Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 4, Issue 3, 2026

BLOCKCHAIN-INTEGRATED SECURE DATA MANAGEMENT ARCHITECTURE FOR FOG-EDGE NETWORKS IN HEALTHCARE MONITORING SYSTEMS

Imran Siddique[*1], Dr. Muhammad Mohsin Nazir[2]

[*1]*Department of Computer Science, Icbs-Imperial College of Business Studies, Lahore, Pakistan*
[2]*Department of Software Engineering, Lahore College for Women University*

[*1]meimransiddiqui@gmail.com, [2]mohsin.nazir@lcwu.edu.pk

DOI: https://doi.org/10.5281/zenodo.19367449

Keywords
blockchain, fog-edge computing, IoMT, healthcare monitoring, secure data management, remote patient monitoring, smart contracts, consensus protocols, privacy-preserving architecture, low-latency processing, decentralized healthcare

Article History
Received: 31 January 2026
Accepted: 14 March 2026
Published: 31 March 2026

Corresponding Author: *
Imran Siddique

Abstract

The rapid proliferation of Internet of Medical Things (IoMT) devices in remote and continuous healthcare monitoring generates massive volumes of sensitive physiological data, exposing traditional centralized cloud architectures to unacceptable latency, single points of failure, privacy breaches, and scalability limitations. This review examines the integration of blockchain technology with hierarchical fog-edge-cloud (EFC) computing as a transformative paradigm for secure, decentralized data management in healthcare systems. Blockchain provides immutable audit trails, tamper-resistant storage, transparent access control, and patient-centric data ownership through smart contracts, while fog and edge layers enable low-latency preprocessing, real-time anomaly detection, and localized decision-making for time-critical signals (ECG, EEG, vital signs). Key architectural components include lightweight consensus mechanisms (PBFT variants, PoS, G-PBFT), cryptographic primitives (ECC, SHA-256, zero-knowledge proofs), role-based access control (RBAC) enhanced by smart contracts, and hybrid off-chain/on-chain storage models to balance performance and security. The framework addresses regulatory compliance (HIPAA, GDPR), interoperability challenges, and energy constraints in resource-limited edge nodes. Case studies demonstrate reduced latency (up to 90% compared to pure cloud), enhanced privacy, and resilience against tampering and single-point failures. Future directions emphasize scalable consortium blockchains, AI-driven anomaly detection at the edge, and standardization to accelerate clinical adoption of blockchain-integrated fog-edge healthcare monitoring.

