encryption and decentralized trust in their approach to secure data generated by IoT in healthcare. Even though the framework offers great data confidentiality, it is more IoT oriented and lacks complete potential over patient-centric access control in complicated healthcare systems. An in-service survey by Hassan et al. [17] was based on intelligent, secure, and distributed structures of Healthcare 5.0. The authors have indicated the intersection of blockchain, AI, and point-to-point computing to enable individualized and safe health care. Nonetheless, the research is quite theoretical and fails to offer practical validation and a comparison of the results of various worksheets. Hemdan Ezz El-Din and Amged [18] discussed smart and secure healthcare systems with the use of digital twins, blockchain, and federated learning. As evidenced in their work, their virtual replicas of patients can be safely handled with the help of blockchain ensuring their data privacy with the help of decentralized learning. Nevertheless, the computational complexity and deployment challenges of real-time healthcare applications are high with the innovation of the framework. Javed et al. [19] have suggested an AI-based blockchain and federated learning system of the electronic health-record sharing (EHRs) security. Their model uses blockchain-based access control as well as decentralized learning in order to avoid the leakage of data. Although this strategy improves privacy and collaborative learning, it implements the use of complex AI models that could restrain scalability in healthcare facilities with limited resources.

Krishnan et al. [20] designed a blockchain-based IoT-based health system based on a multiscale stacked Residual-GRU model of transmitting data using special encryption and the blockchain security system. They have demonstrated a better ability to predict and provide safe communication. The paper is however more

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1974 -1978

concerned with data transmission security and less about the holistic process of data sharing and access. Kurt et al. [21] examined how smart contracts and blockchain have developed in terms of healthcare policy implementation. Their input has a regulatory and governance emphasis and no technical assessment of system performance. Vishnu Kumar and Madhumathi [22] suggested a demonstrable principle of partitioned secure blockchain with encryption as a means to improve privacy in IoT-based healthcare although the problem of scalability remains. In Mallick et al. [24,25], the authors proposed two-layered blockchain and IPFS based architectures of secure and scalable smart-based healthcare systems. These papers enhance storage efficiency and credibility but they fail to consider smart anomaly detection. Lastly, Maravi and Mishra [26] came up with a security data storage and sharing approach based on blockchain in the form of an electronic health passport, which increases portability but has less real-time monitoring of access. In general, the current literature shows how blockchain could be used in healthcare security, but tends to focus on individual areas through privacy, integration with IoT, or monetisation. The presented work stands out as it combines cryptographic security, access control built on smart contracts, scalability, as well as intelligent anomaly identification into one, experimentally proven framework.

III. METHODS AND MATERIALS

Data Description

The framework takes into account electronic health record (EHR) data that were measured in a set of simulated multi-hospital settings. Its data consists of patient demographics, diagnosis code, laboratory report, metadata of medical images, and treatment history. The information that can be identified as personal (PII) like names and addresses will be anonymized through cryptographic hash and then processed. The real medical records are stored in off-chain storage (e.g. cloud or distributed file system), an access permissions and encrypted hash is stored on the blockchain and only logs of transactions [4]. This hybrid will guarantee scale with privacy and adherence to healthcare data protection laws.

System Architecture and Tools

In the system, the permissioned blockchain network has hospitals, labs, and insurers serving as authorized nodes. Smart contracts are used to implement access controls and cryptographic algorithms are used to provide secure authentication and data transfer. The framework utilizes four core algorithms including uses of SHA-256 in data integrity, AES in data confidentiality, smart contract-based access control, and anomaly detection based on machine learning to detect misuse [5].

Algorithm 1: SHA-256 Hashing for Data Integrity

SHA-256 is an encryption whitewashed bar that is applied to guarantee the integrity of healthcare documents. The original health record is fed through SHA-256 to code a fixed length hash value before any reference of the medical data is stored on the blockchain. Even the slightest change in the data re-hashes the data to an entirely different value and manipulation of the data is instantly spotted. Within the proposed model, the on-chain storage is the storage of SHA-256 hashes, whereas the files remain off-chain [6]. In the process of accessing information, the hash of information that was accessed is recalculated and the calculated one is compared against the one that was stored to ensure authenticity and integrity.

```
"Input: Medical_Record
Hash_Value = SHA256(Medical_Record)
Store Hash_Value on Blockchain
Retrieve Record
New_Hash = SHA256(Retrieved_Record)
If Hash_Value == New_Hash
  Data is Authentic
Else
  Data Tampered"
```

