Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.061965

REVIEW

MediGuard: A Survey on Security Attacks in Blockchain-IoT Ecosystems for e-Healthcare Applications

Shrabani Sutradhar[1,2], Rajesh Bose[3], Sudipta Majumder[1], Arfat Ahmad Khan[4,*], Sandip Roy[3], Fasee Ullah[5] and Deepak Prashar[6,7]

[1]Institute of Engineering and Technology, Dibrugarh University, Dibrugarh, 786004, Assam, India
[2]Departments of Computational Sciences, Brainware University, Kolkata, 700125, West Bengal, India
[3]Department of Computer Science & Engineering, JIS University, Kolkata, 700109, West Bengal, India
[4]Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, 40002, Thailand
[5]Department of Computer and Information Sciences, Universiti Teknologi PETRONAS, Seri Iskandar, 32610, Perak Darul Ridzuan, Malaysia
[6]Department of Computer Science and Engineering (CSE), Lovely Professional University, Phagwara, 144411, Punjab, India
[7]Jadara University Research Center, Jadara University, Irbid, 21110, Jordan

*Corresponding Author: Arfat Ahmad Khan. Email: arfatkhan@kku.ac.th

Received: 06 December 2024; Accepted: 07 April 2025; Published: 19 May 2025

ABSTRACT: Cloud-based setups are intertwined with the Internet of Things and advanced, and technologies such as blockchain revolutionize conventional healthcare infrastructure. This digitization has major advantages, mainly enhancing the security barriers of the green tree infrastructure. In this study, we conducted a systematic review of over 150 articles that focused exclusively on blockchain-based healthcare systems, security vulnerabilities, cyberattacks, and system limitations. In addition, we considered several solutions proposed by thousands of researchers worldwide. Our results mostly delineate sustained threats and security concerns in blockchain-based medical health infrastructures for data management, transmission, and processing. Here, we describe 17 security threats that violate the privacy and data integrity of a system, over 21 cyber-attacks on security and QoS, and some system implementation problems such as node compromise, scalability, efficiency, regulatory issues, computation speed, and power consumption. We propose a multi-layered architecture for the future healthcare infrastructure. Second, we classify all threats and security concerns based on these layers and assess suggested solutions in terms of these contingencies. Our thorough theoretical examination of several performance criteria—including confidentiality, access control, interoperability problems, and energy efficiency—as well as mathematical verifications establishes the superiority of security, privacy maintenance, reliability, and efficiency over conventional systems. We conducted in-depth comparative studies on different interoperability parameters in the blockchain models. Our research justifies the use of various positive protocols and optimization methods to improve the quality of services in e-healthcare and overcome problems arising from laws and ethics. Determining the theoretical aspects, their scope, and future expectations encourages us to design reliable, secure, and privacy-preserving systems.

KEYWORDS: Blockchain; internet of medical things; cloud infrastructure; cyber-attacks; privacy issues

1 Introduction

In contemporary society, good health is fundamental to human well-being, profoundly influencing the quality of life and happiness. While money does not guarantee good health, it can buy access to essential medical services. Effective healthcare, including prevention, diagnosis, treatment, and rehabilitation, is

crucial for maintaining and improving health outcomes, a collective endeavor aimed at equitable access to services (Gupta et al., 2022) [1]. The World Health Organization (WHO) defines health as a state of complete physical, mental, and social well-being, emphasizing the multifaceted nature of health. Recent technological advancements and digitalization have transformed healthcare. Automation enhances efficiency, accuracy, and cost-effectiveness, thus reducing errors. Digital technologies like the Internet of Medical Things (IoMT), machine learning, and wearable sensors have further improved patient care and operational efficiency. The healthcare industry comprises six major sectors: biotechnology, equipment and supplies, services, facilities, life science toads & services, and pharmaceuticals.

Healthcare services, both medical and non-medical, enhance patient health [2]. Advancements such as online consultations and medication delivery have redefined healthcare delivery, integrating technology to improve patient experiences [2,3]. Patient satisfaction, which is crucial for high-quality healthcare service, is influenced by factors like responsiveness and staff quality [4]. Technological innovations drive cost-effective, efficient healthcare with improved patient outcomes [5]. Post-pandemic digital technologies such as IoMT, machine learning, and wearable sensors are essential for efficient and affordable healthcare. These innovations enable real-time patient monitoring and personalized care, thereby reducing costs.