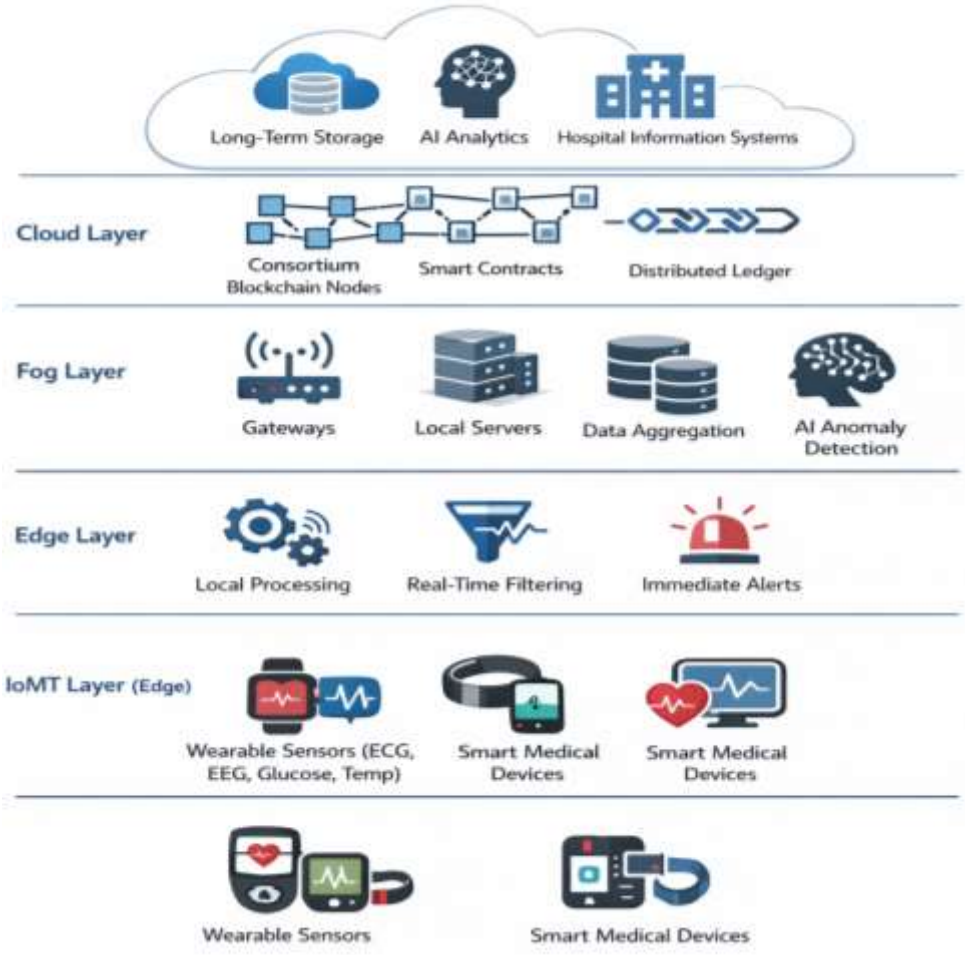
1. Introduction

The global healthcare sector is currently navigating a period of unprecedented digital transformation, characterized by the move from reactive clinical settings to proactive, continuous, and remote patient monitoring (Altman Ferreira, 2025). This transition is fundamentally underpinned by the Internet of Medical Things (IoMT), a specialized subset of the Internet of Things (IoT) that encompasses a vast array of medical devices, wearable sensors, and health-related software applications (Laouamri et al., 2025). As these devices generate an ever-increasing volume of sensitive physiological data, the requirement for robust, secure, and high-performance data management architectures has become a critical priority for healthcare providers and system designers (Aledhari et al., 2022).

Traditional data management models, which have historically relied on centralized cloud infrastructures, are increasingly recognized as inadequate for the demands of modern healthcare (Beyer, 2025). The inherent limitations of centralization specifically regarding latency, single points of failure, and the lack of transparent data ownership necessitate a paradigm shift toward decentralized architectures (Rajagopal et al., 2024).

The convergence of blockchain technology with the hierarchical edge-fog-cloud (EFC) computing paradigm offers a viable solution to these long-standing challenges. By distributing computational and storage resources across the network from the patient-facing edge to the intermediate fog layer and the high-capacity cloud it is possible to optimize performance according to the specific needs of medical data streams (Kumar et al., 2025). Blockchain serves as the immutable, decentralized ledger that provides the security, trust, and auditability required for handling confidential patient information (Jennath et al., 2020). This review article provides an exhaustive analysis of the architectures, cryptographic mechanisms, consensus protocols, and regulatory frameworks that define the current state of blockchain-integrated secure data management for fog-edge networks in healthcare monitoring systems (Yakubu et al., 2024). As shown in Figure 1, data originating from IoMT sensors is processed locally at the edge, aggregated at fog nodes, and secured through blockchain-based distributed ledgers before long-term archival and analytics in the cloud.

Figure 1: Blockchain-Integrated Fog–Edge–Cloud Architecture for Healthcare Monitoring



2. Evolution of Computing Paradigms in Healthcare Monitoring

The architectural requirements for healthcare monitoring systems are dictated by the nature of the data they process. Physiological signals, such as electrocardiograms (ECG), electroencephalograms (EEG), and real-time blood pressure metrics, are often life-critical and delay-sensitive (Serhani et al., 2020). In contrast, historical medical records and administrative data are more delay-tolerant but require high levels of long-term security and interoperability (Rajagopal et al., 2024).

2.1. Limitations of Centralized Cloud-Based Architectures

Cloud computing has served as the backbone of digital health for decades, providing the massive storage and high-intensity processing power required for medical imaging and genomic analysis (Gou et al., 2024). However, the centralization of data in distant servers creates significant bottlenecks. In high-stakes medical scenarios, such as a patient experiencing a heart attack, the time required to transmit sensor data to a cloud server, process it, and send an alert back to a clinician often referred to as round-trip time can exceed acceptable limits, potentially resulting in fatal outcomes (Wu & Gu, 2025). Furthermore, centralized repositories represent attractive targets for cyberattacks; a single breach of a central database can expose the sensitive information of millions of patients (Ngabo et al., 2021).