Algorithm 2: AES Encryption for Data Confidentiality

Healthcare data protection against unauthorized access is provided with the help of Advanced Encryption Standard (AES). Before the off-chain storage, medical records are encrypted by means of a symmetric AES key. The plaintext data can only be accessed by the authorized users with the right decryption key. Within this framework, the encryption keys are safely handled with the help of smart contracts and are not disclosed until there is an identity verification [7]. The security of AES is high with low computational cost thus applicable to the use of AES in large health care data systems like lab reports and medical images whilst keeping it confidential during storage and transmission.

```
"Input: Medical_Record, Secret_Key
Encrypted_Data = AES_Encrypt(Medical_Record, Secret_Key)
Store Encrypted_Data Off-chain
Authorized_User decrypts using Secret_Key"
```

Algorithm 3: Smart Contract–Based Access Control

Smart contracts enforce access control policies within the network of blockchain networks. Every patient is considered the owner of the data and is able to revoke or give access rights to healthcare providers on a dynamic basis. The smart contract identifies the identity, role and purpose of access of the requester and permits the data to be retrieved. The approval and every request of access is stored as immutable transactions on the blockchain which makes it transparent and audit-traceable [8]. The algorithm is used to remove the need to use centralized authorities and provide patient-based control over the sharing of healthcare data.

```
"Input: User_Request
Verify User_Identity
Check Access_Permission
If Permission_Granted
  Allow Data Access
Log Transaction on Blockchain
Else
  Deny Access"
```

Algorithm 4: Machine Learning–Based Anomaly Detection

To improve security, an anomaly detector algorithm that is powered by machine learning controls the access patterns to the blockchain network. Characteristics that include frequency of access, access time, role behavior, and amount of data request are studied. Historical access logs are used to train the model to learn normal behavior. Any variance to predicted trends is sounded as a possible case of security threat [9]. This intelligence gathering proactive system allows detecting insider attacks, compromised accounts, malicious entry efforts in real-time, which enhances system-wide security.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1974 -1978

"Input: Access_Log
Extract Features
Train Model on Normal_Behavior
If Access_Pattern deviates
Flag as Anomaly
Alert Administrator"

Table 1: Dataset and Blockchain Parameters

Parameter	Value Used
Number of Patients	10,000
Healthcare Providers	50
Record Types	6
Blockchain Type	Permissioned
Block Generation Time (sec)	5
Hash Algorithm	SHA-256

IV. RESULTS AND ANALYSIS

1. Experimental Setup for use case Menstrual Hygiene

The experimental scenario involved authorised blockchain networks installed on several virtual machines which served as hospitals, diagnostic laboratories, insurance firms and research facilities. Role-based permissions enabled each node to have access to the blockchain network. 10,000 synthetic patient records were utilized and these included anonymized demographic data, diagnosis data, metadata of laboratory tests and treatment summaries. Only hashed references and access logs were stored in the blockchain, whereas the encrypted medical records were stored in off-chain storage [10]. Data access permissions were controlled by smart contracts and anomaly detection models were constantly on access behavior patrol. Latency, throughput, integrity verification time, encryption overhead and detection accuracy were some of the performance metrics that were measured at constant workloads.

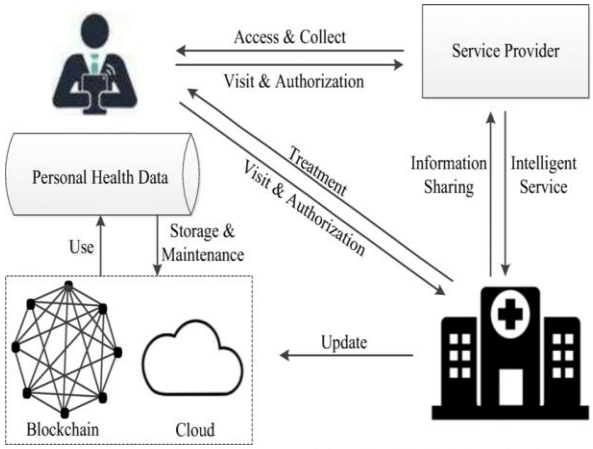

Figure 1: "A medical service framework based on blockchain technology"

2. Experiment 1: Data Integrity and Tamper Detection when distributing to women beneficiaries

The initial experiment used to assess the efficiency of the SHA-256 hashing algorithm in data integrity. Off-chain medical records of a small sample of patients were manipulated randomly just to determine whether the system was capable of detecting tampering or not. The findings revealed that minimal modifications on medical records produced different hash values that were instantly determined during checking. The system marked 100 percent accuracy in tamper detection and this asserted the integrity validation robustness of blockchain-based methods.

