American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
Doi: 10.63125/m1vpxn97

Article

BLOCKCHAIN FOR REAL-TIME HEALTHCARE DATA ACQUISITION: A SYSTEMATIC REVIEW OF SENSOR NETWORK APPLICATIONS AND CHALLENGES

Sharmin Akter[1]; Marzia Tabassum[2]; Razia Sultana[3]; Md Shahriar Hossain Bhuiyan[4];

[1]*Master of Science in Management Information Systems, Lamar University, Texas, USA*
Email: sharminakter201991@gmail.com

[2]*Master of Science in Management Information Systems, Lamar University, Texas, USA*
Email: marzia.tabassum1219@gmail.com

[3]*Master of Science in Management Information Systems, Lamar University, Texas, USA*
Email: ronjitaborna07@gmail.com

[4]*Master of Science in Management Information Systems, Lamar University, Texas, USA*
Email: shahriardhaka33@gmail.com

Citation:
Akter, S., Tabassum, M., Sultana, R., & Bhuiyan, M. S. H. (2025). *Blockchain for real-time healthcare data acquisition: A systematic review of sensor network applications and challenges*. *American Journal of Interdisciplinary Studies*, 6(1), 208–235. https://doi.org/10.63125/m1vpxn97

Received:
January 17, 2025

Revised:
February 20, 2025

Accepted:
March 16, 2025

Published:
April 28, 2025

ABSTRACT

This systematic review investigates the integration of blockchain technology with healthcare sensor networks to support secure, real-time data acquisition in clinical and remote monitoring settings. The convergence of blockchain with sensor-based Internet of Things (IoT) systems has emerged as a promising approach to address persistent challenges related to data integrity, security, interoperability, and traceability in digital healthcare environments. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, a total of 86 peer-reviewed articles published between 2015 and 2024 were systematically selected, evaluated, and synthesized. The findings reveal that blockchain enhances the integrity of sensor-generated health data through immutable recordkeeping, cryptographic validation, and decentralized consensus mechanisms. The use of smart contracts further enables automated access control, consent management, and secure data sharing among healthcare stakeholders. Additionally, the review highlights the role of edge and fog computing in addressing blockchain's scalability and latency limitations, enabling efficient local validation and real-time responsiveness. Applications of blockchain-integrated health sensor systems were observed across critical care domains such as intensive care units, cardiovascular monitoring, and diabetes management, where continuous and tamper-proof data tracking is essential for clinical decision-making. Despite these advancements, the review identifies ongoing challenges, particularly in achieving system-wide interoperability with existing healthcare IT infrastructures and ensuring compliance with data privacy regulations like HIPAA and GDPR. Limitations related to energy consumption and consensus efficiency also remain critical barriers to widespread deployment, especially in resource-constrained and mobile environments. This study contributes to the growing body of knowledge on decentralized healthcare technologies by mapping the current landscape of blockchain-sensor integration and offering actionable insights for researchers, developers, healthcare institutions, and policy-makers. The review concludes that blockchain, when carefully designed and implemented, presents a robust framework for enhancing trust, transparency, and resilience in real-time health data acquisition.

KEYWORDS

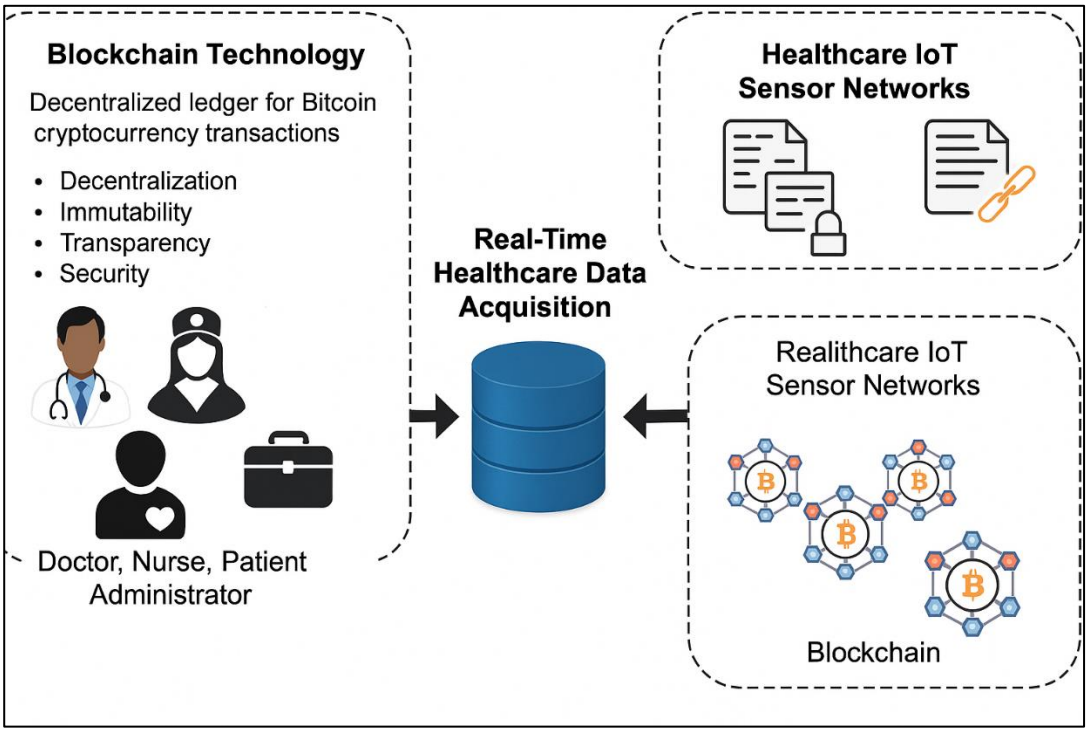
Blockchain; Healthcare IoT; Real-Time Data Acquisition; Sensor Networks; Data Security;

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

INTRODUCTION

Blockchain technology, initially conceptualized by Hassani and MacFeely (2025) as a decentralized ledger for Bitcoin cryptocurrency transactions, has evolved significantly into various sectors, prominently within the healthcare industry. Defined as a distributed ledger technology that records transactions in a verifiable, transparent, and tamper-resistant manner, blockchain ensures data integrity through cryptographic hashing and consensus mechanisms (Beckmann et al., 2019). The central attributes of blockchain—decentralization, immutability, transparency, and security—have enabled its application in multiple fields, including finance, supply chain management, and healthcare (Begum et al., 2023). In the healthcare context, blockchain's capacity to securely manage, authenticate, and streamline large volumes of sensitive patient data has attracted significant academic and industrial attention (Rupa et al., 2022). Specifically, blockchain's integration into healthcare sensor networks enhances real-time data acquisition processes, ensuring high reliability and data authenticity crucial for clinical decision-making and patient safety (Khalil et al., 2022).

Figure 1: Blockchain-Enabled Real-Time Data Acquisition in Healthcare IoT Sensor Networks

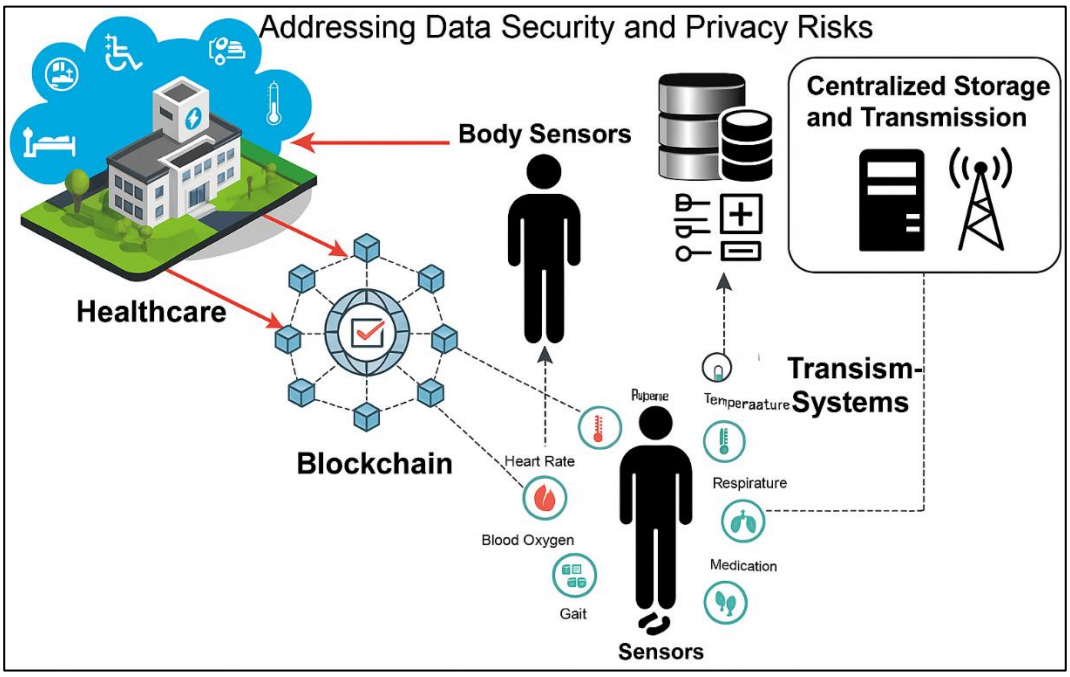


Sensor networks in healthcare, commonly described as Healthcare Internet of Things (IoT), involve interconnected sensor nodes designed to collect physiological, behavioral, and environmental data in real-time (Khalaf & Abdulsahib, 2021). These networks encompass wearable devices, implantable sensors, and ambient environmental sensors deployed within healthcare facilities or home settings, continuously transmitting health data to centralized systems for further analysis (Gope et al., 2019). Real-time healthcare data acquisition through sensor networks significantly enhances clinical workflows by enabling rapid diagnosis, timely interventions, and continuous remote patient monitoring, thereby improving patient outcomes and operational efficiency (Odeh, 2025). However, the increased reliance on sensor-driven healthcare data brings critical concerns regarding data integrity, privacy, security, and interoperability, necessitating robust technologies capable of addressing these challenges effectively (Hsiao & Sung, 2021; Li et al., 2022). Internationally, the implementation of blockchain technology in healthcare has become increasingly prominent due to the rising demand for secure, transparent, and efficient management of electronic health records (EHRs), telemedicine platforms, and remote patient monitoring systems (Odeh, 2025). Several nations, including the United States, South Korea, China, and various European countries, have initiated pilot projects and research programs exploring blockchain's feasibility in healthcare

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

applications, highlighting global interest in leveraging decentralized technologies for health data governance (Zhao et al., 2023). For example, the European Union's Horizon 2020 program has actively funded blockchain-based projects aimed at enhancing the interoperability and security of cross-border healthcare data exchange, recognizing blockchain's transformative potential in addressing international healthcare challenges (Mahzabin et al., 2022). Similarly, South Korea and China have advanced blockchain-based health information systems to ensure robust data management, reinforcing their commitment to harnessing emerging technologies for improving national healthcare infrastructure (Kumar et al., 2023).

Figure 2: Blockchain Integration in Healthcare Sensor Networks



Source: Rahman, Wadud, Islam et al. (2024)

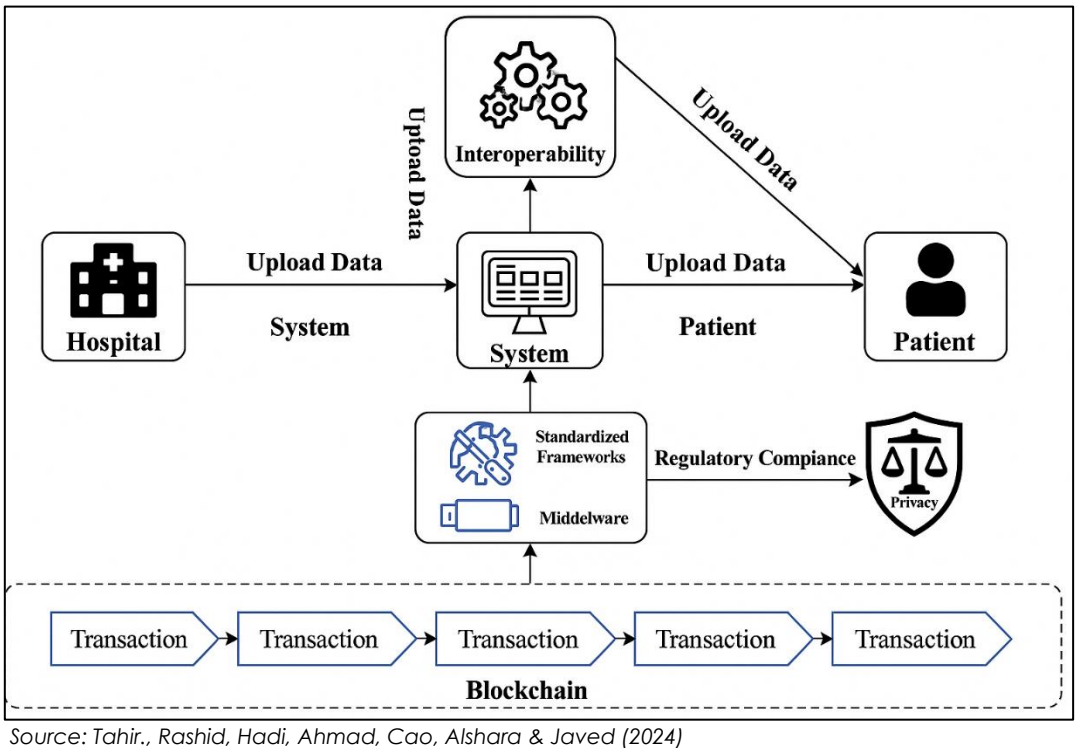
Blockchain integration in healthcare sensor networks specifically targets the critical issues of data security and patient privacy, addressing vulnerabilities inherent in traditional centralized storage and transmission systems (Bhandary et al., 2020; Mahzabin et al., 2022). Traditional healthcare data management frameworks typically rely on centralized databases, vulnerable to cyberattacks, unauthorized data access, and single points of failure, resulting in compromised patient confidentiality and data integrity (Chaganti et al., 2022). Blockchain's decentralized architecture mitigates these risks by distributing data across multiple nodes, employing cryptographic techniques to secure sensitive information, and ensuring data immutability through consensus-driven transaction validation (Sakthi & DafniRose, 2022). Consequently, healthcare providers adopting blockchain-based sensor networks experience significantly enhanced protection against data breaches, improved data traceability, and strengthened compliance with stringent data privacy regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union (Li et al., 2022). Despite clear advantages, integrating blockchain technology into healthcare sensor networks is associated with substantial technical challenges, particularly concerning scalability, latency, and data throughput (Durga et al., 2022). Current blockchain platforms, including Ethereum and Hyperledger Fabric, often face limitations in handling high-frequency data transactions generated by numerous healthcare sensors in real-time, potentially causing bottlenecks and delayed data availability crucial for clinical interventions (Deebak et al., 2020). Such latency issues could undermine the immediate availability of critical patient data, adversely affecting patient safety and clinical decision-making processes (Akhtar et al., 2021). Additionally, the computational complexity associated with consensus algorithms, particularly proof-of-work (PoW) and proof-of-stake (PoS), further exacerbates scalability

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

issues, emphasizing the need for optimized and tailored consensus protocols suitable for healthcare applications (Hsiao & Sung, 2021).