2.2. The Emergence of Edge and Fog Computing

To mitigate the deficiencies of the cloud, researchers and engineers have introduced the edge and fog computing layers. Edge computing shifts data processing directly to the source the medical devices and sensors themselves (Kumari et al., 2018). This layer is responsible for real-time monitoring and basic filtering, ensuring that immediate decisions can be made without network delays (Kuchuk et al., 2024). For instance, an intelligent insulin pump can adjust dosages based on immediate blood glucose readings at the edge, rather than waiting for cloud-based verification (Angel et al., 202).

Fog computing acts as a bridge between the edge and the cloud. It consists of decentralized nodes such as routers, gateways, and local servers positioned at the network's edge. These nodes possess more computational and storage capacity than edge devices, allowing them to perform more complex analytics, data aggregation, and localized storage (Hong & Varghese. 2019). This distributed approach reduces the strain on the backhaul network, lowers bandwidth costs, and enhances the overall resilience of the system by removing single points of failure (Muthanna et al., 2019).

Table 1. Characteristics of Healthcare Computing Layers

Computing Layer	Primary Function	Proximity to Source	Latency	Resource Capacity
Edge	Sensing, real-time response	Immediate	Ultra-low	Low
Fog	Aggregation, local analytics	Close	Low	Moderate
Cloud	Long-term archival, big data	Distant	High	Very High

The synergy between these layers creates a fluid environment where data is processed where it is most efficient to do so. However, distributing data across multiple nodes in an EFC environment introduces new security and privacy challenges. Each node in the fog and edge layers represents a potential entry point for attackers, and the decentralized nature of the system makes it difficult to maintain a unified security posture (Yadav, 2024).

3. Blockchain as the Secure Foundation for Decentralized Health Data

Blockchain technology provides the cryptographic framework necessary to secure data management in decentralized EFC networks. At its core, a blockchain is a distributed ledger of

transactions that is replicated across a network of nodes, ensuring that all participants have access to a consistent and tamper-proof record of data interactions (Bedogni et al., 2025).

3.1. Core Characteristics and Their Clinical Relevance

The fundamental properties of blockchain decentralization, immutability, transparency, and traceability directly address the core concerns of healthcare data management (Yaqoob et al., 2022).

- Decentralization: In a blockchain-based healthcare system, no single entity has total control over the data. This eliminates the risk of data monopolization and ensures that records remain available even if several nodes fail or are compromised (Mbanugo et al., 2020).
- Immutability: Once a medical record or transaction is recorded in a block and verified by the consensus mechanism, it cannot be altered or deleted. This provides a guarantee of data integrity, preventing unauthorized modification of patient histories (Liu et al., 2019).
- Traceability: Each block in the chain contains a cryptographic hash of the preceding block, creating a chronological and auditable record of all changes. This is vital for clinical accountability and regulatory compliance (Dwivedi et al., 2022).
- Anonymity and Privacy: While blockchains are transparent in their operation, they can use pseudonymous identifiers (public keys) to protect the identities of patients and physicians, ensuring that sensitive information is only accessible to authorized parties (Fan et al., 2018).

3.2. Blockchain Types and Their Suitability for Healthcare

The choice of blockchain type public, private, or consortium significantly impacts performance and privacy (Oh et al., 2025).

Table 2. Suitability of Blockchain Types for Healthcare

Blockchain Type	Access Control	Participant Trust	Speed/Performance	Healthcare Suitability
Public	Permissionless	Low (Trustless)	Low	Low (Privacy concerns)
Private	Permissioned (Single org)	High	High	Moderate (Centralization risk)
Consortium	Permissioned (Multi-org)	Moderate	High	High (Balanced governance)

Public blockchains are often unsuitable for raw medical data because of their low throughput and public visibility of transactions. Consortium blockchains, governed by a group of trusted organizations, are widely regarded as the most effective model for healthcare, offering a balance between high performance and robust data privacy (Patel, 2019).

4. Cryptographic Mechanisms for Fog-Edge Security

The implementation of blockchain in a fog-edge environment requires sophisticated cryptographic primitives to ensure data confidentiality while respecting resource constraints (Sellami, 2024).