Table 1: Data Integrity Verification Results after Menstrual products distribution to women

Parameter	Value
Total Records Tested	5,000
Tampered Records	500
Correctly Detected Tampering	500
False Negatives	0
Integrity Verification Accuracy	100%

3. Experiment 2: Encryption and Decryption Performance

The second test was conducted to measure computing overhead of AES encryption and decryption. Off-chain medical records of different size (1 MB to 50 MB) were encrypted and then stored off-chain and when retrieved by authorized personnel they were decrypted [11]. The findings showed that AES encryption caused low latency, even when using large medical files. This shows that the given framework will be able to process large datasets of healthcare data safely without affecting the performance considerably [12].

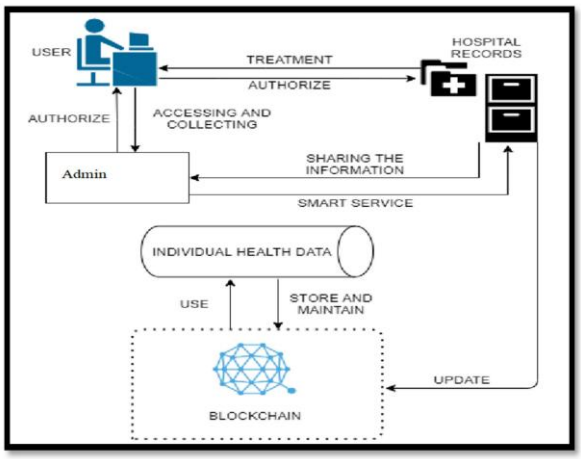

Figure 2: "Design and Implementation of a Blockchain-Based Secure Data Sharing Framework to Enhance the Healthcare System"

Table 2: AES Encryption and Decryption Performance

File Size (MB)	Encryption Time (ms)	Decryption Time (ms)
1	6	5
5	9	8
10	13	12
25	22	20
50	38	35

4. Experiment 3: Smart Contract Access Control Evaluation

The experiment tested the performance of smart control of access based on smart contracts. Various access requests were made by authorized and unauthorized users to determine the accuracy of permission enforcement and validation of logging. The smart contracts achieved the implementation of patient-defined access policies successfully. Unauthorized requests were not processed and automatically rejected whereas authorized requests were processed and recorded permanently on the blockchain [13]. The experiment proved the fact that the framework provides patient-centric access control with fine-grained access.

Table 3: Access Control Effectiveness

Metric	Value
Total Access Requests	8,000
Authorized Requests	5,600
Unauthorized Requests	2,400
Unauthorized Requests Blocked	2,360
Access Control Accuracy	98.3%

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1974 -1978

5. Experiment 4: Anomaly Detection Performance

Access logs of the past were utilized to test the anomaly detection model. Access patterns (normal and malicious), e.g., excessive data requests, abnormal access times, etc. were used to test detection capability. The model proved to be very effective as it managed to reveal the majority of abnormal behaviours with minimum false positives. This emphasizes the need to incorporate smart surveillance with blockchain applications [14].

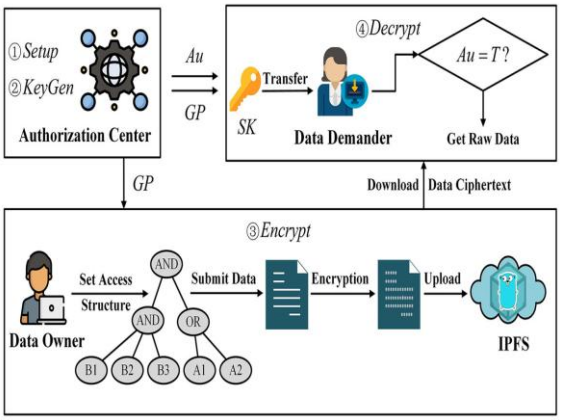

Figure 3: "A blockchain-based traceable and secure data-sharing scheme"