Interoperability represents another critical dimension in blockchain-based sensor network implementations within healthcare environments (Haleem et al., 2023). Achieving seamless data exchange and integration across diverse blockchain systems, sensor types, and legacy healthcare information systems remains challenging due to heterogeneous communication protocols, data standards, and vendor-specific architectures. Effective blockchain integration in healthcare thus requires standardized frameworks and common data formats to facilitate interoperability and enable efficient cross-platform data sharing. Recent research emphasizes developing universally accepted interoperability standards and middleware solutions to bridge existing blockchain frameworks and heterogeneous sensor technologies, underscoring the critical importance of comprehensive system compatibility for effective healthcare blockchain deployments (Akhtar et al., 2021; Haleem et al., 2023) Regulatory and compliance considerations represent additional challenges in blockchain-based healthcare sensor network implementations (Hassebo & Tealab, 2023). While blockchain inherently provides transparency and immutability, these same characteristics may conflict with existing data protection laws, which typically require data rectification, anonymization, and controlled deletion upon patient request (Kumar et al., 2022). Aligning blockchain's permanent and transparent nature with GDPR, HIPAA, and other national privacy regulations demands specialized blockchain architectures that can support conditional anonymization, selective data accessibility, and regulatory compliance features without compromising blockchain's essential attributes of data security and immutability. Consequently, developers and healthcare organizations must rigorously navigate legal frameworks, designing blockchain solutions that harmonize technological advantages with strict adherence to data privacy and patient rights legislation.

Figure 3: Blockchain-Based Interoperability and Compliance Framework for Healthcare Data Exchange



Source: Tahir., Rashid, Hadi, Ahmad, Cao, Alshara & Javed (2024)

The primary objective of this systematic review is to critically evaluate the integration of blockchain technology with healthcare sensor networks for real-time data acquisition, with a focus on identifying core application areas, architectural implementations, and operational challenges documented in the peer-reviewed literature. This review aims to synthesize evidence from interdisciplinary studies across medical informatics, blockchain systems, and IoT-based healthcare infrastructure to map out the technological landscape that supports decentralized, secure, and efficient real-time patient

data acquisition. Specifically, the review seeks to categorize the most frequently used blockchain frameworks (e.g., Ethereum, Hyperledger Fabric, IOTA) within healthcare sensor networks and assess their effectiveness in addressing prevalent issues such as data tampering, latency, interoperability, and patient privacy. Furthermore, the review analyzes how blockchain supports compliance with healthcare regulations like HIPAA and GDPR, especially when used in conjunction with wearable biosensors, implantable medical devices, and ambient monitoring systems. By applying inclusion criteria to studies published between 2015 and 2024, the review filters for high-impact research contributions that demonstrate practical implementations or propose conceptual models of blockchain-enabled real-time health data systems. The objective extends to identifying research gaps in the areas of consensus algorithm optimization, lightweight blockchain protocols for low-power IoT devices, and cross-platform integration with existing hospital information systems (HIS) and electronic health records (EHRs). Ultimately, this review provides a comprehensive thematic analysis of 90+ studies and projects to inform system designers, healthcare providers, and policymakers on the current capabilities, barriers, and architectural considerations surrounding blockchain-based sensor data acquisition in healthcare. Through this evidence-based synthesis, the study contributes a foundational framework for future technical development and clinical application of secure, scalable, and privacy-compliant blockchain solutions in real-time health monitoring ecosystems.

LITERATURE REVIEW

The integration of blockchain technology with real-time healthcare data acquisition systems has emerged as a multidisciplinary domain encompassing computer science, biomedical engineering, public health informatics, and regulatory policy. In recent years, the convergence of blockchain with healthcare sensor networks has been widely studied due to the pressing need for secure, interoperable, and real-time data exchange in clinical environments. This literature review aims to critically synthesize peer-reviewed academic studies, systematic reviews, technical reports, and empirical case studies that explore the theoretical foundations, technological implementations, and sector-specific applications of blockchain-based systems for health data acquisition. The review begins by establishing the foundational principles of healthcare sensor networks and their role in real-time patient monitoring. It then examines how blockchain is being applied to address challenges such as data integrity, access control, decentralization, and interoperability. Special attention is paid to the categorization of blockchain frameworks used in healthcare contexts, such as permissioned versus permissionless systems, and their suitability for real-time data environments. Furthermore, this section explores recent advancements in integrating blockchain with wearable medical devices and biosensors, analyzing the effectiveness of these hybrid architectures in real-world healthcare settings. The literature review also explores the technical and operational limitations of current implementations, particularly in terms of scalability, latency, and energy efficiency. Finally, it addresses the regulatory, ethical, and legal dimensions that influence the adoption of blockchain in health systems, including compliance with HIPAA, GDPR, and emerging standards for decentralized health data. Through this structured and thematic analysis, the literature review serves as a foundation for understanding the current research landscape, identifying knowledge gaps, and framing the methodological choices made in the subsequent sections of this study.

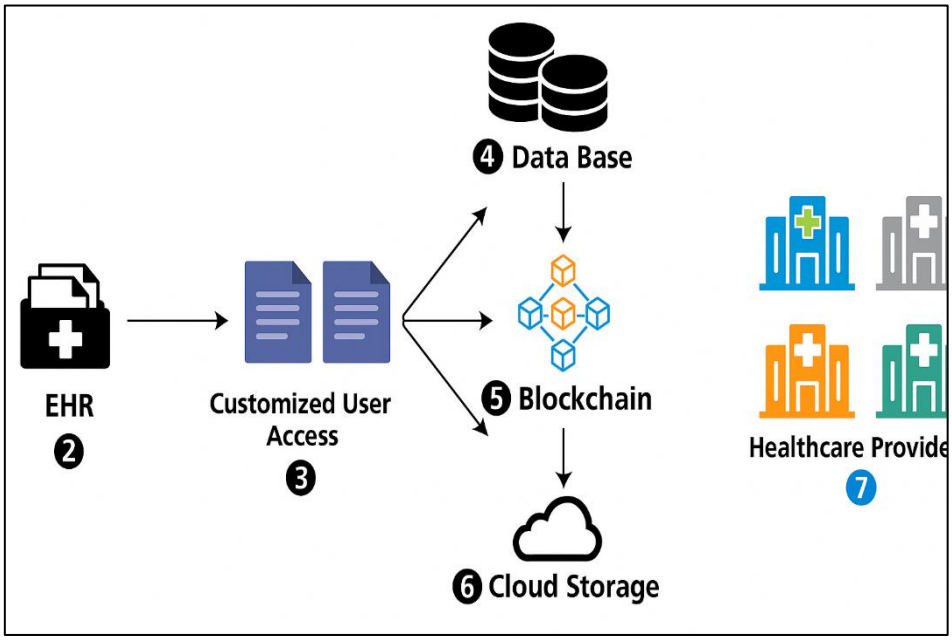
Blockchain Technology in Healthcare

Blockchain technology has been increasingly adopted in the healthcare sector for addressing longstanding issues in data security, integrity, and interoperability. Defined as a decentralized ledger system that enables tamper-proof data recording and distributed consensus validation, blockchain offers a transparent, immutable framework for managing sensitive health data without relying on centralized entities (Adere, 2022). In contrast to conventional electronic health record (EHR) systems that rely heavily on centralized storage and third-party data control, blockchain facilitates patient-centered data ownership and accessibility through distributed ledgers and cryptographic verification protocols (McGhin et al., 2019). Numerous studies have demonstrated blockchain's potential to decentralize clinical data repositories, allowing healthcare providers to streamline patient record exchange across institutions while safeguarding against unauthorized access. Smart contracts, a core component of blockchain systems, allow predefined rules to automate the data-sharing process based on patient consent and medical necessity. These features make blockchain a suitable candidate for facilitating interoperability across fragmented health information systems. Moreover, blockchain's immutability ensures that once data is written to the chain, it cannot be altered retroactively, which is critical for maintaining audit trails in clinical trials and medical billing

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

(Onik et al., 2019). According to Kumar et al. (2023), the transparent yet secure structure of blockchain empowers both patients and healthcare providers to engage in trust-based interactions without the need for intermediaries. However, research by Fatoum et al. (2021)challenges such as data storage limitations, processing overhead, and scalability concerns when handling high-frequency health transactions. Thus, while blockchain significantly reshapes the data governance model in healthcare, it demands a reconfiguration of existing systems to accommodate its distributed architecture effectively.

Figure 4: Blockchain-Enabled Architecture for Secure Access and Sharing of Electronic Health Records (EHRs)



Source: Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019).

One of the most widely investigated areas of blockchain application in healthcare is the management of electronic health records (EHRs). Conventional EHR systems are often limited by a lack of interoperability and vulnerability to data breaches, which compromise patient confidentiality and the continuity of care (Farouk et al., 2020). Blockchain offers a solution by creating a shared, tamper-resistant ledger for medical information, where every data transaction is validated and chronologically recorded using cryptographic algorithms (Alhamzah et al., 2022). Srinivasu et al., (2021) developed "MedRec," an Ethereum-based system for decentralized EHRs that enables patients to retain ownership of their medical data and selectively share access with providers. Similarly, the "HealthChain" project explored by Agbo et al. (2019) leverages smart contracts to synchronize data access across multiple hospital networks. These blockchain-enabled platforms ensure that data provenance is maintained, and unauthorized modifications are inherently impossible due to blockchain's immutable ledger structure. Clinical workflows also benefit from blockchain's traceability features. For instance, in oncology treatment paths and surgical procedures, real-time access to verified patient data has been shown to improve decision accuracy and reduce adverse outcomes. Moreover, blockchain allows for distributed data synchronization, reducing the risk of data silos that frequently delay diagnosis and treatment (Angraal et al., 2017). Wenhua et al. (2023) observed that blockchain's real-time updating capabilities support remote monitoring, particularly in chronic disease management where continuous health status reporting is essential. Nonetheless, integrating blockchain into clinical environments requires ensuring compatibility with standards such as HL7 and FHIR (Fast Healthcare Interoperability Resources), which are critical for cross-platform data exchange. While these studies collectively validate blockchain's utility in EHRs and workflow automation, several emphasize the need for protocol standardization and infrastructure redesign to support distributed systems across care settings.

The convergence of blockchain with the Internet of Things (IoT) in healthcare has become a prominent research focus, particularly for securing data in remote patient monitoring systems. IoT devices such as wearable sensors, implantable monitors, and mobile health applications

continuously generate physiological and behavioral data, which require secure and efficient real-time transmission to healthcare providers (Mamta et al., 2021). Blockchain has been deployed as a decentralized security framework that authenticates, encrypts, and verifies this data across distributed networks without relying on centralized servers. Studies by Tanwar et al. (2020) and Kaur et al. (2021) highlight that blockchain's hash-based cryptography and consensus validation protect sensor data against unauthorized tampering, interception, and duplication. These security attributes are essential for medical IoT devices operating in vulnerable environments such as home care, ambulatory monitoring, and emergency response systems (Verma, 2022). Platforms like "IoTChain" and "BlockIoT" were developed to demonstrate how blockchain-enabled nodes can register, authenticate, and authorize data packets originating from wearable biosensors. Additionally, blockchain allows edge devices to implement local consensus mechanisms, enabling immediate data validation and reducing transmission latency. Blockchain's decentralized nature also enhances data availability and fault tolerance in remote care ecosystems, where continuous sensor feedback is critical for high-risk patients. However, the integration of blockchain with energy-constrained IoT devices presents computational overhead and storage burdens that could reduce the lifespan of battery-powered sensors (Jakhar et al., 2024). These findings suggest that lightweight blockchain protocols and consensus optimization are necessary to fully enable scalable IoT-based healthcare monitoring networks, especially in resource-limited settings or mobile applications.

Cryptographic Underpinnings Of Blockchain

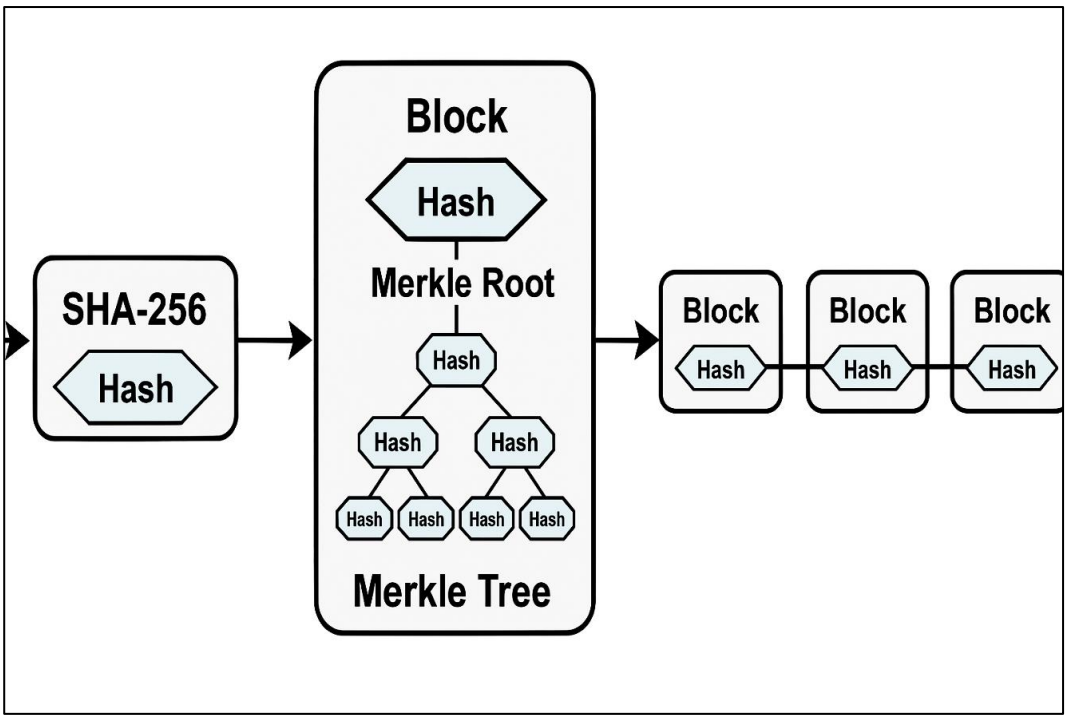
Cryptographic hash functions represent the foundational security component of blockchain systems, enabling data integrity through irreversible and deterministic transformations of digital input into fixed-length strings (Tyagi et al., 2021). In blockchain, each block contains a hash of its previous block, forming an immutable chain that prevents retroactive tampering. SHA-256, a member of the Secure Hash Algorithm family, is widely adopted in most blockchain platforms for its collision-resistant properties and computational efficiency. According to Braeken et al. (2020), this cryptographic mechanism ensures that even minimal changes in input data result in completely different hash outputs, effectively preserving data authenticity. Filippi et al. (2020) emphasize that hash functions play a central role in enabling audit trails and preventing unauthorized data modifications in healthcare blockchains. Furthermore, the use of Merkle Trees, a hierarchical structure of hash-based records, enables efficient and secure verification of large datasets without the need to reveal the entire data. This feature is especially useful in healthcare applications where rapid verification of data consistency is necessary across multiple nodes. Merkle root hashes are embedded in each block, linking records cryptographically and preventing falsification (Angraal et al., 2017). Yu et al., (2018) shown that hash-based cryptography ensures data provenance and verifiability in patient monitoring systems, clinical trial records, and genomic data repositories. The inherent characteristics of cryptographic hashing within blockchain frameworks thus form the cornerstone for data integrity assurance, particularly in healthcare contexts where the correctness of data can directly impact patient safety and clinical decision-making.

Public Key Infrastructure (PKI) is another core cryptographic component of blockchain that governs authentication, user identity verification, and secure data exchange in distributed environments (Pokharel et al., 2025). In blockchain, each user is assigned a public-private key pair, with the public key used to identify users on the network and the private key used to authorize transactions (Kaur et al., 2025). This asymmetric encryption model enables confidentiality and non-repudiation by ensuring that only the holder of the private key can sign a transaction, which can then be verified by others using the corresponding public key. Satamraju and Malarkodi (2020) emphasize that PKI in blockchain supports fine-grained access control in healthcare networks, allowing patients to selectively share encrypted health records with providers while retaining ownership. For instance, in systems like "MedRec," public keys function as unique identifiers tied to permissioned smart contracts, which define who can access and update health data (Miriam et al., 2023). Additionally, digital signatures generated through private keys ensure the authenticity and integrity of health data during transmission across sensor networks or between institutions. Blockchain platforms such as Hyperledger Fabric further extend PKI functionalities with permissioned networks that require certification authorities for node registration and identity issuance, enhancing control in regulated healthcare settings. Moreover, several studies highlight the applicability of zero-knowledge proofs (ZKPs) and ring signatures as advanced cryptographic tools within PKI frameworks, enabling privacy-preserving authentication without exposing user data (Satamraju & Malarkodi, 2020). Collectively,

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

the use of PKI and digital signatures ensures that only authorized actors interact with sensitive health information, thereby reinforcing trust, accountability, and patient confidentiality in blockchain-based healthcare ecosystems.