4.1. Elliptic Curve Cryptography and Digital Signatures

Elliptic Curve Cryptography (ECC) has emerged as the preferred security solution for blockchain-integrated IoMT systems. ECC provides a high level of security with significantly shorter key lengths compared to traditional RSA encryption, which is critical for medical sensors with limited processing power (Savadatti et al., 2025). A 256-bit ECC key offers security strength equivalent to a 3072-bit RSA key while remaining approximately 10,000 times stronger in terms of computational resistance (Khan et al., 2020).

4.2. Hashing and the Avalanche Effect

Secure data management relies on cryptographic hash functions, most commonly SHA-256. These functions produce a unique, fixed-size output for any given input. A key property of SHA-256 is the "avalanche effect," where even a single bit change in the input data results in a radically different hash value (Niu, 2025). This property is leveraged in blockchain to link blocks together; any unauthorized attempt to alter a record would invalidate the subsequent chain, making the breach immediately apparent (Ali, 2023).

4.3. Advanced Encryption and Access Control

To ensure that sensitive data stored in the fog and cloud layers remains confidential, researchers use advanced techniques such as homomorphic encryption and Attribute-Based Access Control (ABAC) (Pu et al., 2024). Homomorphic encryption allows computational operations to be performed directly on encrypted data without first decrypting it, which enables fog nodes to perform medical analytics while physiological values remain hidden (Singh et al., 2024). ABAC allows for fine-grained access policies based on the attributes of the requesting entity, such as role, location, or time (Pu et al., 2024).

5. Architectural Frameworks for Healthcare Data Management

Several comprehensive frameworks have been developed to integrate blockchain into hierarchical EFC architectures (Oktian et al., 2020).

5.1. The EdgeLinker Framework

The EdgeLinker framework enhances security in edge-IoT communications by offloading heavy computational tasks to the fog layer (Dastani et al., 2025). It utilizes the Proof-of-Authority (PoA) consensus mechanism and integrates smart contracts on the Ethereum blockchain to automate access control. Evaluations demonstrated a 35 percent improvement in data read times compared to existing state-of-the-art blockchain solutions (Akbari Zarkesh et al., 2024).

5.2. The ESBAC Architecture

ESBAC (Efficient and Secure Blockchain-Based Access Control) is designed for Electronic Medical Record (EMR) sharing within fog-assisted IoT cloud environments (Fugkeaw et al., 2023). It uses a consortium blockchain and the InterPlanetary File System (IPFS) for storage. Heavy EMR files are stored in IPFS, while only the unique cryptographic hashes are stored on the blockchain ledger to prevent the chain from becoming bloated (Sujitha et al., 2024).

5.3. The SCR-BAC Model

The SCR-BAC model integrates blockchain with risk-adaptive access control (RAdAC). It quantifies the risk of granting access in real-time based on both a doctor's current behavior and their historical record (West et al., 2016). The risk is quantified using a formula that incorporates a time decay factor, ensuring that past malicious actions negatively impact a user's risk score for a period (Albahri et al., 2018).

5.4. The EGBUH Framework

The EGBUH (Edge-Gateways Based Ubiquitous Healthcare) framework focuses on reliable, access-controlled healthcare while ensuring the anonymity of data producers. It leverages blockchain at edge gateways to provide tamper-proof analytics closer to the patient, using resource-efficient neural networks for real-time classification of conditions such as arrhythmia (Sindhushree et al., 2025).

6. Consensus Mechanisms in Resource-Constrained Environments

The consensus mechanism ensures that all nodes agree on the state of the ledger. However, traditional mechanisms like Proof of Work (PoW) require massive computational resources and generate high latency, making them unsuitable for real-time healthcare (Nguyen et al., 2019).