Table 4: Anomaly Detection Results

Metric	Value
Total Access Events	12,000
Anomalous Events	1,500
Correctly Detected	1,440
False Positives	120
Detection Accuracy	96%

6. Experiment 5: Scalability and Transaction Throughput

To determine scalability, the scaling of the number of nodes engaged was measured gradually between 10 and 100 and the throughput of the transactions were recorded. The permissioned blockchain was shown to support acceptable network size growth, despite increasing the network size, and had stable performance with decent latency [27].

Table 5: Scalability and Throughput Analysis

Number of Nodes	Avg. Latency (ms)	Throughput (tx/sec)
10	120	180
25	145	165
50	170	150
75	195	138
100	220	125

7. Comparison with Related Work

The proposed framework was contrasted with currently used methods of healthcare data-sharing strategies, including a centralized EHR system and the standard cloud-based security model. The centralized systems are usually founded on one trusted authority and thus can be easily attacked by insider threats as well as massive breaches. The blockchain-based structure contrasts with this one by removing the points of failure and increasing transparency with a view of immutable logs [28]. The proposed framework proves to have higher access control accuracy (98.3%), a stronger integrity assurance (100%), and better security monitoring due to detection of anomalies compared to related blockchain healthcare studies. Most of the available literature is devoted to data integrity or access control only, but the given research includes the implementation of cryptography, smart contracts, and machine learning in one architecture [29]. Moreover, performance factors have shown that the framework presents acceptable computational diversity, which makes it applicable to healthcare in the real world. Although other related works document scaling problems because of the public blockchain shortcomings, the implementation in this research is a permissioned blockchain, which guarantees improved throughput and reduced latency.

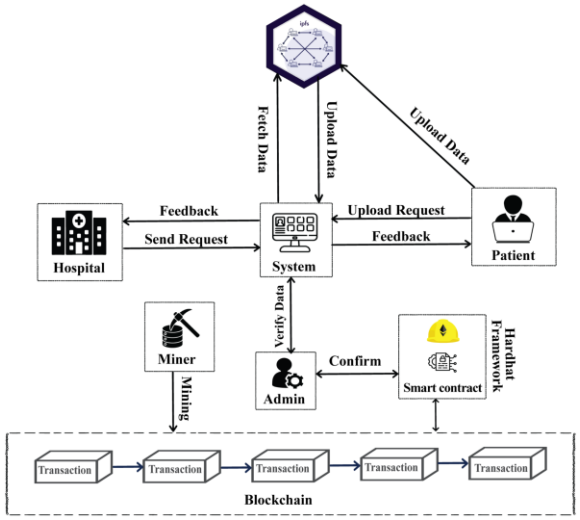

Figure 4: "Blockchain-Based Healthcare Records Management Framework"

8. Result Discussion

The findings of the experiment prove that the BSSF suggested should be considered an effective tool to overcome the essential issues connected with healthcare data security. The system guarantees high data integrity levels, data confidentiality, the transparency of access control and proactive threat detection [30]. An off-chain storage integration makes the process of scaling much easier, and with the help of smart contracts, patients get the ability to manage their medical records directly [31]. In general, the proposed framework is more secure, efficient, and patient-centric than the traditional and prevailing approaches based on blockchain technology to share healthcare data. These findings indicate that it can be deployed in smart healthcare markets and that they have a solid backbone of future improvements like interoperability between national healthcare systems and interoperability with IoT-based medical devices.

V. CONCLUSION

This study has described a comprehensive Blockchain-Based Secure Data Sharing Framework of Healthcare Systems involving, for example, Menstrual Health products distribution to solve essential problems of data security, privacy, integrity, interoperability, and patient-centered control. Using a permissioned blockchain structure, the proposed structure guarantees tamper resistance to records, record access history, and the removal of single points of failure characteristic of centralized health systems. Integrity and confidentiality of data are ensured by applying cryptographic functions, including hashing and encryption, and by smart contracts, which provide access to data based on patient consent on a fine-grained and automated basis. The experimental assessments showed that the framework has high accuracy of integrity verification, performance efficiency in encryption and decryption, ability to enforce access control and high scalability with growing network