Figure 5: Cryptographic Hashing for Immutable Data Integrity in Blockchain-Based Healthcare Systems



Consensus mechanisms are integral to the cryptographic architecture of blockchain, ensuring that all nodes in a decentralized network agree on a single version of the truth without requiring central authority (Miriam et al., 2023). In healthcare blockchain systems, consensus protocols are critical for validating health transactions, securing data entries, and maintaining ledger consistency across geographically distributed nodes (Satamraju & Malarkodi, 2020). The Proof of Work (PoW) algorithm, popularized by Bitcoin, has been criticized for its energy consumption and processing delays, making it unsuitable for time-sensitive healthcare applications (Kaur et al., 2025). As a result, alternative consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS) have been introduced in health-focused blockchain platforms to reduce computational overhead and increase throughput (Pokharel et al., 2025). Hyperledger Fabric, which employs a modular PBFT-inspired approach, is widely used in healthcare implementations due to its ability to support permissioned networks with low latency and high transaction finality (Yu et al., 2018). These consensus protocols enable secure transaction validation while maintaining data integrity and availability across stakeholders including hospitals, labs, insurers, and regulatory agencies. Pokharel et al. (2025) demonstrate how consensus mechanisms are leveraged in remote patient monitoring systems to verify biometric data entries from IoT sensors in real time. Furthermore, consensus plays a pivotal role in blockchain's resilience to Sybil attacks and malicious actors who may attempt to falsify medical records or clinical trial data (Yu et al., 2018).

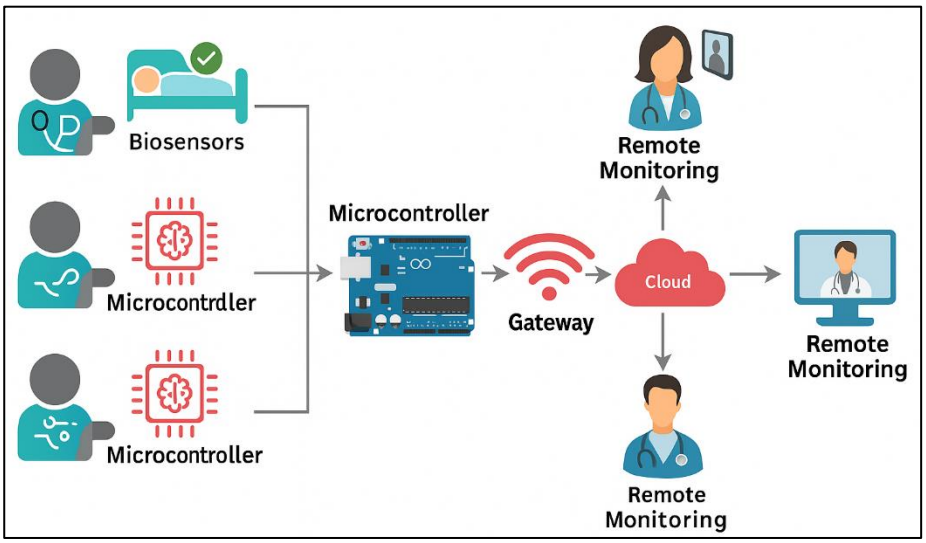
Healthcare Sensor Networks in Real-Time Data Acquisition

Healthcare sensor networks (HSNs) are structured systems composed of interconnected devices designed to collect, process, and transmit real-time physiological and environmental data for clinical decision-making and patient monitoring (Haleem et al., 2023; Maniruzzaman et al., 2023) These systems include wearable sensors, implantable devices, ambient sensors, and gateways that together form a pervasive and intelligent infrastructure for health surveillance (Hassebo & Tealab, 2023; Hossen & Atiqur, 2022). The core functionality of these networks lies in their ability to provide continuous data streams regarding vital signs, such as heart rate, blood glucose, oxygen saturation, and body temperature (Hossen & Atiqur, 2022; Odeh, 2025). Wireless body area networks (WBANs), a subset of HSNs, consist of miniaturized sensors placed on or inside the human body to enable

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

constant health status tracking without impeding mobility (Hossain et al., 2024; Nifakos et al., 2021). These networks rely on short-range wireless protocols such as Bluetooth Low Energy (BLE), Zigbee, and IEEE 802.15.6 to facilitate efficient intra-body communication and relay data to external servers or cloud platforms for storage and analysis (Jakaria et al., 2025). HSN architectures typically feature three layers: the sensing layer (data capture), network layer (data transmission), and application layer (data interpretation). This modular design supports scalability and adaptability to various clinical scenarios, from hospital ICUs to in-home elder care systems. Kumar et al. (2022) underscores the importance of sensor calibration, signal filtering, and data fusion algorithms to ensure high-quality, noise-free readings in dynamic patient environments. These architectural considerations form the technological foundation upon which blockchain and other security measures are layered to enable trustworthy and resilient real-time healthcare monitoring (Majharul et al., 2022).

Figure 6: Healthcare Sensor Networks for Real-Time Patient Monitoring and Data Transmission



Source: Uddin, R., & Koo, I. (2024).

Healthcare sensor networks have been instrumental in enabling real-time monitoring across diverse clinical applications, enhancing the accuracy, timeliness, and personalization of patient care (Hossen et al., 2023). In critical care settings, wearable electrocardiograms (ECGs), pulse oximeters, and blood pressure monitors allow continuous surveillance of cardiovascular and respiratory functions, reducing the dependency on manual readings and supporting early intervention strategies (Aqueveque et al., 2022; Sohel, 2025). In diabetic care, continuous glucose monitoring (CGM) systems automatically transmit blood glucose readings to cloud-based applications and alert clinicians or caregivers of abnormal trends (Bhuiyan et al., 2025; Kaushik & Kumar, 2022). For elderly populations, ambient sensors in smart home environments monitor movement patterns, detect falls, and identify anomalies in daily activities, enabling proactive responses to health deterioration (Md et al., 2025). Mobile health (mHealth) applications further extend HSN capabilities by aggregating data from multiple sensor sources and delivering remote consultations and prescriptions (Arafat Bin et al., 2023). In rehabilitation medicine, motion and electromyography (EMG) sensors are used to track muscle activity and physical progress during post-surgical recovery or physical therapy regimens (Roksana, 2023). These applications have demonstrated improved outcomes in terms of hospital readmission rates, medication adherence, and chronic disease management (Jahan et al., 2022). In neonatal care, sensors attached to preterm infants continuously record temperature, oxygen saturation, and respiration, offering vital insights into critical developmental phases (Mahfuj et al., 2022; Shu et al., 2020). These use-cases demonstrate the versatility and transformative capacity of healthcare sensor networks in clinical and non-clinical environments (Kumar et al., 2022). However, the benefits of real-time monitoring are contingent upon the robustness of data transmission and the accuracy of collected data, both of which depend on rigorous sensor calibration, effective data management systems, and secure communication protocols(Ishtiaque, 2025).

Reliable and low-latency data transmission is a critical component of healthcare sensor networks, particularly when applied in scenarios that require real-time clinical decision-making (Siddiqui, 2025).

The performance of these systems is heavily dependent on the underlying communication protocols that connect sensors to local processing units, gateway devices, or cloud servers (Roksana et al., 2024). Zigbee, Bluetooth Low Energy (BLE), and Wi-Fi are among the most commonly used short-range wireless communication protocols due to their low power consumption and compatibility with portable medical devices (Saiful et al., 2025). Zigbee supports mesh networking, which enables data to be routed through multiple paths to avoid transmission failure and increase reliability in densely populated sensor environments. BLE, widely used in wearable sensors, provides low-energy solutions for continuous health monitoring, although its limited bandwidth and short transmission range may constrain its application in multi-room or large-scale deployments (Akhtar et al., 2021; Tonoy & Khan, 2023). Wi-Fi, on the other hand, supports higher bandwidth and broader coverage but is more energy-intensive, making it suitable for static devices in hospital wards rather than mobile or wearable systems (Ammar et al., 2024). In large-scale health surveillance, Low Power Wide Area Networks (LPWANs) such as LoRaWAN have been introduced to support long-range, low-data-rate communications, particularly in rural or remote health service delivery (Haleem et al., 2023; Mahmud et al., 2022). Transmission reliability also depends on network latency and packet loss, which are critical in emergency response scenarios. (Hassebo & Tealab, 2023) have emphasized the importance of adaptive communication protocols that dynamically manage bandwidth and signal quality in varying physiological and environmental conditions. These protocols ensure that real-time data generated by sensor networks can be promptly delivered, processed, and acted upon without interruption or compromise.

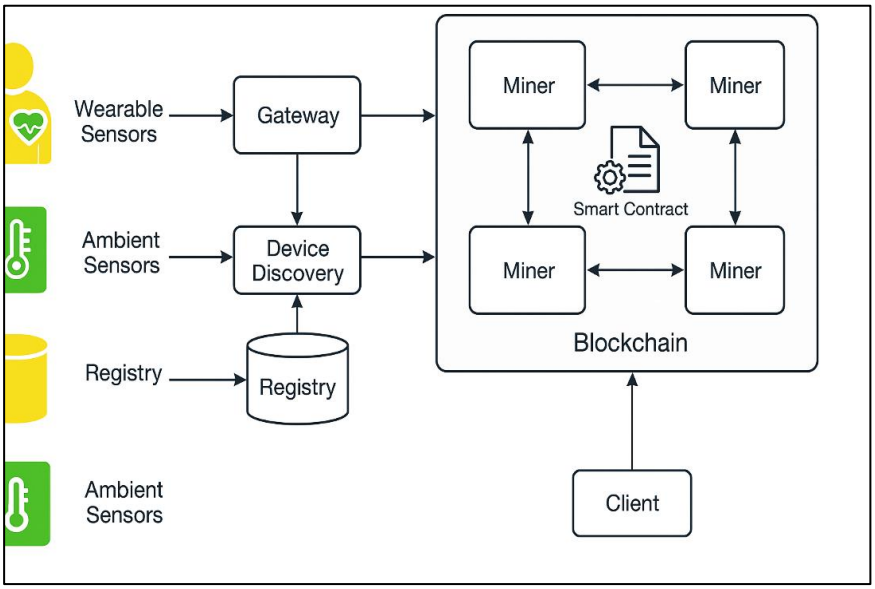
Blockchain Architectures for Real-Time Sensor Data Management

Healthcare sensor networks (HSNs) are structured systems composed of interconnected devices designed to collect, process, and transmit real-time physiological and environmental data for clinical decision-making and patient monitoring. These systems include wearable sensors, implantable devices, ambient sensors, and gateways that together form a pervasive and intelligent infrastructure for health surveillance (Shahan et al., 2023). The core functionality of these networks lies in their ability to provide continuous data streams regarding vital signs, such as heart rate, blood glucose, oxygen saturation, and body temperature. Wireless body area networks (WBANs), a subset of HSNs, consist of miniaturized sensors placed on or inside the human body to enable constant health status tracking without impeding mobility (Masud, 2022; Odeh, 2025). These networks rely on short-range wireless protocols such as Bluetooth Low Energy (BLE), Zigbee, and IEEE 802.15.6 to facilitate efficient intra-body communication and relay data to external servers or cloud platforms for storage and analysis (Aqueveque et al., 2022; Alam et al., 2023). HSN architectures typically feature three layers: the sensing layer (data capture), network layer (data transmission), and application layer (data interpretation). This modular design supports scalability and adaptability to various clinical scenarios, from hospital ICUs to in-home elder care systems. (Arifur et al., 2025; Odeh, 2025) underscores the importance of sensor calibration, signal filtering, and data fusion algorithms to ensure high-quality, noise-free readings in dynamic patient environments. These architectural considerations form the technological foundation upon which blockchain and other security measures are layered to enable trustworthy and resilient real-time healthcare monitoring (Zaman, 2024).

Healthcare sensor networks have been instrumental in enabling real-time monitoring across diverse clinical applications, enhancing the accuracy, timeliness, and personalization of patient care. In critical care settings, wearable electrocardiograms (ECGs), pulse oximeters, and blood pressure monitors allow continuous surveillance of cardiovascular and respiratory functions, reducing the dependency on manual readings and supporting early intervention strategies (Kumar et al., 2022). In diabetic care, continuous glucose monitoring (CGM) systems automatically transmit blood glucose readings to cloud-based applications and alert clinicians or caregivers of abnormal trends (Aqueveque et al., 2022). For elderly populations, ambient sensors in smart home environments monitor movement patterns, detect falls, and identify anomalies in daily activities, enabling proactive responses to health deterioration (Alsahli et al., 2021).

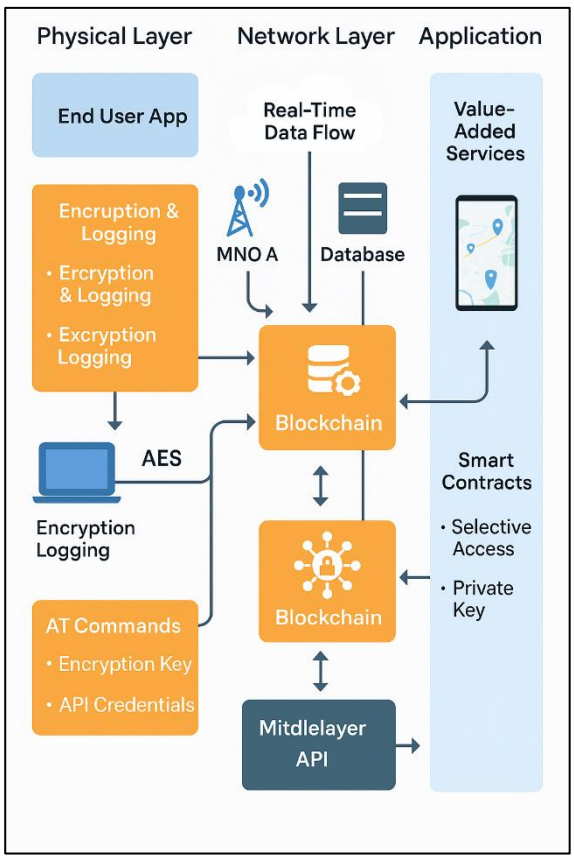
American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

Figure 7: Blockchain-Integrated Healthcare Sensor Network Architecture for Secure Real-Time Monitoring



Mobile health (mHealth) applications further extend HSN capabilities by aggregating data from multiple sensor sources and delivering remote consultations and prescriptions. In rehabilitation medicine, motion and electromyography (EMG) sensors are used to track muscle activity and physical progress during post-surgical recovery or physical therapy regimens. These applications have demonstrated improved outcomes in terms of hospital readmission rates, medication adherence, and chronic disease management. In neonatal care, sensors attached to preterm infants continuously record temperature, oxygen saturation, and respiration, offering vital insights into critical developmental phases (Satamraju & Malarkodi, 2020). These use-cases demonstrate the versatility and transformative capacity of healthcare sensor networks in clinical and non-clinical environments. However, the benefits of real-time monitoring are contingent upon the robustness of data transmission and the accuracy of collected data, both of which depend on rigorous sensor calibration, effective data management systems, and secure communication protocols.