Table 3. Comparison of Blockchain Consensus Mechanisms

Consensus Mechanism	Fault Tolerance	Scalability	Efficiency	Throughput	Suitability
PoW	High	Moderate	Very Low	Low	Low
PBFT	One-third of nodes	Low	High	High	High
PoA	Authority-based	High	Very High	Very High	High

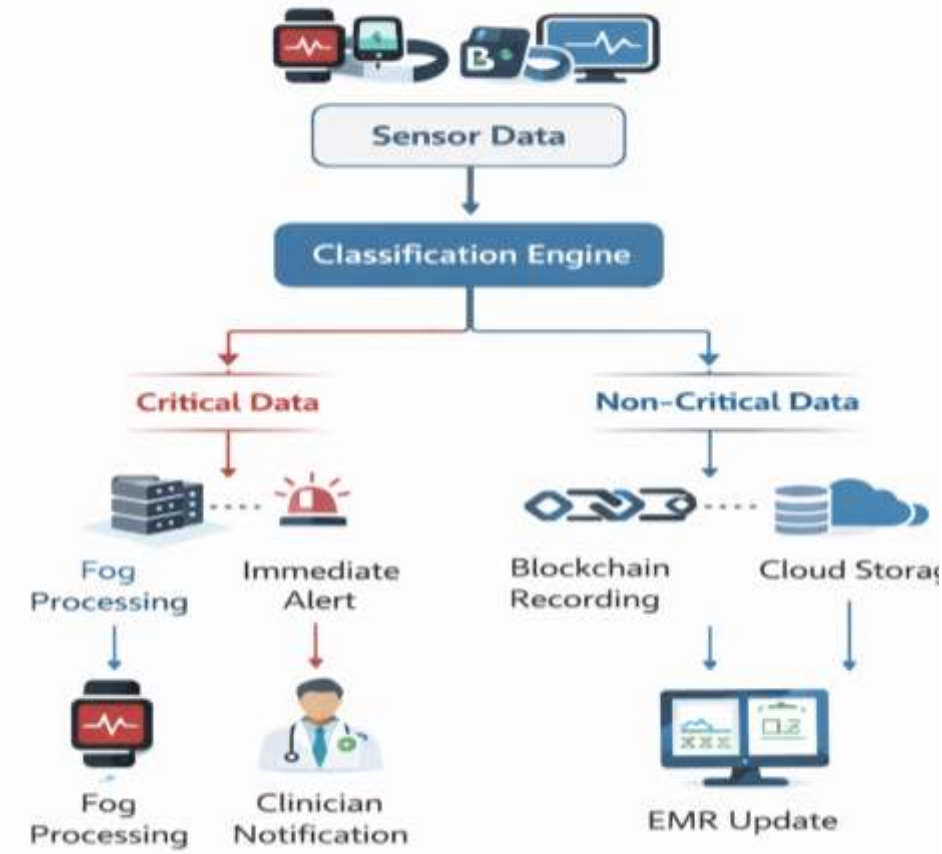
Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) have emerged as more efficient alternatives for permissioned healthcare networks. PBFT is effective for high transaction throughput but can struggle with scalability as the number of nodes increases due to communication overhead (Lao et al., 2020). To overcome this, reputation-integrated mechanisms like BR-PBFT use reputation scoring systems to select the most reliable nodes for consensus, significantly improving CPU and memory efficiency (Yuan et al., 2025).

7. Data Management Logic: Message Classification and Tiered Processing

A sophisticated architecture must differentiate between medical data types to ensure critical information is prioritized (Abu-Elkheir et al., 2013). In tiered architectures, the fog layer is logically divided into critical and non-critical clusters. Critical messages, such as alerts for heart rate anomalies (greater than 150 beats per minute) or temperature spikes (greater than 102 degrees Fahrenheit), are prioritized and processed at the fog layer for near-instantaneous response (Dhayne et al., 2019). Non-critical messages, which include routine health updates, are delay-tolerant and are managed using blockchain technology to ensure long-term privacy and immutability (Ngabo et al., 2021). As illustrated in Figure 2, critical physiological signals are prioritized for immediate fog-level processing, whereas non-critical data is securely archived through blockchain and cloud systems.

8. Performance Metrics and Empirical Evaluation Results

Figure 2: Tiered Healthcare Data Processing in Fog–Edge Networks



The validation of blockchain-integrated EFC architectures involves analyzing diagnostic accuracy and network performance.

8.1. Model Classification Accuracy

For systems incorporating machine learning, performance is measured against expert identification. Results from integrated IoT-fog-blockchain systems show diagnostic accuracy reaching approximately 96.6 percent, with precision rates often hitting 100 percent after system tune-ups (Laouamri et al., 2025).