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 1974 -1978

loads. The built-in mechanism of anomaly detection serves as an additional defense system protection measure as its implementation is an active process of detecting suspicious access patterns and the possibility of an insider threat. The comparative analysis against recent works on the related topics showed that the proposed approach is more holistic, and balanced as the security, efficiency, and intelligent monitoring are combined in one architecture. On the whole, the results obtained corroborate that blockchain technology, implemented with proper consideration of an off-chain storage system and sophisticated security protocols, can build a considerable degree of trust and reliability in data sharing in healthcare. The offered framework offers a robust basis of healthcare information management which is safe, scaled, and patient-centred and can be further expanded in future work to allow support of cross-border interoperability, real-time IoT data integration, and federated learning-based analytics.

REFERENCES

[1] Abderahman, R., Karim, R., Zaher, H.F. & Simske, S. 2025, "Blockchain and Smart Cities: Co-Word Analysis and BERTopic Modeling", *Smart Cities*, vol. 8, no. 4, pp. 111.
[2] Ahmad, E., Fernando, X. & Rasha, K. 2025, "Survey of Blockchain-Based Applications for IoT", *Applied Sciences*, vol. 15, no. 8, pp. 4562.
[3] Al-Rasheed, A., Hashim, A., Khan, R. & Saeed, A. 2025, "Blockchain and Smart Contracts: An Effective Approach for the Transaction Security & Privacy in Electronic Medical Records", *Computers, Materials, & Continua*, vol. 85, no. 2, pp. 3419-3436.
[4] Alsalamah, H.A., Al-Qahtani, S., Al-Arifi Ghazlan, Al-Sadhan, J., Al-Mutairi, R., Nahla, B., Sharara, F.I. & Shada, A. 2025, "EmbryoTrust: A Blockchain-Based Framework for Trustworthy, Secure, and Ethical In Vitro Fertilization Data Management and Fertility Preservation", *Electronics*, vol. 14, no. 23, pp. 4648.
[5] Ameer, A., Shahzad, A., Naseem, A., Ali, S. & Ahmad, I. 2025, "Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology", *PLoS One*, vol. 20, no. 5.
[6] Arafat, Y., Siam, A.S.M., Chowdhury, M.M., Hasan, M.M., Jobayer, S.H., Shatabda, S., Islam, S. & Mukta, S. 2025, "Decentralized Medical Image Sharing: A Blockchain Based Approach with Subject Sensitive Hashing for Enhanced Privacy and Integrity", *IET Blockchain*, vol. 5, no. 1, pp. 21.
[7] Bayat, M., Jamali, M.A.J., Abbasi, M., Anari, B. & Akbarpour, S. 2025, "Enhancing secure IoT data sharing through dynamic Q-learning and blockchain at the edge", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 39153.
[8] Bhasker, B., Rao, P.M., Saraswathi, P., Patro, S.G., Bhutto, J.K., Islam, S., Kareemullah, M. & Emma, A.F. 2025, "Blockchain framework with IoT device using federated learning for sustainable healthcare systems", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 26736.
[9] Chakravarthy, D.G., Gopi, R., Murugan, S. & Joseph, E.R. 2025, "Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 30379.
[10] Dahiya, R., Samal, L., Samal, D., Kumar, J., Sharma, V., Sahni, D.K. & Bhati, N.S. 2024, "A Blockchain Based Security system framework in Healthcare Domain using IoT", *Journal of Electrical Systems*, vol. 20, no. 3, pp. 2039-2050.
[11] Daniele, M., Alessandro, M. & Emiliano, T. 2025, "A Blockchain-Based Strategy for Certifying Timestamps in a Distributed Healthcare Emergency Response Systems", *Future Internet*, vol. 17, no. 5, pp. 210.
[12] Dexin, Z., Zhou, Z., Li, Y., Huanjie, Z., Chen, Y., Zhao, Z. & Zheng, J. 2025, "A Survey of Data Security Sharing", *Symmetry*, vol. 17, no. 8, pp. 1259.