There are many significant research gaps in the current healthcare situation that require immediate attention. Modern healthcare infrastructures have enormous interoperability problems on various platforms, and current decentralized and blockchain systems are unable to meet the requirements for smooth data integration. Crisis-grade security vulnerabilities persist in medical software, wireless networks, and cloud computing, leading to widespread data leaks and patient data theft. In IoMT networks, issues such as cloning attacks, masquerading, de-synchronization, and node compromise remain inadequately addressed. The computational speed, power consumption, and technology scalability limits along with the standardization and key management issues in IoMT pose significant operational challenges. Although cloud integration improves efficiency and lowers costs, particularly in the developing world, centralized storage of IoMT-led data poses tremendous security and privacy issues [6,7]. Cloud technology simplifies procedures such as medical imaging and emergency treatment, thereby facilitating the time tracking of patients and enhancing patient-provider communication. Although blockchain technology's decentralized and unchangeable setup holds great hope for secure solutions in the protection of medical information, existing studies do not have end-to-end solutions to meet these security challenges effectively. Thus, this study proposes a systematic literature review to determine the vulnerabilities, privacy issues, attacks, and holistic solutions to improve the security of electronic healthcare systems.

1.1 Objectives

Our survey provides a comprehensive overview of the blockchain, IoMT, and healthcare applications. By reviewing the literature from 2010 to 2023, this study focuses on various attacks against the blockchain-IoMT integrated healthcare system. The focus lies on investigating the difficulties and vulnerabilities present at each layer of these technologies, represented with Fig. 1, with the aim of strengthening the privacy protection and security measures employed in e-healthcare systems. The objectives of this survey are as follows:

- To analyze the motivations and challenges in integrating blockchain with IoMT, focusing on security, privacy, interoperability, and unresolved issues (2010–2023).
- This study proposes layered blockchain architecture for healthcare systems to address security threats and enhance data integrity, scalability, and efficiency.
- To investigate IoMT-driven healthcare vulnerabilities, including device authentication, unauthorized access, privacy leaks, and smart contract weaknesses.

- To assess healthcare data management risks by considering storage trade-offs, network threats, regulatory compliance, and privacy-preserving solutions.
- To compare blockchain-based healthcare systems with traditional models, highlighting improvements in security, interoperability, fraud prevention, and patient control.

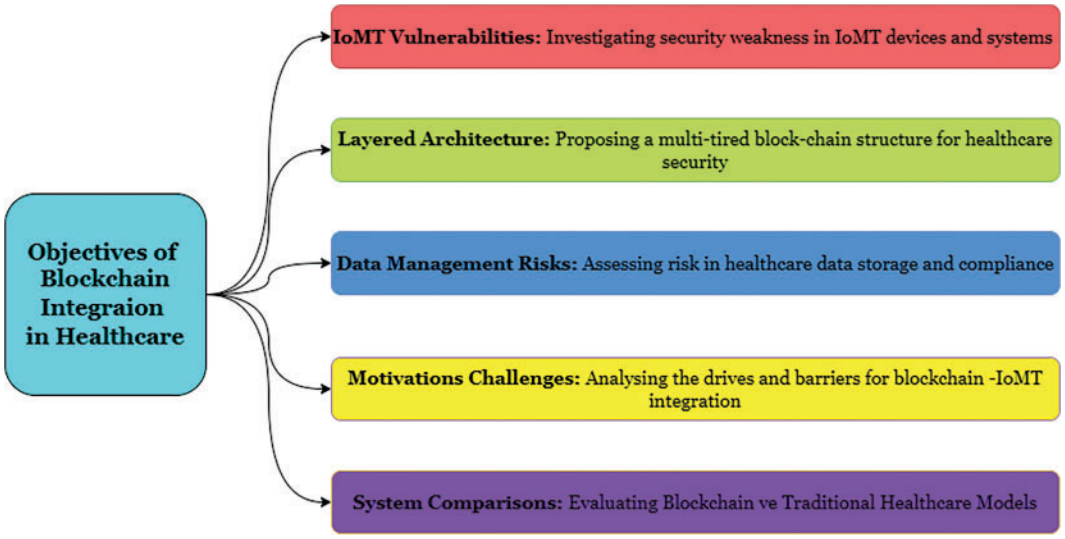

Figure 1: Objectives of the work

1.2 Contribution and Validation

Our research contributes to healthcare security in several ways by filling in current research and practice. With sound methodology and thorough analysis, we have confirmed our research goals and safeguarding sensitive healthcare information and systems. The following points summarize the originality and contribution of our research, setting it apart from earlier studies in this area.

Objective 1: To examine the motivations and challenges in blockchain-IoMT integration (2010–2023)

➢ **Validation:** Our analysis validates Objective 1 by systematically examining 17 threats, 21 attacks, and 16 challenges in blockchain-IoMT integration across 2010–2023, establishing clear insights into security trends and adoption motivations.

Objective 2: To propose layered blockchain architecture for healthcare systems

➢ **Validation:** Creation of a multi-layered architectural framework that systematically classifies and analyses blockchain-based healthcare systems in an organized manner, offering a systematic approach to testing proposed solutions against determined security contingencies in subsequent healthcare infrastructure development.

Objective 3: To examine IoMT-led healthcare vulnerabilities an in-depth analysis of the security land scapeape

➢ **Validation:** This study addresses device authentication, unauthorized access, and smart contract vulnerabilities. However, these particular aspects are not clearly expressed.