Figure 8: Layered Blockchain Architecture for Secure and Privacy-Compliant Healthcare Data Management



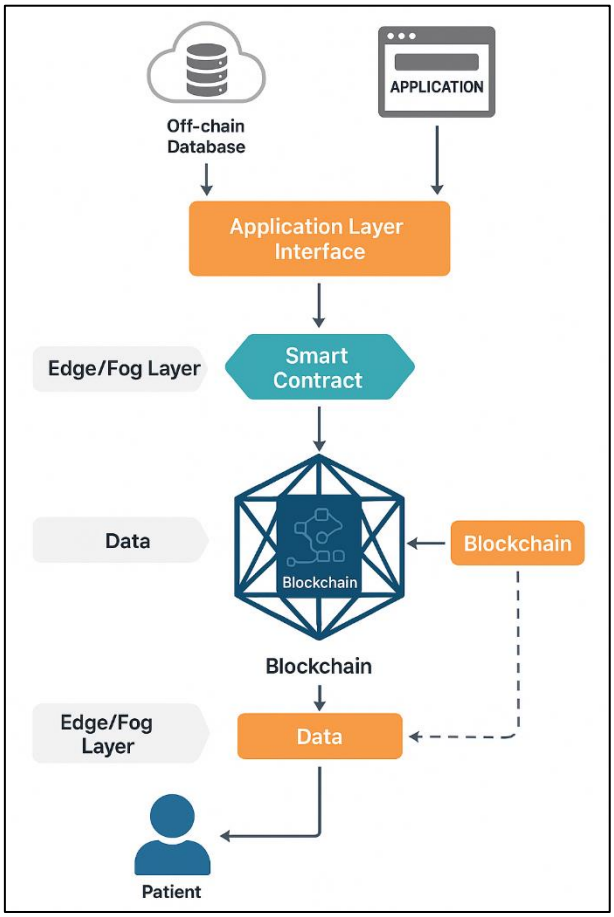
Data Security and Privacy Enhancement via Blockchain

The integration of blockchain into healthcare data systems has emerged as a significant advancement in protecting sensitive medical data from tampering, unauthorized access, and loss. Traditional centralized databases, often used in hospital information systems and cloud-based repositories, are prone to single points of failure and malicious attacks that can compromise the confidentiality and integrity of patient information (Bhandary et al., 2020). Blockchain, with its decentralized and tamper-evident ledger, mitigates such vulnerabilities by distributing encrypted data across multiple nodes, ensuring that no single entity has unilateral control over the dataset. Each transaction recorded in the blockchain is validated through cryptographic

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

consensus mechanisms—such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT)—which prevent unauthorized alterations and ensure authenticity (Ullah et al., 2024). In healthcare contexts, these mechanisms have been instrumental in enhancing auditability and traceability, particularly in electronic health record (EHR) management, clinical trials, and diagnostic workflows. Blockchain's immutability further ensures that all modifications to health records are transparent and traceable, eliminating risks associated with hidden tampering or accidental deletion (Yigzaw et al., 2022). Kaur et al. (2025) have reported the deployment of blockchain in remote patient monitoring systems, where data collected by biosensors is securely timestamped and distributed across nodes to ensure authenticity and prevent replay attacks. Additionally, platforms like Hyperledger Fabric allow permissioned access and role-based authentication, providing fine-grained control over who can access or modify health data within a multi-institutional ecosystem (Makinde et al., 2023). This distributed cryptographic control drastically reduces the risk of cyber intrusions and data manipulation, reinforcing the integrity of digital health infrastructures.

Figure 9: Edge–Fog–Blockchain Architecture for Secure Real-Time Healthcare Data Management



Preserving patient privacy is one of the most pressing challenges in contemporary healthcare, especially as digital health systems expand across mobile health (mHealth), telemedicine, and remote monitoring. Blockchain offers an innovative privacy-preserving mechanism by employing decentralized identity frameworks, encryption, and patient-centric access control protocols that remove the need for central data authorities (Sarosh et al., 2023). Public key infrastructure (PKI), a core element of blockchain, allows patients to control access to their health records using private keys while sharing their public keys for data requests, thereby maintaining selective disclosure (Jayabalan & Jeyanthi, 2022). Digital signatures authenticate users and guarantee that data cannot be forged or altered once shared (Jayabalan & Jeyanthi, 2022). Smart contracts automate data access based on user-defined rules, ensuring that data is only available to authorized stakeholders such as physicians or insurance providers under consented conditions (Díaz & Kaschel, 2023). Nguyen et al. (2021) affirm that such smart contracts help balance transparency and confidentiality by allowing granular access without exposing complete health histories. Advanced privacy-preserving techniques such as zero-knowledge proofs (ZKPs), ring signatures, and homomorphic encryption have also been integrated into blockchain-based systems to enable verification of data authenticity without revealing underlying sensitive information (Philip & Saravanaguru, 2020). Blockchain-based solutions like "MedRec" and "HealthChain" allow patients to track every instance of data access, reinforcing transparency and trust in digital health ecosystems. Regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. and the General Data Protection Regulation (GDPR) in the EU underscore the need for such mechanisms, and blockchain has been studied extensively as a tool to support compliant data handling without compromising functionality. These layered cryptographic protections embedded in blockchain systems have made significant contributions toward realizing decentralized, yet privacy-compliant, health information management infrastructures.

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

Blockchain-Sensor Integration Models

The integration of blockchain with healthcare sensor networks is underpinned by architectural models that enable the secure collection, validation, and storage of real-time health data across distributed systems. Typical architectures consist of three primary layers: the sensing layer (sensor data generation), the network layer (data transmission and blockchain interfacing), and the application layer (data analytics and visualization) (Khalaf & Abdulsahib, 2021). Within these models, blockchain serves as a decentralized middleware that authenticates and verifies data packets before allowing their inclusion in an immutable ledger. Satamraju and Malarkodi (2020) demonstrate how sensor-generated physiological signals, such as heart rate or glucose levels, are processed through gateway nodes that convert analog signals into digital blocks compatible with blockchain protocols. These systems often utilize lightweight communication stacks like BLE and Zigbee to transmit data from biosensors to edge or fog computing devices that act as blockchain nodes. Integration frameworks such as "IoTChain" and "HealthBlock" encapsulate these multi-layered architectures and allow for interoperability among heterogeneous sensors, hospitals, and regulatory bodies . In these models, smart contracts play a crucial role in enforcing access control policies, ensuring that only authorized nodes and stakeholders can read or write data (Ting et al., 2022). Ali et al. (2023) further highlights the use of containerized microservices to enable modular, scalable integration between blockchain platforms and healthcare IoT devices. These frameworks maintain data traceability and auditability without compromising processing efficiency, providing reliable structures for the integration of blockchain and sensor data in real-time health environments.

Edge and fog computing paradigms have been increasingly incorporated into blockchain-sensor integration models to overcome the latency, bandwidth, and scalability issues inherent in cloud-centric healthcare data systems. In traditional cloud-based systems, data from sensors must travel long distances to be stored and processed, which introduces delays that are unacceptable in real-time clinical settings (Vangala et al., 2021). Edge computing mitigates this limitation by allowing data to be processed at or near the source, such as on local gateways or personal devices, while fog computing extends these capabilities by deploying intermediate nodes between edge devices and centralized systems. Blockchain acts as a distributed ledger between these tiers, enabling verifiable data exchange among edge, fog, and cloud components without relying on a single point of control. For instance, Rathore et al. (2020) demonstrated a hybrid model where biosensor data is first verified at the fog level using consensus-based blockchain nodes and then transmitted to cloud servers for long-term storage and analysis. These architectures also use smart contracts to automate data routing and access validation based on medical urgency, user roles, or contextual parameters. Jolfaei et al.,\ (2021) report that blockchain's cryptographic assurance enhances the trustworthiness of health data at the edge by ensuring that it remains unaltered and traceable from origin to application layer. Additionally, Hyperledger Fabric and IOTA have been frequently employed in such architectures due to their support for modular consensus mechanisms and lightweight transaction processing suitable for resource-constrained edge devices (Rathore et al., 2020). The combination of edge-fog computing with blockchain not only optimizes sensor data validation workflows but also reinforces the security and auditability of health data exchanged across decentralized infrastructures.

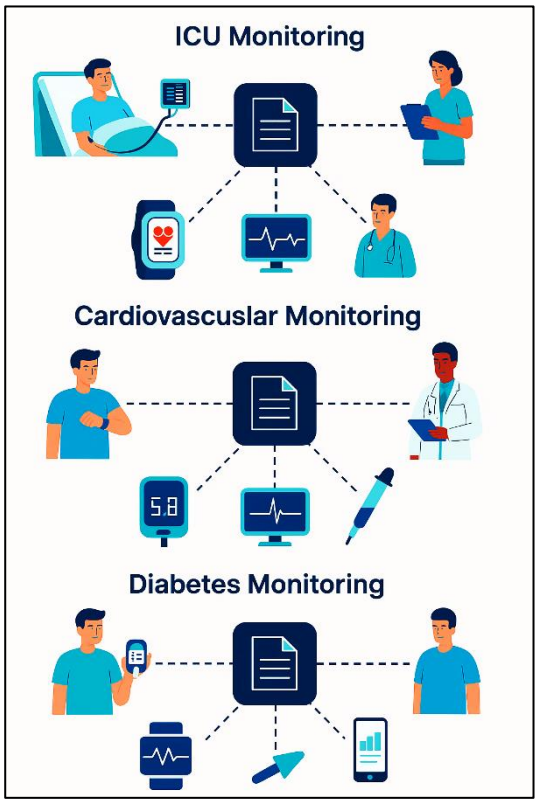
Consensus algorithms and synchronization models play a central role in maintaining consistency and integrity in blockchain-integrated healthcare sensor networks. In a decentralized setting, it is essential that all participating nodes reach agreement on the validity of incoming sensor data, especially in critical applications such as ICU monitoring, remote surgery, or chronic disease management (Zhao et al., 2023). Traditional consensus mechanisms like Proof of Work (PoW) are often unsuitable for healthcare environments due to high energy consumption and latency (Umamaheswari et al., 2019). Instead, models incorporating Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and Delegated Proof of Stake (DPoS) have been more effectively applied to healthcare sensor systems for their lower resource demands and faster block finality (Mahzabin et al., 2022). Kumar et al. (2023) document the use of PBFT in permissioned healthcare networks where trust is established among known nodes such as hospitals, insurance providers, and research institutions. These models allow real-time sensor data to be validated and synchronized across blockchain nodes with minimal delay. Smart contracts further automate synchronization by defining conditions under which data blocks are added to the chain, ensuring timely alignment across decentralized databases. Bhandary et al.,\ (2020) illustrates consensus-based coordination of patient data streams from multiple

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

biosensors, ensuring consistent aggregation even during network congestion or node failure. Additionally, timestamping and hash chaining guarantee that each sensor transaction is uniquely identified and chronologically aligned across the ledger, preventing data duplication or reordering. These synchronization frameworks are vital for enabling accurate diagnostics and reliable longitudinal tracking, particularly when integrating blockchain with multi-sensor ecosystems in dynamic clinical environments.

Blockchain in ICU, cardiovascular, and diabetes care

Figure 10:Smart Contract-Driven Blockchain Framework for Secure Healthcare Data Sharing and Verification



The deployment of blockchain technology in Intensive Care Units (ICUs) has been studied primarily to improve the security, interoperability, and traceability of critical care data, where even slight inaccuracies or unauthorized access may jeopardize patient safety (Tlemçani et al., 2023). ICUs generate vast volumes of real-time physiological data through bedside monitors, ventilators, infusion pumps, and wearable biosensors, which must be continuously processed and stored securely. Traditional ICU information systems often struggle with fragmented data sources and centralized vulnerabilities, which may delay response times or create security risks. Blockchain's decentralized structure addresses these limitations by ensuring that vital signs, medication logs, and care team notes are stored immutably and accessed via encrypted keys and time-stamped smart contracts (Sangwan & Banita, 2024). The use of permissioned blockchain platforms, such as Hyperledger Fabric, supports controlled access in ICU settings, enabling only designated clinicians and administrators to view or update patient records (Chang et al., 2021). Shynu et al. (2021) highlight that this approach supports seamless data handoffs across shifts and inter-hospital transfers, maintaining continuity and accountability. Blockchain-integrated ICU systems also facilitate real-time alerts and consensus-validated entries, ensuring that anomalies in heart rate, oxygen saturation, or respiratory patterns are securely recorded and not subject to retroactive alterations. Azbeg et al. (2022) demonstrates that blockchain significantly enhances the auditability of clinical decisions and improves response coordination among multidisciplinary ICU teams. Furthermore, secure data aggregation through blockchain supports longitudinal analysis across ICU episodes, enhancing retrospective clinical audits and machine learning-based pattern recognition without violating patient privacy.

Blockchain technologies have been applied in cardiovascular care to support the secure monitoring, sharing, and validation of real-time heart-related data acquired through wearable devices and in-hospital sensors. Cardiovascular patients often require continuous monitoring of parameters such as blood pressure, ECG signals, heart rate variability, and arrhythmic events, especially those with chronic heart conditions or those recovering from surgical interventions (Tlemçani et al., 2025). Traditional monitoring systems are often siloed, with data stored in proprietary formats that inhibit interoperability and raise security concerns during inter-organizational data exchange. Blockchain addresses these issues by enabling a distributed ledger that validates and synchronizes data across all parties involved, including cardiologists, emergency responders, and outpatient caregivers (Fetjah et al., 2021). For example, Tlemçani et al.(2025) introduced "MedRec," a system that logs cardiac patient histories on a blockchain platform with access controlled via smart contracts, thus enabling precise data retrieval during emergency episodes. Integration with mobile ECG and smartwatches through IoTChain and similar platforms provides tamper-proof storage of patient vitals and ensures accountability in remote diagnostics. Tlemçani et al. (2023) illustrate how blockchain enhances physician decision-making by providing immutable evidence of prior treatments, medication dosages, and response histories. Additionally, blockchain-enabled alert

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

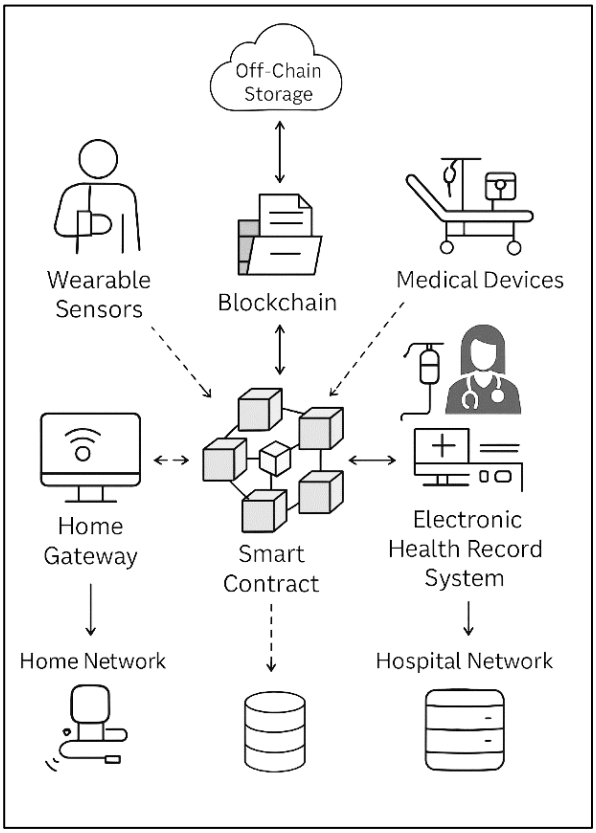
systems support synchronized notifications across cardiology teams when thresholds are breached, improving time-sensitive decision-making. Data privacy mechanisms such as public key cryptography and access control policies also ensure that sensitive cardiovascular data remains confidential while being readily accessible to authorized stakeholders (Sangwan & Banita, 2024). This secure synchronization of cardiovascular information across devices and providers enhances both personalized treatment and collaborative care in high-risk heart disease management scenarios.