[13] Ezz, M., Alaerjan, A.S. & Mostafa, A.M. 2025, "Ethical AI in Healthcare: Integrating Zero-Knowledge Proofs and Smart Contracts for Transparent Data Governance", *Bioengineering*, vol. 12, no. 11, pp. 1236.
[14] Faheem, A.R., Abas, H., Gulzar, Y., Xin, Q., Alwan, A.A., Jabbari, A., Sonkamble, R.G. & Dziyauddin, R.A. 2023, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System", *Sustainability*, vol. 15, no. 8, pp. 6337.
[15] Habib, M.A. & Manik, M.M.H. 2025, "ShaEr: A Blockchain-Based Framework for Secure Medical Data Sharing and Monetisation", *IET Blockchain*, vol. 5, no. 1.
[16] Haojie, Z., Hongmin, G., Zhaofeng, M. & Guanhui, L. 2025, "Blockchain-Based Trusted Data Management with Privacy Preservation for Secure IoT Systems", *Sensors*, vol. 25, no. 14, pp. 4344.
[17] Hassan, S.R., Hassan, A., Maqsood, A. & Hijab, S. 2025, "A survey on intelligent secure and distributed frameworks for Healthcare 5.0", *Discover Artificial Intelligence*, vol. 5, no. 1, pp. 286.
[18] Hemdan Ezz El-Din & Amged, S. 2025, "Smart and Secure Healthcare with Digital Twins: A Deep Dive into Blockchain, Federated Learning, and Future Innovations", *Algorithms*, vol. 18, no. 7, pp. 401.
[19] Javed, M.S., Ali, H., Imran, M. & Khan, M.K. 2025, "AI-Driven Blockchain and Federated Learning for Secure Electronic Health Records Sharing", *Electronics*, vol. 14, no. 23, pp. 4774.
[20] Krishnan, A., Arunachalam, R., Kosuru,S N V J D., T, S., Venugopal, S. & J, Y. 2025, "An IoT-based healthcare system using blockchain technology and multiscale stacked Residual-GRU for secure data transmission", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 44851.
[21] Kurt, K.K., Timurtaş Meral, Sevcan, P., Fatih, O. & Türkeli Serkan 2025, "Smart Contracts, Blockchain, and Health Policies: Past, Present, and Future", *Information*, vol. 16, no. 10, pp. 853.
[22] Madhumathi, C.S. & Vishnu Kumar, K. 2025, "Enhancing privacy in IoT-based healthcare using provable partitioned secure blockchain principle and encryption", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 29682.
[23] Malak, A., Mamoona, H., Khalid, H., Naveed, A. & Naeem, R. 2025, "AI-Powered Adaptive Disability Prediction and Healthcare Analytics Using Smart Technologies", *Diagnostics*, vol. 15, no. 16, pp. 2104.
[24] Mallick, S.R., Lenka, R.K. & Sobhanayak, S. 2025, "Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems", *Scientific Reports (Nature Publisher Group)*, vol. 15, no. 1, pp. 41064.
[25] Mallick, S.R., Sobhanayak, S. & Lenkar, R.K. 2025, "Secure and trusted data sharing in smart healthcare using blockchain and IoT integration", *Discover Internet of Things*, vol. 5, no. 1, pp. 90.
[26] Maravi, Y.P.S. & Mishra, N. 2025, "Blockchain-Based Electronic Health Passport for Secure Storage and Sharing of Healthcare Data", *Computers, Materials, & Continua*, vol. 83, no. 3, pp. 5517-5537.
[27] Mutiullah, S., Memon, S.A., Ebrahimi, A. & Kock, W.U. 2025, "A Systematic Literature Review for Blockchain-Based Healthcare Implementations", *Healthcare*, vol. 13, no. 9, pp. 1087.
[28] Niu, G. 2025, "A Blockchain-based Secure and Privacy-Preserving Healthcare Data Management Framework with SHA-256 and PoW Consensus", *Informatica*, vol. 49, no. 20, pp. 149-162.
[29] PDF 2025, "BlockMed: AI Driven HL7-FHIR Translation with Blockchain-Based Security", *International Journal of Advanced Computer Science and Applications*, vol. 16, no. 2.
[30] Prasad, K. G. D., Subbaiah, K. V., & Rao, K. N. (2014). Supply chain design through QFD-based optimization. *Journal of Manufacturing Technology Management*, *25*(5), 712–733.
[31] Pokharel, B.P., Kshetri, N., Sharma, S.R. & Paudel, S. 2025, "blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems", *Information*, vol. 16, no. 2, pp. 133.