Table 4. System Diagnostic Performance Metrics

Performance Actor	Before System Tune-up	After System Tune-up	Average Performance
Precision	100 percent	100 percent	100 percent
Recall	96.3 percent	97.0 percent	96.7 percent
Accuracy	96.3 percent	97.0 percent	96.6 percent

8.2. Network System Performance

In terms of network efficiency, time-based metrics are primary success indicators.

- Response Time: At the edge, response times as low as 650 milliseconds have been reported.

- Latency: In fog environments, a delay of only 1 millisecond has been recorded for up to 100 concurrent users.
- Energy Consumption: Edge computing consumes significantly less energy (approximately 63.75 watts) compared to cloud-based alternatives (approximately 548 watts) (Jaddoa, 2022).

9. Interoperability and Scalability Challenges

Scalability is often cited as the primary drawback of early blockchain implementations. To address this, current research focuses on the use of sidechains and node clustering. By implementing sidechains, a system can offload specific transactions from the main blockchain, reducing congestion (Ramzi, 2025).

Interoperability is further enhanced through Federated Learning (FL). In a FedBLOC architecture, machine learning models are trained locally at hospitals, and only model parameters not raw patient data are transmitted to the blockchain. This approach ensures both data privacy and cross-institutional interoperability (Rajagopal et al., 2024).

10. Regulatory Compliance and Ethical Governance

The deployment of these networks must navigate regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Yakubu et al., 2024). A significant challenge is the multi-jurisdictional nature of fog computing, where nodes in different countries may be subject to conflicting privacy laws (Yadav, 2024). Furthermore, the GDPR's right to be forgotten presents a technical challenge for the immutable nature of blockchain; solutions include storing patient data off-chain in systems like IPFS so that it can be deleted while the audit trail remains intact (Singh et al., 2024).

11. Future Directions and Strategic Synthesis

The field is evolving toward quantum-secure communication and 5G/6G network slicing to handle massive IoMT deployments. The integration of blockchain technology within hierarchical fog-edge networks represents the most viable path forward for modern healthcare (Beyer, 2025; Sindhushree et al., 2025). By leveraging the cryptographic strength of ECC and the automated governance of smart contracts, healthcare providers can ensure the absolute integrity and confidentiality of patient data (Ngabo et al., 2021).

The transition from reactive to proactive care through blockchain-integrated architectures will ultimately depend on continued collaboration between technologists and policymakers to build a secure foundation for the future of global medicine (Kumar et al., 2025).

Conclusion

The convergence of blockchain with fog-edge-cloud architectures offers a compelling solution to the inherent vulnerabilities of centralized systems in IoMT-based healthcare monitoring, delivering the essential triad of security, privacy, low latency, and scalability demanded by continuous physiological data streams. By decentralizing trust through immutable ledgers and smart contracts, distributing computation across edge and fog nodes for real-time responsiveness, and enforcing fine-grained, patient-controlled access, this paradigm fundamentally redefines secure data management in digital health. Despite remaining challenges computational overhead of consensus, energy efficiency at resource-constrained edges, interoperability across heterogeneous devices, and regulatory harmonization the demonstrated reductions in latency, improved tamper resistance, and enhanced auditability position blockchain-integrated EFC frameworks as foundational for next-generation healthcare systems. Sustained progress in lightweight protocols, hybrid storage designs, and cross-domain standardization will be critical to translate these architectures from research prototypes into widespread clinical deployment, ultimately enabling safer, more equitable, and truly patient-centric remote monitoring ecosystems in an increasingly connected medical landscape.

12. REFERENCES

Akbari Zarkesh, M., Dastani, E., Safaei, B., & Movaghar, A. (2024). EdgeLinker: Practical blockchain-based framework for healthcare fog applications to enhance security in edge-IoT data communications. Proceedings of the 5th CPSSI International Symposium on Cyber-Physical Systems (Applications and Theory), 1–8. https://doi.org/10.1109/CPSAT64082.2024.10745419

Beyer, A. (2025). Enhancing healthcare workflows with blockchain-enabled deep reinforcement learning and mobile-fog-cloud architecture. In Advanced Smart Healthcare Systems (pp. 215–240). Springer. https://doi.org/10.1007/978-3-030-31978-6_12

Kumar, N., Jaiprakash, S. P., & Prakash, C. S. (2025). Introduction to cloud, fog, and edge computing in healthcare. In Cloud, Fog, and Edge Computing in Healthcare (pp. 1–25). Springer.