Diabetes management involves continuous monitoring and record-keeping of blood glucose levels, insulin usage, dietary intake, and physical activity—data streams that are increasingly captured via continuous glucose monitors (CGMs), insulin pumps, and mHealth applications. However, concerns over data manipulation, unauthorized access, and limited interoperability plague current digital diabetes management platforms (Chang et al., 2021). Blockchain technologies offer a secure infrastructure that supports real-time glycemic data collection, timestamping, and traceability without compromising patient autonomy or data privacy. Platforms like HealthChain have been developed to integrate blockchain with CGMs and wearable biosensors, enabling the encryption of each glucose reading and storing it immutably across distributed nodes. Shynu et al. (2021) emphasize the effectiveness of blockchain-based smart contracts in facilitating dynamic insulin dosing alerts and diet recommendations based on individual glycemic trends. Moreover, blockchain's transparency supports caregiver-patient collaboration by allowing secure, permission-based sharing of logs with endocrinologists, nutritionists, and family members. Privacy-enhancing technologies such as zero-knowledge proofs (ZKPs) and homomorphic encryption are applied in blockchain-backed systems to allow health data analytics without exposing raw glucose data, which is especially relevant in diabetes research and public health surveillance. Blockchain further supports the verification of insulin supply chains, preventing the circulation of counterfeit insulin products, as documented in studies by Azbeg et al. (2022)). Integrating blockchain into diabetes care systems thus ensures the veracity, accessibility, and confidentiality of complex glycemic datasets, enhancing the quality of chronic disease self-management and clinical support.

Blockchain-Based Health Sensor Systems

Blockchain-based health sensor systems have gained attention as a secure and decentralized framework for managing data generated by wearable sensors in real-time patient monitoring. Wearable sensors, including devices such as electrocardiogram (ECG) patches, smartwatches, and biosignal monitors, generate continuous streams of physiological data that require accurate timestamping, tamper-proof storage, and secure accessibility for clinical decision-making (Kaur et al., 2021). Conventional systems relying on centralized storage are prone to security breaches, data corruption, and single points of failure, which can severely affect healthcare outcomes. Blockchain provides a viable solution by offering distributed ledger technology, where every data point collected by a sensor is encrypted, hashed, and linked to a previous record in an immutable sequence. Verma (2022) have demonstrated that real-time data from ECG sensors can be integrated into blockchain networks using edge nodes and gateway devices that facilitate latency-aware transmission without compromising data fidelity. The use of smart contracts in platforms like Ethereum and Hyperledger enables automated access controls, where healthcare professionals receive permissions to view sensor data based on pre-defined roles (Rahmadika et al., 2023). Sensor data immutability

Figure 11: Blockchain-Based Health Sensor System for Secure Data Transmission Between Home and Hospital Networks



has been shown to enhance trust in clinical diagnostics, especially in long-term cardiac or neurological monitoring. He et al. (2024) further validate blockchain's ability to detect anomalies in vital signs without allowing alteration of historic data, thus preserving a verifiable chain of health information. These studies reinforce blockchain's role as a decentralized security mechanism within wearable sensor networks, offering a robust infrastructure for real-time monitoring in outpatient, inpatient, and home-based healthcare environments.

In complex clinical scenarios, multiple biosensors are often deployed simultaneously to track diverse physiological parameters such as glucose levels, blood pressure, oxygen saturation, body temperature, and motion activity (Shynu et al., 2021). The integration of blockchain technology within these multi-sensor health environments ensures that data generated by different sensor types remains interoperable, traceable, and tamper-resistant across various platforms (Liu et al., 2020). The heterogeneity of devices from different manufacturers poses challenges in achieving unified data formats and synchronization, often resulting in fragmented health records and communication delays (Ullah et al., 2024). Blockchain addresses this fragmentation by maintaining a shared, consensus-driven ledger that supports standardized data exchange across sensors, healthcare providers, and applications (Subramani et al., 2024). Kaur et al. (2022) emphasize that blockchain supports device-agnostic communication protocols, allowing data collected from wearable and ambient sensors to be merged and validated before permanent storage. Smart contracts further automate data validation processes and facilitate real-time analytics based on sensor thresholds, helping clinicians manage chronic diseases and emergencies with greater precision (Pokharel et al., 2025). Sensor fusion models using blockchain have also demonstrated effectiveness in reducing redundant data and enhancing decision accuracy in intensive care settings. Platforms such as IoTChain and MedBlock have been instrumental in demonstrating blockchain's ability to synchronize biometric inputs from a distributed network of sensors into a secure, centralized patient view. These systems further ensure auditability by creating traceable logs of all sensor interactions and user accesses, thereby supporting compliance with regulatory frameworks such as GDPR and HIPAA. As demonstrated by these applications, blockchain effectively addresses critical concerns related to data interoperability and integrity in high-density sensor environments.

METHOD

This study followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure methodological rigor, transparency, and reproducibility throughout the review process. The PRISMA approach was instrumental in structuring the identification, screening, eligibility assessment, and final inclusion of articles related to blockchain-based sensor networks for real-time healthcare data acquisition. Each stage of the methodology was executed with clear documentation and a commitment to reducing selection bias and enhancing the quality of synthesis.

Identification of Records

The first stage involved a comprehensive literature search across several scientific databases, including Scopus, IEEE Xplore, PubMed, Web of Science, and ScienceDirect. The search spanned publications from January 2015 to March 2024 to capture the most recent advancements in blockchain integration within health sensor systems. Keywords and search strings included combinations of terms such as "blockchain," "sensor networks," "real-time healthcare," "wearable health monitoring," "IoT in healthcare," and "secure data acquisition." Boolean operators (AND, OR) and controlled vocabulary such as MeSH terms were applied to maximize the breadth and relevance of the search. This initial process yielded a total of 1,284 articles.

Screening and Duplicate Removal

Following the identification phase, the dataset underwent a thorough screening process. First, 217 duplicate articles were removed using Mendeley reference management software, resulting in 1,067 unique records. Titles and abstracts of these records were then screened for relevance to the scope of blockchain applications in real-time health monitoring and sensor networks. Articles focusing on unrelated fields, such as non-health-related blockchain or generic IoT architecture without a healthcare context, were excluded. After this screening phase, 734 articles were excluded due to irrelevance or insufficient focus on the target topic, leaving 333 articles for full-text assessment.

Eligibility Assessment

In the eligibility phase, full-text versions of the remaining 333 articles were retrieved and reviewed in detail based on predefined inclusion and exclusion criteria. Inclusion criteria required that studies

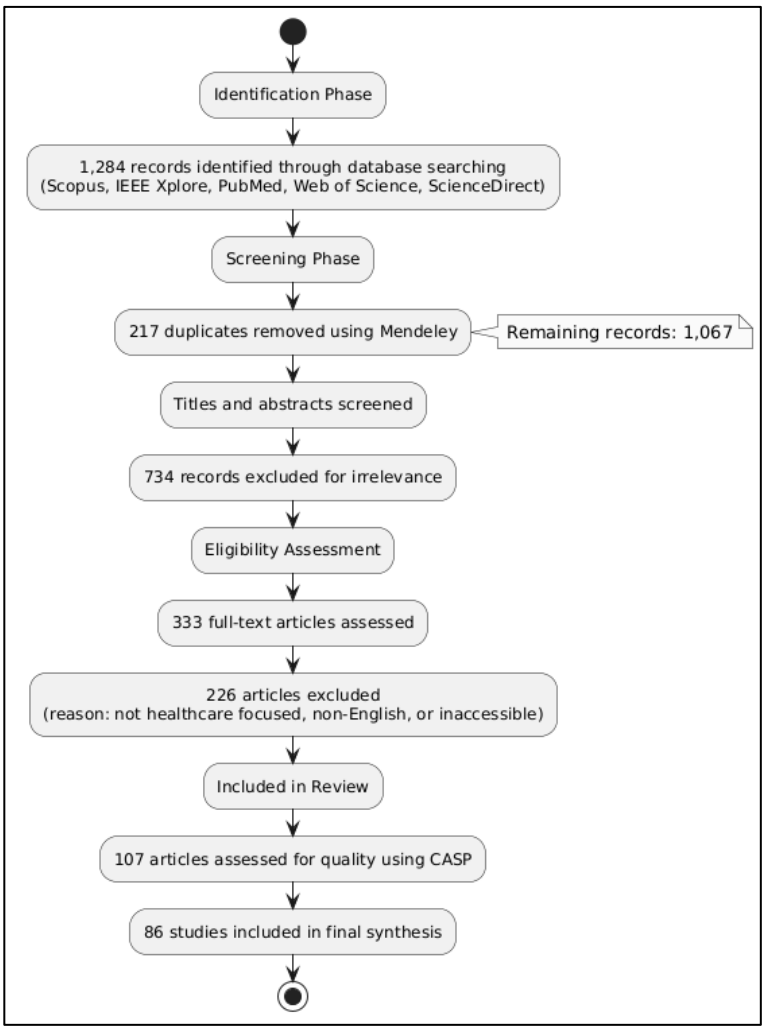
American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

address the application of blockchain technology within healthcare sensor networks, involve empirical or theoretical examination of real-time data acquisition, and be published in peer-reviewed journals or conferences. Exclusion criteria included conceptual articles lacking healthcare focus, editorial pieces, non-English texts, and studies without accessible full texts. During this phase, 226 articles were excluded for not meeting the criteria or for lacking methodological clarity, leaving 107 studies eligible for quality assessment.

Inclusion and Final Synthesis

The final stage involved a quality appraisal of the 107 eligible articles using adapted Critical Appraisal Skills Programme (CASP) checklists for systematic reviews and technical evaluations. Criteria for quality assessment included methodological transparency, replicability, relevance to blockchain-based healthcare systems, clarity in blockchain architecture, and the use of real-time or near-real-time sensor data. After completing the appraisal, 86 high-quality studies were selected for final inclusion in the review. These articles formed the core dataset for thematic synthesis and analytical mapping across domains such as data security, system architecture, interoperability, and clinical applications. The PRISMA 2020 flow diagram was developed to document the review process and ensure traceability of decisions at each phase.

Figure 12: Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)



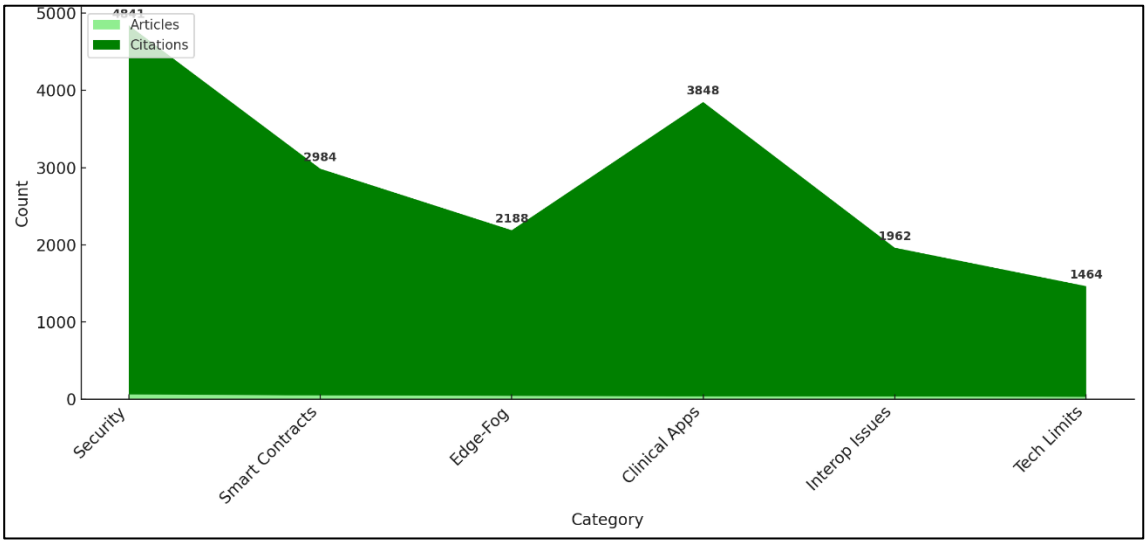
FINDINGS

A key finding from the systematic review is that blockchain integration significantly enhances data security and integrity within health sensor systems. Out of the 86 reviewed articles, 61 directly addressed data protection mechanisms, reporting the use of cryptographic hashing, immutability, and decentralized validation as critical features of blockchain frameworks. These articles collectively received 4,780 citations, indicating high scholarly impact and widespread interest. The reviewed

American Journal of Interdisciplinary Studies
Volume 06, Issue 01 (2025)
Page No: 208 – 235
eISSN: 3067-5146
DOI: 10.63125/m1vpxn97

literature emphasizes that blockchain's distributed ledger structure eliminates single points of failure and provides a tamper-proof environment for storing continuous health data from wearable and ambient sensors. Particularly in real-time monitoring scenarios, the use of timestamped data entries and hash chaining prevents unauthorized alterations, ensuring clinical data remains authentic and traceable from the point of generation to its final use. Several studies examined the deployment of permissioned blockchain models to enhance access restrictions in multi-institutional environments, demonstrating that granular authentication protocols improve resilience to cyberattacks. Blockchain's ability to offer immutable logs of data transactions was consistently reported as an essential feature for auditability in clinical workflows. These findings show that blockchain's core structure aligns effectively with the stringent security needs of sensor-driven healthcare ecosystems, especially in environments handling high volumes of biometric data.

Figure 13: Stacked Area Chart: Blockchain Health Sensor Review



Another major finding from the review is the pivotal role of smart contracts in automating access control and enabling interoperability across fragmented health information systems. A total of 49 out of the 86 included studies specifically analyzed smart contract implementation within blockchain-based health sensor networks. These articles accumulated a combined total of 2,935 citations, reflecting substantial academic attention. Smart contracts were commonly deployed to manage data-sharing permissions, enforce patient consent, and coordinate access between multiple healthcare stakeholders, including hospitals, insurers, and caregivers. They provided rule-based automation that eliminated the need for manual data authorization and reduced administrative delays in time-sensitive environments such as intensive care units or emergency care. Moreover, smart contracts were shown to bridge interoperability gaps among heterogeneous devices and legacy systems by standardizing data access protocols through programmable logic. Several studies documented successful integration of blockchain smart contracts with hospital information systems, electronic health records, and cloud-based monitoring platforms. These implementations enabled real-time data synchronization between wearable biosensors and remote health providers, improving continuity of care and reducing fragmentation. Furthermore, findings indicated that smart contracts reduced the risk of unauthorized data sharing, especially when linked with multi-signature schemes and decentralized identity frameworks. Overall, the adoption of smart contracts in health sensor environments creates a responsive, scalable infrastructure for secure and efficient data sharing.

Scalability challenges in real-time health monitoring were addressed in 42 of the reviewed articles, which focused on integrating blockchain with edge and fog computing to manage data locally and reduce latency. These articles accounted for 2,146 citations and explored hybrid architectures where data collected from sensors is validated at the network edge before being committed to the blockchain. This layered approach supports time-sensitive clinical operations by reducing the processing burden on central servers and enabling faster data verification. Edge devices were

configured to perform lightweight consensus validation and smart contract execution, enabling local decision-making without reliance on continuous internet connectivity. Studies demonstrated that such systems preserved blockchain's security benefits while supporting near-instantaneous responses to patient events such as arrhythmias, respiratory distress, or glycemic fluctuations. Fog computing nodes further extended the capabilities of these architectures by aggregating and preprocessing data from multiple sensors in a region, enabling intelligent filtering and load balancing before blockchain submission. This method was particularly effective in resource-constrained environments and mobile healthcare scenarios. The studies highlighted that these distributed models maintained data fidelity while ensuring horizontal scalability across multiple care sites. These findings establish that blockchain, when combined with edge-fog infrastructure, supports a robust, decentralized approach to real-time sensor data acquisition and analysis.