Laouamri, A., Cherbal, S., Mosbah, Y., Benrebbouh, C., & Kharoubi, K. (2025). Blockchain approach for healthcare using fog topology and lightweight consensus. Acta Informatica Pragensia, 14(1), 128–154. https://doi.org/10.18267/j.aip.256

Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of Internet of Things. Electronics, 10(17), 2110. https://doi.org/10.3390/electronics10172110

Pu, X., Jiang, R., Song, Z., Liang, Z., & Yang, L. (2024). A medical big data access control model based on smart contracts and risk in the blockchain environment. Frontiers in Public Health, 12, 1358184. https://doi.org/10.3389/fpubh.2024.1358184

Rajagopal, S. M., M., S., & Buyya, R. (2024). Blockchain integrated federated learning in edge-fog-cloud systems for IoT based healthcare applications: A survey (arXiv:2406.05517). arXiv. https://doi.org/10.48550/arXiv.2406.05517

Ramzi, A. (2025). A scalable and secure model for fog and cloud computing in healthcare systems that depend on sidechains and the clustering of the available fog nodes. Informatica, 49(1). https://doi.org/10.31449/inf.v49i1.5580

Sindhushree, M. A. P. M., P., G., R., A., P., G., P., J., & S., S. (2025). Experimental evaluation of an IoT powered healthcare monitoring scheme based on blockchain technology assistance. Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25), 4, 328–337. https://doi.org/10.5220/0013912400004919

Singh, S., Bhatt, P., Kandasamy, N., & Singh, N. P. (2024). Efficient and secure blockchain-based access control for fog-assisted IoT cloud in electronic medical records sharing. Journal of Electrical Systems, 20(1s), 138–151.

Sora-Cardenas, L., Dwivedi, A. D., & Sharma, G. (2025). Enhancing healthcare consensus mechanism - A reputation integrated variant of PBFT (BR-PBFT). Journal of Information Security.

Yadav, S. (2024). Challenges with fog computing in healthcare: Regulatory and security perspectives. Journal of Public Health, 15(3), 412–425.

Altman Ferreira, P. S. (2025). Managing operational resilience during the implementation of digital transformation in healthcare organisational practices. Journal of Health Organization and Management, 39(3), 334-358.

Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: enabling technologies, architectural elements, challenges, and future directions. IEEE Access, 10, 31306-31339.

Yakubu, M. M., Hassan, F. B., Danyaro, K. U., Junejo, A. Z., Siraj, M., Yahaya, S., ... & Abdulsalam, K. (2024). A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges. Computer Systems Science & Engineering, 48(6).

Serhani, M. A., T. El Kassabi, H., Ismail, H., & Nujum Navaz, A. (2020). ECG monitoring systems: Review, architecture, processes, and key challenges. Sensors, 20(6), 1796.

Jennath, H. S., Anoop, V. S., & Asharaf, S. (2020). Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence.

Gou, F., Liu, J., Xiao, C., & Wu, J. (2024). Research on artificial-intelligence-assisted medicine: a survey on medical artificial intelligence. Diagnostics, 14(14), 1472.

Wu, J., & Gu, N. (2025). New orientation of interdisciplinarity in medicine: engineering medicine. Engineering, 45, 252-261.

Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for Healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering, 72, 1-13.

Kuchuk, H., & Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: a review. Advanced Information Systems, 8(2), 65-78.

Angel, N. A., Ravindran, D., Vincent, P. D. R., Srinivasan, K., & Hu, Y. C. (2021). Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies. Sensors, 22(1), 196.

Hong, C. H., & Varghese, B. (2019). Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms. ACM computing surveys (csur), 52(5), 1-37.

Muthanna, A., A. Ateya, A., Khakimov, A., Gudkova, I., Abuarqoub, A., Samouylov, K., & Koucheryavy, A. (2019). Secure and reliable IoT networks using fog computing with software-defined networking and blockchain. Journal of Sensor and Actuator Networks, 8(1), 15.

Bedogni, L., Mamei, M., Picone, M., Pietri, M., & Zambonelli, F. (2025). Fluid Computing & Digital Twins for intelligent interoperability in the IoT ecosystem. Future Generation Computer Systems, 171, 107855.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 34(14), 11475-11490.

Mbanugo, O. J., Taylor, A., & Sneha, S. (2025). Buttressing the power of entity relationships model in database structure and information visualization: Insights from the Technology Association of Georgia's Digital Health Ecosystem. World J Adv Res Rev, 25(02), 1294-1313.

Liu, X., Wang, Z., Jin, C., Li, F., & Li, G. (2019). A blockchain-based medical data sharing and protection scheme. IEEE Access, 7, 118943-118953.

Dwivedi, S. K., Amin, R., Lazarus, J. D., & Pandi, V. (2022). Blockchain-Based Electronic Medical Records System with Smart Contract and Consensus Algorithm in Cloud Environment. Security and Communication Networks, 2022(1), 4645585.

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. Journal of medical systems, 42(8), 136.

Oh, L. K., & Sukmana, H. T. (2025). A comprehensive study on public and private blockchain performance. Journal of Current Research in Blockchain, 2(1), 13-27.

Patel, V. (2019). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. Health informatics journal, 25(4), 1398-1411.

Sellami, Y. (2024). Secure data management in an IoT-Fog/Edge computing architecture (Doctoral dissertation, Université Polytechnique Hauts-de-France; Institut national des sciences appliquées Hauts-de-France).

Savadatti, S. G., Dhariwal, S. K., Krishnamoorthy, S., & Delhibabu, R. (2025, January). Analyzing RSA, AES, and ECC Across 13 Critical Factors in the Healthcare Domain. In 2025 International Conference on Next Generation Communication & Information Processing (INCIP) (pp. 593-598). IEEE.

Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEe Access, 8, 52018-52027.

Niu, G. (2025). A Blockchain-based Secure and Privacy-Preserving Healthcare Data Management Framework with SHA-256 and PoW Consensus. Informatica, 49(20).

Ali, A. Z. M. (2023). The Power of Cryptography: Hashing and Encryption for Data Protection. J Artif Intell Mach Learn & Data Sci, 1(1), 1857-1861.

Oktian, Y. E., Lee, S. G., & Lee, H. J. (2020). Hierarchical multi-blockchain architecture for scalable internet of things environment. Electronics, 9(6), 1050.

Dastani, E., Zarkesh, M. A., Davoodzadeh, M., Safaei, B., & Movaghar, A. (2025). Blockchain-Based IoT Framework with In-Depth Security Analysis and Performance Benchmarks for Real-World Healthcare Fog Applications. Scientia Iranica, (Articles in Press).

Fugkeaw, S., Wirz, L., & Hak, L. (2023). Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing. IEEE access, 11, 62998-63012.

Sujitha, S. J., & Selvi, P. T. (2024, May). Ensuring access control reliability and security of lightweight blockchain-based iot cloud-based electronic medical records sharing. In 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI) (pp. 1-5). IEEE.

West, P., Giordano, R., Van Kleek, M., & Shadbolt, N. (2016, May). The quantified patient in the doctor's office: Challenges & opportunities. In Proceedings of the 2016 chi conference on human factors in computing systems (pp. 3066-3078).

Albahri, O. S., Zaidan, A. A., Zaidan, B. B., Hashim, M., Albahri, A. S., & Alsalem, M. A. (2018). Real-time remote health-monitoring Systems in a Medical Centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects. Journal of medical systems, 42(9), 164.

Lao, L., Dai, X., Xiao, B., & Guo, S. (2020, May). G-PBFT: A location-based and scalable consensus protocol for IoT-blockchain applications. In 2020 IEEE international parallel and distributed processing symposium (IPDPS) (pp. 664-673). IEEE.

Yuan, F., Huang, X., Zheng, L., Wang, L., Wang, Y., Yan, X., ... & Peng, Y. (2025). The evolution and optimization strategies of a PBFT consensus algorithm for consortium blockchains. Information, 16(4), 268.

Abu-Elkheir, M., Hayajneh, M., & Ali, N. A. (2013). Data management for the internet of things: Design primitives and solution. Sensors, 13(11), 15582-15612.

Dhayne, H., Haque, R., Kilany, R., & Taher, Y. (2019). In search of big medical data integration solutions-a comprehensive survey. IEEE Access, 7, 91265-91290.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE access, 7, 85727-85745.

Jaddoa, A. (2022). Multi-criteria decision support for energy-efficient IoT edge computing offloading (Doctoral dissertation, University of Greenwich).