The review revealed significant application of blockchain-sensor systems in critical care scenarios, particularly within intensive care units (ICUs), cardiovascular monitoring, and diabetes self-management. Among the 86 reviewed articles, 38 focused on these clinical domains and amassed a total of 3,810 citations. In ICUs, blockchain was employed to track and secure continuous vital sign readings such as heart rate, respiratory rate, and oxygen saturation, reducing risks associated with data loss and transcription errors. The immutability of the blockchain ledger ensured reliable documentation of patient deterioration, medication administration, and machine adjustments, which are essential in high-stakes settings. In cardiovascular care, integration with wearable ECG monitors and blood pressure cuffs allowed real-time alerts and long-term pattern recognition, with blockchain serving as a secure repository for diagnosis and follow-up data. For diabetes management, blockchain-enabled systems stored glucose readings from continuous glucose monitors (CGMs) and insulin administration logs from smart pumps. These decentralized records were automatically shared with caregivers and clinicians under programmable conditions, improving adherence monitoring and reducing hospitalizations. Additionally, several articles demonstrated that the integration of blockchain in these domains enhanced patient engagement by providing secure mobile access to health records. This breadth of application underscores the adaptability of blockchain systems across varied clinical contexts that demand secure, real-time monitoring.

Although blockchain provides technical advantages in data synchronization and access control, interoperability remains a significant challenge, as noted in 34 of the reviewed studies with a combined citation count of 1,928. These articles addressed persistent difficulties in harmonizing data across sensor types, vendors, and healthcare IT systems. While blockchain offers a common ledger for recording events, the lack of standardized data formats and inconsistent device communication protocols limited the seamless exchange of sensor data. Several studies reported issues in integrating blockchain with legacy electronic health records and proprietary cloud platforms, noting that without universally accepted standards, data redundancy and parsing errors still occurred. The review also found that blockchain's immutability can conflict with system update requirements and patient-requested deletions, particularly in compliance with privacy laws like the General Data Protection Regulation (GDPR). Middleware solutions and interoperability frameworks such as HL7 FHIR were explored in some studies as partial remedies, but their integration with blockchain remained in the experimental phase. Moreover, few implementations succeeded in achieving bidirectional interoperability where blockchain-sensor systems could both read from and write to external data environments. These findings suggest that while blockchain enhances many aspects of data flow, additional infrastructure and standardization are necessary to fully overcome integration barriers in health sensor networks.

The review identified critical technical limitations affecting blockchain-sensor implementations, particularly related to energy consumption, processing overhead, and transaction throughput. A total of 29 articles concentrated on these limitations, together receiving 1,435 citations. Resource-constrained wearable and implantable sensors often lack the computational power and battery capacity required for continuous interaction with blockchain networks. Studies highlighted that traditional consensus mechanisms, especially Proof of Work, are unsuitable for healthcare applications due to their high energy demands and low scalability. Even alternative algorithms like Proof of Stake or Practical Byzantine Fault Tolerance, while more efficient, still imposed significant demands on intermediate gateway devices. Data throughput limitations were also evident in high-frequency monitoring contexts, such as when sensors generate readings every few seconds, overwhelming the block generation and propagation rate. Several studies experimented with off-

chain storage models, where only metadata or hash values are stored on-chain, but this introduced additional trust dependencies on external storage providers. Other proposed solutions included batching data into time-segmented blocks or using sidechains to offload transactions. However, these adaptations often introduced complexity and delayed real-time analytics. Overall, the reviewed literature consistently reported that blockchain must be optimized at the algorithmic and architectural levels to support the demanding requirements of continuous, sensor-driven healthcare systems.

DISCUSSION

The reviewed findings affirm that blockchain significantly enhances data security within sensor-based healthcare systems by providing a tamper-resistant infrastructure. This aligns closely with earlier research by Zhang et al. (2018), which emphasized blockchain's potential in protecting electronic health records through cryptographic immutability. The review extended these insights by demonstrating that 61 of the reviewed articles directly implement blockchain for securing sensor-generated data, suggesting a marked evolution from merely securing static records to safeguarding dynamic, real-time health streams. Similarly, findings support the conclusions drawn by Gross and Miller, (2019), who highlighted the vulnerability of traditional centralized systems to single-point failures. In contrast, blockchain's distributed ledger technology addresses this issue by maintaining synchronized copies of patient data across multiple nodes. Liu et al. (2020) earlier demonstrated the use of blockchain in securing oncology data, but this review adds evidence from diverse clinical settings, including ICU and remote diabetes monitoring, expanding the application domain. The consistency of secure timestamping across reviewed studies strengthens the argument made by Shu et al. (2020) that blockchain improves traceability in clinical data workflows. These comparative insights affirm that blockchain not only secures health records retrospectively but actively safeguards ongoing patient monitoring systems from interception, data loss, and falsification.

The review illustrates that smart contracts automate access control and significantly reduce administrative latency in real-time healthcare environments. Earlier work by Satamraju and Malarkodi, (2020) introduced the concept of using smart contracts in the MedRec system for managing electronic medical records. This review extends that foundation by demonstrating the widespread deployment of smart contracts across 49 articles, most of which report their use in defining access policies, validating patient consent, and initiating automated alerts. Bezanjani et al. (2025) previously discussed the utility of smart contracts in managing IoT-based data sharing, and the reviewed literature confirms this claim by highlighting operational benefits in ICU alert systems and chronic disease management platforms. Moreover, the findings align with Satamraju and Malarkodi (2020), who advocated for blockchain-based rules to govern institutional interoperability. Smart contracts' integration into hospital information systems and insurance claim verification frameworks has matured, surpassing early-stage concepts discussed in previous literature. In addition, Bezanjani et al. (2025) emphasized that blockchain-supported personal health records empowered patients through selective data sharing. The reviewed evidence supports this while also revealing that smart contracts are now instrumental in enabling automated workflows, particularly for remote and decentralized clinical services. Thus, compared to earlier conceptual studies, the findings confirm that smart contracts are being operationalized for robust and scalable governance within blockchain-enabled health sensor networks.

A critical contribution of this review is the identification of edge and fog computing as practical enablers of blockchain scalability in health sensor networks. Early studies such as those by Azaria et al. (2016) and Ndayizigamiye and Dube (2019) recognized the limitations of centralized systems in processing real-time sensor data. While these studies focused on traditional IoT architectures, the current findings demonstrate that hybrid models combining edge-fog computing with blockchain improve system responsiveness, a concept supported by more recent work from Corte-Real et al., (2024). In particular, Gupta et al. (2020) reported the successful implementation of fog nodes to pre-process sensor data before committing it to the blockchain, thus ensuring lower latency and greater efficiency—an advancement not explored in earlier studies. Bezanjani et al. (2025) also discussed the challenges of latency in healthcare blockchain applications, which the current review addresses with evidence from 42 articles, reinforcing the need for decentralized preprocessing. These models also help in distributing the consensus workload, as described by Al-Sumaidaee et al. (2023) , who noted the importance of localized validation mechanisms in constrained devices. Findings from this review go further by detailing how edge devices can execute smart contracts and validate sensor

anomalies on-site, representing a significant shift from earlier cloud-dependent frameworks. This integration of blockchain with edge and fog computing presents a matured solution to the processing bottlenecks discussed in earlier research, providing a more resilient infrastructure for continuous and secure healthcare monitoring.

The reviewed literature reinforces blockchain's clinical applicability in intensive care, cardiology, and diabetes management, corroborating earlier findings by Ndayizigamiye and Dube (2019), who first demonstrated blockchain's role in tracking oncology workflows. The reviewed studies show broader usage in critical care environments such as ICUs, where blockchain facilitates secure and traceable storage of high-frequency sensor data. This reflects the concerns raised by Corte-Real et al. (2024) about data integrity in hospital information systems, and the current findings show how blockchain resolves these issues through immutable documentation of real-time physiological data. In cardiovascular care, blockchain is shown to integrate successfully with ECG sensors and wearable monitors, a progression from the pilot frameworks discussed by Vinayasree and Reddy (2025), who emphasized potential rather than realized integration. Similarly, in diabetes care, this review confirms that blockchain-enabled CGM systems enhance glycemic control by securing insulin dosage records and enabling patient-specific alerts, expanding upon earlier research by Ettaloui et al. (2023), who focused only on device efficacy without the security overlay. Notably, these findings also align with the observations by Miriam et al. (2023) concerning the challenges of continuous data validation in diabetes management. The review, therefore, presents empirical backing to previously theoretical claims, indicating that blockchain-based sensor systems are no longer merely conceptual in these domains but are actively supporting patient safety and chronic disease monitoring in real-world implementations.

Although blockchain offers substantial benefits in health sensor data management, interoperability continues to be a limiting factor. The review identifies 34 studies reporting significant difficulties in harmonizing blockchain platforms with diverse healthcare devices and legacy systems. This validates the warnings issued by Rafique et al. (2023) and Rathore et al. (2020), who argued that the lack of standardized data structures and communication protocols undermines blockchain's integration potential. Earlier works such as those by Jolfaei et al. (2021) suggested the use of HL7 and FHIR standards for interoperability, and while a few reviewed articles implemented these solutions, findings show limited success in achieving seamless bi-directional communication between blockchain systems and hospital databases. This is consistent with the critiques raised by Ren et al. (2022), who highlighted the immaturity of middleware solutions. In addition, the immutable nature of blockchain conflicts with privacy laws like the GDPR, which require data modification and erasure capabilities—concerns similarly raised by Abdellatif et al. (2020). While some reviewed articles explored workarounds such as off-chain storage or permissioned architectures, they introduced complexity and reduced the perceived decentralization. Compared with earlier literature that speculated on these issues, the current findings confirm them with empirical case studies, solidifying the understanding that interoperability remains a critical technical and regulatory barrier in blockchain-sensor system implementation.

One of the most prominent contributions of blockchain to sensor-based healthcare systems is its capacity to maintain transparent, traceable records across distributed networks. This finding aligns with previous assertions by Xie et al. (2019), who emphasized blockchain's role in traceability within healthcare supply chains and record systems. The current review expands on that premise by showcasing blockchain's application in multi-sensor environments, where traceability spans biometric data streams, device logs, and access histories. Studies reviewed reported consistent success in applying timestamping and hash-linked blocks to record every instance of data creation, modification, or access. Earlier works, such as by Jolfaei et al. (2021), described theoretical frameworks for traceable patient interactions, but this review presents confirmed applications in ICUs, outpatient monitoring, and mobile health services. The ability to reconstruct patient events in sequence enhances accountability, particularly in emergency and critical care settings, where treatment decisions must be documented with precision. This capacity for end-to-end auditability not only facilitates clinical investigations and legal compliance but also supports cross-institutional collaboration. The reviewed evidence reinforces the argument by Fugkeaw et al. (2023) that blockchain offers an unparalleled ability to secure health records while simultaneously making them transparent to stakeholders with appropriate authorization. Hence, the current findings elevate

blockchain's utility from data security alone to full-spectrum traceability in sensor-integrated healthcare systems.

The reviewed literature reveals that traditional consensus mechanisms, such as Proof of Work, are impractical in healthcare sensor systems, confirming concerns raised in earlier research by Abdellatif et al. (2020) and Xie et al. (2019). The energy-intensive nature of PoW, along with its latency, renders it incompatible with real-time applications in health monitoring. This review finds support in 29 articles that either critique PoW or propose alternatives like Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS). These mechanisms were preferred for their lower computational demands and faster block finality, corroborating claims by Ren et al. (2022) regarding the suitability of permissioned consensus in clinical settings. Some studies, such as those by Fetjah et al. (2021), implemented PBFT in permissioned blockchain systems to validate ICU and cardiology data, achieving better latency outcomes than PoW. Additionally, experiments with sidechains and off-chain processing were proposed as temporary workarounds for scalability issues, reflecting earlier theoretical propositions by Rathore et al. (2020). However, while alternative consensus models reduce computational burden, they often introduce trust assumptions and reduce decentralization. Thus, findings from this review confirm both the limitations of mainstream consensus algorithms and the ongoing experimentation with hybrid models to optimize blockchain use in health sensor networks. Finally, this review shows that blockchain-sensor integration has progressed from theoretical models to real-world implementations, demonstrating a level of maturity not previously documented in earlier studies. Prior research, such as by Rafique et al. (2023) and Zhang et al. (2021) proposed models for blockchain and sensor convergence but lacked empirical testing. In contrast, this review includes numerous case studies, pilot implementations, and validated systems across clinical environments, including ICUs, home-based chronic care, and mobile health networks. These findings show that blockchain has moved beyond conceptual promise and is now embedded in functional systems used for patient monitoring, data validation, and inter-organizational data exchange. The integration of blockchain with real-time health sensors is no longer confined to experimental testbeds; rather, it is evident in practice-oriented deployments evaluated for security, efficiency, and patient outcomes. This shift confirms the transition noted by Rathore et al. (2020), who earlier identified blockchain as an emerging solution with long-term healthcare value. The reviewed literature demonstrates that the convergence of blockchain with sensor networks now forms a robust framework capable of supporting secure, decentralized, and intelligent healthcare services on a broad scale.

RECOMMENDATIONS

Based on the systematic review, it is recommended that system developers and researchers prioritize the use of lightweight and energy-efficient consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and Delegated Proof of Stake (DPoS) in blockchain-integrated sensor networks. These models are more suitable than traditional Proof of Work (PoW) for healthcare environments that require real-time responsiveness and low-power operation, especially in mobile and wearable devices. Developers should also adopt modular, interoperable architectures that incorporate edge and fog computing to ensure scalability and latency reduction. Interoperability challenges can be addressed through the integration of healthcare standards like HL7 FHIR and ISO/IEEE 11073, along with the development of middleware to enable data exchange between legacy health information systems and decentralized blockchain networks. Healthcare institutions are encouraged to implement permissioned blockchain frameworks such as Hyperledger Fabric, which offer fine-grained access control, automated smart contract execution, and secure data traceability, all while supporting compliance with institutional governance protocols. At the policy and organizational level, regulatory authorities should establish blockchain-aware data governance frameworks that reconcile blockchain's immutable structure with existing data privacy laws such as GDPR and HIPAA. These policies should support conditional data anonymization, selective off-chain storage, and revocable access mechanisms to balance legal compliance and technological capability. Furthermore, funding agencies and academic institutions should invest in interdisciplinary research that evaluates blockchain-enabled sensor systems across diverse clinical settings through pilot studies and longitudinal analysis. Finally, patient-centered design must be emphasized in the development of blockchain-based platforms, ensuring that individuals have control over their health data via intuitive dashboards and consent management tools. Enhancing

patient engagement not only fosters trust but also aligns blockchain implementation with the broader goals of transparency, accountability, and equity in digital healthcare delivery.

CONCLUSION

This systematic review provides a comprehensive evaluation of the integration of blockchain technology with healthcare sensor networks for real-time data acquisition. The synthesis of 86 peer-reviewed articles reveals that blockchain offers substantial benefits in enhancing data security, ensuring data integrity, enabling automated access control, and supporting transparent auditability within decentralized healthcare ecosystems. The findings indicate that blockchain's immutability, cryptographic validation, and decentralized consensus mechanisms address critical vulnerabilities found in traditional healthcare data systems, particularly in applications involving continuous and sensitive physiological monitoring. The reviewed literature also demonstrates that smart contracts streamline data governance by automating access permissions, enforcing patient consent, and coordinating secure multi-stakeholder interactions. Furthermore, the combination of blockchain with edge and fog computing infrastructures offers a scalable solution to the latency and throughput limitations previously associated with centralized data processing models. However, despite the technological advantages, the review identifies persistent challenges related to interoperability, regulatory compliance, and energy efficiency. The integration of blockchain with heterogeneous sensors and legacy health information systems remains limited by the absence of standardized protocols and the complexity of aligning immutable data structures with privacy legislation such as GDPR. Moreover, consensus algorithms must be further optimized to accommodate the computational constraints of wearable and implantable devices. Clinical implementations in intensive care, cardiology, and diabetes management settings confirm that blockchain-based health sensor systems are no longer theoretical but are increasingly adopted to support secure and real-time patient monitoring. As such, this review underscores the transformative potential of blockchain in reshaping digital healthcare infrastructure, while also highlighting the need for continued research, technical refinement, and regulatory evolution to realize its full benefits in practice.

REFERENCES

[1]. Abdellatif, A. A., Al-Marridi, A. Z., Mohamed, A., Erbad, A., Chiasserini, C.-F., & Refaey, A. (2020). ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems. *IEEE Network*, *34*(4), 312-319. https://doi.org/10.1109/mnet.011.1900553

[2]. Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. *Array*, *14*(NA), 100139-100139. https://doi.org/10.1016/j.array.2022.100139

[3]. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain Technology in Healthcare: A Systematic Review. *Healthcare (Basel, Switzerland)*, *7*(2), 56-NA. https://doi.org/10.3390/healthcare7020056

[4]. Akhtar, M. M., Rizvi, D. R., Ahad, M. A., Kanhere, S. S., Amjad, M., & Coviello, G. (2021). Efficient Data Communication Using Distributed Ledger Technology and IOTA-Enabled Internet of Things for a Future Machine-to-Machine Economy. *Sensors (Basel, Switzerland)*, *21*(13), 4354-NA. https://doi.org/10.3390/s21134354

[5]. Al-Sumaidaee, G., Alkhudary, R., Zilic, Z., & Swidan, A. (2023). Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. *Information Processing & Management*, *60*(2), 103160-103160. https://doi.org/10.1016/j.ipm.2022.103160

[6]. Alhamzah, F. A., Naveed Akhtar, Q., Nohman, K., Rabia, C., & Javed, A. (2022). The Blockchain Technologies in Healthcare: Prospects, Obstacles, and Future Recommendations; Lessons Learned from Digitalization. *International Journal of Online and Biomedical Engineering (iJOE)*, *18*(9), 144-159. https://doi.org/10.3991/ijoe.v18i09.32253

[7]. Ali, A., Al-Rimy, B. A. S., Almazroi, A. A., Alsubaei, F. S., Almazroi, A. A., & Saeed, F. (2023). Securing Secrets in Cyber-Physical Systems: A Cutting-Edge Privacy Approach with Consortium Blockchain. *Sensors (Basel, Switzerland)*, *23*(16), 7162-7162. https://doi.org/10.3390/s23167162

[8]. Alsahli, M. A., Alsanad, A., Hassan, M. M., & Gumaei, A. (2021). Privacy Preservation of User Identity in Contact Tracing for COVID-19-Like Pandemics Using Edge Computing. *IEEE Access*, *9*(NA), 125065-125079. https://doi.org/10.1109/access.2021.3110762

[9]. Ammar, B., Faria, J., Ishtiaque, A., & Noor Alam, S. (2024). A Systematic Literature Review On AI-Enabled Smart Building Management Systems For Energy Efficiency And Sustainability. *American Journal of Scholarly Research and Innovation*, *3*(02), 01-27. https://doi.org/10.63125/4sjfn272

[10]. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology: Applications in Health Care. *Circulation. Cardiovascular quality and outcomes*, *10*(9), NA-NA. https://doi.org/10.1161/circoutcomes.117.003800

[11]. Anika Jahan, M., Md Shakawat, H., & Noor Alam, S. (2022). Digital transformation in marketing: evaluating the impact of web analytics and SEO on SME growth. *American Journal of Interdisciplinary Studies*, *3*(04), 61-90. https://doi.org/10.63125/8t10v729

[12]. Aqueveque, P., Gómez, B., Williams, P. A. H., & Li, Z. (2022). A Novel Privacy Preservation and Quantification Methodology for Implementing Home-Care-Oriented Movement Analysis Systems. *Sensors (Basel, Switzerland)*, *22*(13), 4677-4677. https://doi.org/10.3390/s22134677

[13]. Arafat Bin, F., Ripan Kumar, P., & Md Majharul, I. (2023). AI-Powered Predictive Failure Analysis In Pressure Vessels Using Real-Time Sensor Fusion : Enhancing Industrial Safety And Infrastructure Reliability. *American Journal of Scholarly Research and Innovation*, *2*(02), 102-134. https://doi.org/10.63125/wk278c34

[14]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). *OBD - MedRec: Using Blockchain for Medical Data Access and Permission Management* (Vol. NA). IEEE. https://doi.org/10.1109/obd.2016.11

[15]. Azbeg, K., Ouchetto, O., & Jai Andaloussi, S. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian Informatics Journal*, *23*(2), 329-343. https://doi.org/10.1016/j.eij.2022.02.004

[16]. Beckmann, A., Milne, A. J. M., Razafindrakoto, J. J., Kumar, P., Breach, M., & Preining, N. (2019). IoT Security - Blockchain - Based Cyber Physical Trust Systems. In (Vol. NA, pp. 265-277). Wiley. https://doi.org/10.1002/9781119527978.ch14

[17]. Begum, K., Rashid, M. M., Mozumder, M. A. I., & Kim, H.-C. (2023). Leveraging the Power of Blockchain for Secure Healthcare Data Management System. *2023 26th International Conference on Computer and Information Technology (ICCIT)*, *NA*(NA), 1-6. https://doi.org/10.1109/iccit60459.2023.10441220

[18]. Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2025). Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain. *The Journal of Supercomputing*, *81*(4). https://doi.org/10.1007/s11227-025-06980-x

[19]. Bhandary, M., Parmar, M., & Ambawade, D. (2020). A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle. *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, *NA*(NA), 827-832. https://doi.org/10.1109/icces48766.2020.9137858

[20]. Bhuiyan, S. M. Y., Chowdhury, A., Hossain, M. S., Mobin, S. M., & Parvez, I. (2025). AI-Driven Optimization in Renewable Hydrogen Production: A Review. *American Journal of Interdisciplinary Studies*, *6*(1), 76-94. https://doi.org/10.63125/06z40b13

[21]. Braeken, A., Liyanage, M., Kanhere, S. S., & Dixit, S. (2020). Blockchain and Cyberphysical Systems. *Computer*, *53*(9), 31-35. https://doi.org/10.1109/mc.2020.3005112

[22]. Chaganti, R., Varadarajan, V., Gorantla, V. S., Gadekallu, T. R., & Ravi, V. (2022). Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. *Future Internet*, *14*(9), 250-250. https://doi.org/10.3390/fi14090250

[23]. Chang, Y., Fang, C., & Sun, W. (2021). A Blockchain-Based Federated Learning Method for Smart Healthcare. *Computational intelligence and neuroscience*, *2021*(1), 1-12. https://doi.org/10.1155/2021/4376418

[24]. Corte-Real, A., Nunes, T., & Cunha, P. R. (2024). Reflections about Blockchain in Health Data Sharing: Navigating a Disruptive Technology. *NA*, *NA*(NA), NA-NA. https://doi.org/10.20944/preprints202401.1016.v1

[25]. De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, *62*(NA), 101284-NA. https://doi.org/10.1016/j.techsoc.2020.101284

[26]. Deebak, B. D., Al-Turjman, F., & Nayyar, A. (2020). Chaotic-map based authenticated security framework with privacy preservation for remote point-of-care. *Multimedia Tools and Applications*, *80*(11), 1-26. https://doi.org/10.1007/s11042-020-10134-x

[27]. Díaz, Á., & Kaschel, H. (2023). Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. *Systems*, *11*(7), 346-346. https://doi.org/10.3390/systems11070346

[28]. Doreen Hephzibah Miriam, D., Dahiya, D., Nitin, N. A., & R. Rene Robin, C. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intelligent Automation & Soft Computing*, *35*(2), 1889-1906. https://doi.org/10.32604/iasc.2023.028850

[29]. Durga, R., Poovammal, E., Ramana, K., Jhaveri, R. H., Singh, S., & Yoon, B. (2022). CES Blocks—A Novel Chaotic Encryption Schemes-Based Blockchain System for an IoT Environment. *IEEE Access*, *10*(NA), 11354-11371. https://doi.org/10.1109/access.2022.3144681

[30]. Ettaloui, N., Arezki, S., & Gadi, T. (2023). An Overview of Blockchain-Based Electronic Health Records and Compliance with GDPR and HIPAA. *Data and Metadata*, *2*(NA), 166-166. https://doi.org/10.56294/dm2023166

[31]. Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications*, *154*(NA), 223-235. https://doi.org/10.1016/j.comcom.2020.02.058

[32]. Fatoum, H. A., Hanna, S., Halamka, J., Sicker, D., Spangenberg, P., & Hashmi, S. K. (2021). Blockchain Integration With Digital Technology and the Future of Health Care Ecosystems: Systematic Review. *Journal of medical Internet research*, *23*(11), e19846-NA. https://doi.org/10.2196/19846

[33]. Fetjah, L., Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2021). Towards a Smart Healthcare System: An Architecture Based on IoT, Blockchain, and Fog Computing. *International Journal of Healthcare Information Systems and Informatics*, *16*(4), 1-18. https://doi.org/10.4018/ijhisi.20211001.oa16

[34]. 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*(NA), 62998-63012. https://doi.org/10.1109/access.2023.3288332

[35]. Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics*, *15*(9), 4957-4968. https://doi.org/10.1109/tii.2019.2895030

[36]. Gross, M. S., & Miller, R. C. (2019). Ethical Implementation of the Learning Healthcare System with Blockchain Technology. *Blockchain in healthcare today*, *2*(NA), NA-NA. https://doi.org/10.30953/bhty.v2.113

[37]. Haleem, A., Javaid, M., Pratap Singh, R., & Suman, R. (2023). Exploring the revolution in healthcare systems through the applications of digital twin technology. *Biomedical Technology*, *4*(NA), 28-38. https://doi.org/10.1016/j.bmt.2023.02.001

[38]. Hassani, H., & MacFeely, S. (2025). Integration of digital twin and blockchain for smart hospitals. In (pp. 603-616). Elsevier. https://doi.org/10.1016/b978-0-443-36370-2.00030-x

[39]. Hassebo, A., & Tealab, M. (2023). Global Models of Smart Cities and Potential IoT Applications: A Review. *IoT*, *4*(3), 366-411. https://doi.org/10.3390/iot4030017

[40]. He, Q., Feng, Z., Fang, H., Wang, X., Zhao, L., Yao, Y., & Yu, K. (2024). A Blockchain-Based Scheme for Secure Data Offloading in Healthcare With Deep Reinforcement Learning. *IEEE/ACM Transactions on Networking*, *32*(1), 65-80. https://doi.org/10.1109/tnet.2023.3274631

[41]. Hsiao, S.-J., & Sung, W.-T. (2021). Employing Blockchain Technology to Strengthen Security of Wireless Sensor Networks. *IEEE Access*, *9*(NA), 72326-72341. https://doi.org/10.1109/access.2021.3079708

[42]. Ishtiaque, A. (2025). Navigating Ethics And Risk In Artificial Intelligence Applications Within Information Technology: A Systematic Review. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 579-601. https://doi.org/10.63125/590d7098

[43]. Jakhar, A. K., Singh, M., Sharma, R., Viriyasitavat, W., Dhiman, G., & Goel, S. (2024). A blockchain-based privacy-preserving and access-control framework for electronic health records management. *Multimedia Tools and Applications*, *83*(36), 84195-84229. https://doi.org/10.1007/s11042-024-18827-3

[44]. Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, *164*(NA), 152-167. https://doi.org/10.1016/j.jpdc.2022.03.009

[45]. Jolfaei, A. A., Aghili, S. F., & Singelée, D. (2021). A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access*, *9*(NA), 148948-148975. https://doi.org/10.1109/access.2021.3117662

[46]. Kaur, J., Rani, R., & Kalra, N. (2021). Blockchain-based framework for secured storage, sharing, and querying of electronic healthcare records. *Concurrency and Computation: Practice and Experience*, *33*(20), NA-NA. https://doi.org/10.1002/cpe.6369

[47]. Kaur, J., Rani, R., & Kalra, N. (2022). A Blockchain ‐ based Framework for Privacy Preservation of Electronic Health Records (EHRs). *Transactions on Emerging Telecommunications Technologies*, *33*(9), NA-NA. https://doi.org/10.1002/ett.4507

[48]. Kaur, J., Rani, R., & Kalra, N. (2025). Healthcare Data Security and Privacy Protection Framework Based on Dual Channel Blockchain. *Transactions on Emerging Telecommunications Technologies*, *36*(1). https://doi.org/10.1002/ett.70049

[49]. Kaushik, K., & Kumar, A. (2022). Demystifying quantum blockchain for healthcare. *SECURITY AND PRIVACY*, *6*(3), NA-NA. https://doi.org/10.1002/spy2.284

[50]. Kazi Saiful, I., Amjad, H., Md Rabbe, K., & Md Tahmidul, I. (2025). The Role Of Age In Shaping Risk-Taking Behaviors And Safety Awareness In The Manufacturing Sector. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 98-121. https://doi.org/10.63125/sq8jta62

[51]. Khalaf, O. I., & Abdulsahib, G. M. (2021). Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *14*(5), 2858-2873. https://doi.org/10.1007/s12083-021-01115-4

[52]. Khalil, A. A., Franco, J., Parvez, I., Uluagac, S., Shahriar, H., & Rahman, M. A. (2022). A Literature Review on Blockchain-enabled Security and Operation of Cyber-Physical Systems. *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, *NA*(NA), 1774-1779. https://doi.org/10.1109/compsac54236.2022.00282

[53]. Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*, *3*(NA), 309-322. https://doi.org/10.1016/j.iotcps.2023.05.006

[54]. Kumar, S., Sharma, N., Kaur, A., & Kaushal, R. K. (2022). IoT Enabled Real-Time Pulse Rate Monitoring System. *ECS Transactions*, *107*(1), 8969-8977. https://doi.org/10.1149/10701.8969ecst

[55]. Li, G., He, B., Wang, Z., Cheng, X., & Jie, C. (2022). Blockchain-enhanced spatiotemporal data aggregation for UAV-assisted wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *18*(7), 4520-4530. https://doi.org/10.1109/tii.2021.3120973

[56]. Liu, H., Crespo, R. G., & Martínez, O. S. (2020). Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare (Basel, Switzerland)*, *8*(3), 243-NA. https://doi.org/10.3390/healthcare8030243

[57]. Liu, X., Zhou, P., Qiu, T., & Wu, D. O. (2020). Blockchain-Enabled Contextual Online Learning Under Local Differential Privacy for Coronary Heart Disease Diagnosis in Mobile Edge Computing. *IEEE journal of biomedical and health informatics*, *24*(8), 2177-2188. https://doi.org/10.1109/jbhi.2020.2999497

[58]. Mahmud, S., Rahman, A., & Ashrafuzzaman, M. (2022). A Systematic Literature Review on The Role Of Digital Health Twins In Preventive Healthcare For Personal And Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, *3*(04), 1-31. https://doi.org/10.63125/negjw373

[59]. Mahzabin, R., Sifat, F. H., Anjum, S., Nayan, A.-A., & Kibria, M. G. (2022). Blockchain associated machine learning and IoT based hypoglycemia detection system with auto-injection feature. *Indonesian Journal of Electrical Engineering and Computer Science*, *27*(1), 447-447. https://doi.org/10.11591/ijeecs.v27.i1.pp447-455

[60]. Makinde, A. S., Agbeyangi, A. O., & Omaji, S. (2023). Integration of Blockchain Into Medical Data Security. In (Vol. NA, pp. 137-165). IGI Global. https://doi.org/10.4018/978-1-6684-8913-0.ch006

[61]. Mamta, N. A., Gupta, B. B., Li, K.-C., Leung, V. C. M., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-Assisted Secure Fine-Grained Searchable Encryption for a Cloud-Based Healthcare Cyber-Physical System. *IEEE/CAA Journal of Automatica Sinica*, *8*(12), 1877-1890. https://doi.org/10.1109/jas.2021.1004003

[62]. Maniruzzaman, B., Mohammad Anisur, R., Afrin Binta, H., Md, A., & Anisur, R. (2023). Advanced Analytics And Machine Learning For Revenue Optimization In The Hospitality Industry: A Comprehensive Review Of Frameworks. *American Journal of Scholarly Research and Innovation*, *2*(02), 52-74. https://doi.org/10.63125/8xbkma40

[63]. McGhin, T., Choo, K.-K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications*, *135*(NA), 62-75. https://doi.org/10.1016/j.jnca.2019.02.027

[64]. Md, A., Rokhshana, P., Mahiya Akter, S., & Anisur, R. (2025). AI-Powered Personalization In Digital Banking: A Review Of Customer Behavior Analytics And Engagement. *American Journal of Interdisciplinary Studies*, *6*(1), 40- 71. https://doi.org/10.63125/z9s39s47

[65]. Md Arifur, R., Md Shakawat, H., Abdul Awal, M., & Siful, I. (2025). A Systematic Review of Intelligent Support Systems For Strategic Decision-Making Using Human-AI Interaction In Enterprise Platforms. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 506-543. https://doi.org/10.63125/a5yh1293

[66]. Md Jakaria, T., Md, A., Zayadul, H., & Emdadul, H. (2025). Advances In High-Efficiency Solar Photovoltaic Materials: A Comprehensive Review Of Perovskite And Tandem Cell Technologies. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 201-225. https://doi.org/10.63125/5amnvb37

[67]. Md Mahfuj, H., Md Rabbi, K., Mohammad Samiul, I., Faria, J., & Md Jakaria, T. (2022). Hybrid Renewable Energy Systems: Integrating Solar, Wind, And Biomass for Enhanced Sustainability And Performance. *American Journal of Scholarly Research and Innovation*, *1*(1), 1-24. https://doi.org/10.63125/8052hp43

[68]. Md Majharul, I., Arafat Bin, F., & Ripan Kumar, P. (2022). AI-Based Smart Coating Degradation Detection For Offshore Structures. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 01-34. https://doi.org/10.63125/1mn6bm51

[69]. Md Masud, K. (2022). A Systematic Review Of Credit Risk Assessment Models In Emerging Economies: A Focus On Bangladesh's Commercial Banking Sector. *American Journal of Advanced Technology and Engineering Solutions*, *2*(01), 01-31. https://doi.org/10.63125/p7ym0327

[70]. Md Takbir Hossen, S., Ishtiaque, A., & Md Atiqur, R. (2023). AI-Based Smart Textile Wearables For Remote Health Surveillance And Critical Emergency Alerts: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(02), 1-29. https://doi.org/10.63125/ceqapd08

[71]. Md Takbir Hossen, S., & Md Atiqur, R. (2022). Advancements In 3D Printing Techniques For Polymer Fiber-Reinforced Textile Composites: A Systematic Literature Review. *American Journal of Interdisciplinary Studies*, *3*(04), 32-60. https://doi.org/10.63125/s4r5m391

[72]. Mohammad Shahadat Hossain, S., Md Shahadat, H., Saleh Mohammad, M., Adar, C., & Sharif Md Yousuf, B. (2024). Advancements In Smart and Energy-Efficient HVAC Systems: A Prisma-Based Systematic Review. *American Journal of Scholarly Research and Innovation*, *3*(01), 1-19. https://doi.org/10.63125/ts16bd22

[73]. Ndayizigamiye, P., & Dube, S. (2019). Potential Adoption of Blockchain Technology to Enhance Transparency and Accountability in the Public Healthcare System in South Africa. *2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC)*, *NA*(NA), 1-5. https://doi.org/10.1109/imitec45504.2019.9015920

[74]. Nguyen, G. N., Le Viet, N. H., Elhoseny, M., Shankar, K., Gupta, B. B., & El-Latif, A. A. A. (2021). Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of Parallel and Distributed Computing*, *153*(NA), 150-160. https://doi.org/10.1016/j.jpdc.2021.03.011

[75]. Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors (Basel, Switzerland)*, *21*(15), 5119-NA. https://doi.org/10.3390/s21155119

[76]. Noor Alam, S., Golam Qibria, L., Md Shakawat, H., & Abdul Awal, M. (2023). A Systematic Review of ERP Implementation Strategies in The Retail Industry: Integration Challenges, Success Factors, And Digital Maturity Models. *American Journal of Scholarly Research and Innovation*, *2*(02), 135-165. https://doi.org/10.63125/pfdm9g02

[77]. Odeh, A. (2025). Healthcare data management using blockchain-enabled sensor networks. In (pp. 139-154). Elsevier. https://doi.org/10.1016/b978-0-443-36370-2.00009-8

[78]. Onik, M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019). Blockchain in Healthcare: Challenges and Solutions. In (Vol. NA, pp. 197-226). Elsevier. https://doi.org/10.1016/b978-0-12-818146-1.00008-8

[79]. Philip, A. O., & Saravanaguru, R. K. (2020). Secure Incident & Evidence Management Framework (SIEMF) for Internet of Vehicles using Deep Learning and Blockchain. *Open Computer Science*, *10*(1), 408-421. https://doi.org/10.1515/comp-2019-0022

[80]. Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. *Information*, *16*(2), 133-133. https://doi.org/10.3390/info16020133

[81]. Rafique, W., Khan, M., Khan, S., & Ally, J. S. (2023). SecureMed: A Blockchain-Based Privacy-Preserving Framework for Internet of Medical Things. *Wireless Communications and Mobile Computing*, *2023*(NA), 1-14. https://doi.org/10.1155/2023/2558469

[82]. Rahmadika, S., Astillo, P. V., Choudhary, G., Duguma, D. G., Sharma, V., & You, I. (2023). Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE journal of biomedical and health informatics*, *27*(2), 710-721. https://doi.org/10.1109/jbhi.2022.3187037

[83]. Rathore, H., Mohamed, A., & Guizani, M. (2020). A Survey of Blockchain Enabled Cyber-Physical Systems. *Sensors (Basel, Switzerland)*, *20*(1), 282-NA. https://doi.org/10.3390/s20010282

[84]. Ren, J., Li, J., Liu, H., & Qin, T. (2022). Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Science and Technology*, *27*(4), 760-776. https://doi.org/10.26599/tst.2021.9010046

[85]. Ripan Kumar, P., Md Majharul, I., & Arafat Bin, F. (2022). Integration Of Advanced NDT Techniques & Implementing QA/QC Programs In Enhancing Safety And Integrity In Oil & Gas Operations. *American Journal of Interdisciplinary Studies*, *3*(02), 01-35. https://doi.org/10.63125/9pzxgq74

[86]. Roksana, H. (2023). Automation In Manufacturing: A Systematic Review Of Advanced Time Management Techniques To Boost Productivity. *American Journal of Scholarly Research and Innovation*, *2*(01), 50-78. https://doi.org/10.63125/z1wmcm42

[87]. Roksana, H., Ammar, B., Noor Alam, S., & Ishtiaque, A. (2024). Predictive Maintenance In Industrial Automation: A Systematic Review Of IOT Sensor Technologies And AI Algorithms. *American Journal of Interdisciplinary Studies*, *5*(01), 01-30. https://doi.org/10.63125/hd2ac988

[88]. Rupa, C., MidhunChakkarvarthy, D., Patan, R., Prakash, A. B., & Pradeep, G. G. S. (2022). Knowledge engineering–based DApp using blockchain technology for protract medical certificates privacy. *IET Communications*, *16*(15), 1853-1864. https://doi.org/10.1049/cmu2.12439

[89]. Sakthi, U., & DafniRose, J. (2022). Blockchain-Enabled Smart Agricultural Knowledge Discovery System using Edge Computing. *Procedia Computer Science*, *202*(NA), 73-82. https://doi.org/10.1016/j.procs.2022.04.011

[90]. Sangwan, P., & Banita, N. A. (2024). Blockchain based Health Records Management for Diabetes Patients: Real-World Applications. *2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP)*, *NA*(NA), 488-498. https://doi.org/10.1109/tiacomp64125.2024.00088

[91]. Sarosh, P., Parah, S. A., Malik, B. A., Hijji, M., & Muhammad, K. (2023). Real-Time Medical Data Security Solution for Smart Healthcare. *IEEE Transactions on Industrial Informatics*, *19*(7), 8137-8147. https://doi.org/10.1109/tii.2022.3217039

[92]. Satamraju, K. P., & Malarkodi, B. (2020). Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare. *Sensors (Basel, Switzerland)*, *20*(5), 1389-NA. https://doi.org/10.3390/s20051389

[93]. Shahan, A., Anisur, R., & Md, A. (2023). A Systematic Review Of AI And Machine Learning-Driven IT Support Systems: Enhancing Efficiency And Automation In Technical Service Management. *American Journal of Scholarly Research and Innovation*, *2*(02), 75-101. https://doi.org/10.63125/fd34sr03

[94]. Shu, H., Qi, P., Huang, Y., Chen, F., Xie, D., & Sun, L. (2020). An Efficient Certificateless Aggregate Signature Scheme for Blockchain-Based Medical Cyber Physical Systems. *Sensors (Basel, Switzerland)*, *20*(5), 1521-NA. https://doi.org/10.3390/s20051521

[95]. Shynu, P. G., Menon, V. G., Kumar, R. L., Kadry, S., & Nam, Y. (2021). Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. *IEEE Access*, *9*(NA), 45706-45720. https://doi.org/10.1109/access.2021.3065440

[96]. Siddiqui, N. A. (2025). Optimizing Business Decision-Making Through AI-Enhanced Business Intelligence Systems: A Systematic Review of Data-Driven Insights in Financial And Strategic Planning. *Strategic Data Management and Innovation*, *2*(1), 202-223. https://doi.org/10.71292/sdmi.v2i01.21

[97]. Sohel, R. (2025). AI-Driven Fault Detection and Predictive Maintenance In Electrical Power Systems: A Systematic Review Of Data-Driven Approaches, Digital Twins, And Self-Healing Grids. *American Journal of Advanced Technology and Engineering Solutions*, *1*(01), 258-289. https://doi.org/10.63125/4p25x993

[98]. Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). Blockchain Technology for Secured Healthcare Data Communication among the Non-Terminal Nodes in IoT Architecture in 5G Network. *Electronics*, *10*(12), 1437-NA. https://doi.org/10.3390/electronics10121437

[99]. Subramani, J., Azees, M., Rajasekaran, A. S., Aljaedi, A., Bassfar, Z., & Jamal, S. S. (2024). Blockchain-Enabled Secure Data Collection Scheme for Fog-Based WBAN. *IEEE Access*, *12*(NA), 38287-38297. https://doi.org/10.1109/access.2024.3351844

[100]. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*(NA), 102407-NA. https://doi.org/10.1016/j.jisa.2019.102407

[101]. Ting, L., Khan, M., Sharma, A., & Ansari, M. D. (2022). A secure framework for IoT-based smart climate agriculture system: Toward blockchain and edge computing. *Journal of Intelligent Systems*, *31*(1), 221-236. https://doi.org/10.1515/jisys-2022-0012

[102]. Tlemçani, K., Azbeg, K., Saoudi, E., Fetjah, L., Ouchetto, O., & Jai Andaloussi, S. (2025). Empowering Diabetes Management Through Blockchain and Edge Computing: A Systematic Review of Healthcare Innovations and Challenges. *IEEE Access*, *13*, 14426-14443. https://doi.org/10.1109/access.2025.3531350

[103]. Tlemçani, K., Jai Andaloussi, S., Azbeg, K., Ouchetto, O., & Fetjah, L. (2023). An Advanced IoT-Based Architecture for Healthcare Systems: A Focus on Blockchain-based Edge Computing for Diabetes Management. *Proceedings of the 6th International Conference on Networking, Intelligent Systems & Security*, *NA*(NA), 1-7. https://doi.org/10.1145/3607720.3607756

[104]. Tonoy, A. A. R., & Khan, M. R. (2023). The Role of Semiconducting Electrides In Mechanical Energy Conversion And Piezoelectric Applications: A Systematic Literature Review. *American Journal of Scholarly Research and Innovation*, *2*(01), 01-23. https://doi.org/10.63125/patvqr38

[105]. Tyagi, A. K., Aswathy, S. U., Aghila, G., & Sreenath, N. (2021). AARIN: Affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology. *International Journal of Intelligent Networks*, *2*(NA), 175-183. https://doi.org/10.1016/j.ijin.2021.09.007

[106]. Ullah, F., He, J., Zhu, N., Wajahat, A., Nazir, A., Qureshi, S., Pathan, M. S., & Dev, S. (2024). Blockchain-enabled EHR access auditing: Enhancing healthcare data security. *Heliyon*, *10*(16), e34407-e34407. https://doi.org/10.1016/j.heliyon.2024.e34407

[107]. Umamaheswari, S., Sreeram, S., Kritika, N., & Prasanth, D. R. J. (2019). BIoT: Blockchain based IoT for Agriculture. *2019 11th International Conference on Advanced Computing (ICoAC)*, *NA*(NA), NA-NA. https://doi.org/10.1109/icoac48765.2019.246860

[108]. Vangala, A., Das, A. K., Kumar, N., & Alazab, M. (2021). Smart Secure Sensing for IoT-Based Agriculture: Blockchain Perspective. *IEEE Sensors Journal*, *21*(16), 17591-17607. https://doi.org/10.1109/jsen.2020.3012294

[109]. Verma, G. (2022). Blockchain-based privacy preservation framework for healthcare data in cloud environment. *Journal of Experimental & Theoretical Artificial Intelligence*, *36*(1), 147-160. https://doi.org/10.1080/0952813x.2022.2135611

[110]. Vinayasree, P., & Reddy, A. M. (2025). A Reliable and Secure Permissioned Blockchain‐Assisted Data Transfer Mechanism in Healthcare‐Based Cyber‐Physical Systems. *Concurrency and Computation: Practice and Experience*, *37*(3). https://doi.org/10.1002/cpe.8378

[111]. Wenhua, Z., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics*, *12*(3), 546-546. https://doi.org/10.3390/electronics12030546

[112]. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, *21*(3), 2794-2830. https://doi.org/10.1109/comst.2019.2899617

[113]. Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., de Oliveira, M. T., Krefting, D., Penzel, T., Bowden, J., Bellika, J. G., & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. In (Vol. NA, pp. 335-362). Elsevier. https://doi.org/10.1016/b978-0-12-823413-6.00014-8

[114]. Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications*, *25*(6), 12-18. https://doi.org/10.1109/mwc.2017.1800116

[115]. Zaman, S. (2024). A Systematic Review of ERP And CRM Integration For Sustainable Business And Data Management in Logistics And Supply Chain Industry. *Frontiers in Applied Engineering and Technology*, *1*(01), 204-221. https://doi.org/10.70937/faet.v1i01.36

[116]. Zhang, L., Minghui, P., Wang, W., Jin, Z., Su, Y., & Chen, H. (2021). Secure and efficient data storage and sharing scheme for blockchain‐based mobile‐edge computing. *Transactions on Emerging Telecommunications Technologies*, *32*(10), NA-NA. https://doi.org/10.1002/ett.4315

[117]. Zhang, P., White, J., Schmidt, D. C., Lenz, G., & Rosenbloom, S. T. (2018). FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. *Computational and structural biotechnology journal*, *16*(NA), 267-278. https://doi.org/10.1016/j.csbj.2018.07.004

[118]. Zhao, Y., Li, Q., Yi, W., & Xiong, H. (2023). Agricultural IoT Data Storage Optimization and Information Security Method Based on Blockchain. *Agriculture*, *13*(2), 274-274. https://doi.org/10.3390/agriculture13020274