Objective 4: Evaluate risks in healthcare data management: A solution-focused framework and implementation strategy

➢ **Validation:** These contributions address healthcare data management risks using an integrated mathematical framework that maximizes storage trade-offs, guarantees regulatory compliance, and enforces effective network security measures. The solution-oriented approach maximizes scalability, privacy preservation, and regulatory compliance while reducing risks through practical implementations.

Objective 5: To compare blockchain-based healthcare systems with traditional healthcare systems. A practical implementation strategy.

➢ **Validation:** Our contributions are demonstrated through comprehensive security analysis techniques, including formal verification, penetration testing, threat modelling, and performance benchmarking, with each objective systematically validated using industry-standard tools and quantifiable metrics such as analysis of threats, attacks, and challenges across the blockchain-IoMT integration landscape.

This study offers a uniquely comprehensive and structured approach to analysing the current state and future potential of blockchain technology in healthcare, with a strong focus on security, privacy, and practical implementation challenges. We arrange this paper in a unique graphical manner in Fig. 2, which and every objective within an individual standalone section.

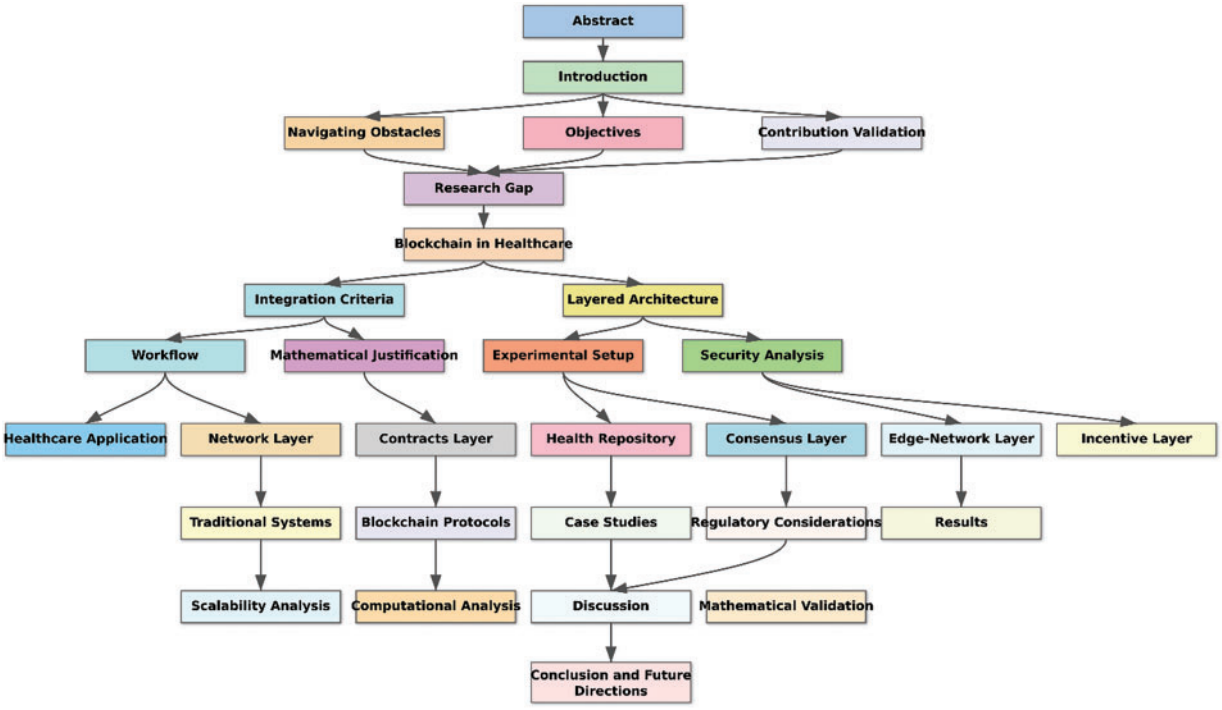

Figure 2: Structure of the paper

2 Navigating Obstacles to Existing Solutions

The shifting healthcare technology environment has demanded multifaceted measures to ensure and process medical data in a secure and efficient manner. Table 1 displays an analysis of 11 technological models and algorithms alongside the startle trade-off between innovation and security concerns within healthcare platforms. The evaluation includes standard cloud-based systems through the adoption of more innovative blockchain frameworks as well as integrating nascent technologies like Internet of Things (IoT), Artificial Intelligence (AI) analysis, and 5G networks. Such a systematic comparison provides a basis for grasping

today's technology context in healthcare security and determines what areas need research and the areas that require development.

Table 1: Comparative analysis of healthcare security models and technologies using the existing method

Feature category	Proposed method	Similar existing methods	Distinctive advantages	Implementation challenges	References
Security protocol	Zero-Knowledge Proofs (ZKP)	Traditional Advanced Encryption Standard (AES)	Privacy preservation during verification	Higher computational overhead	[8,9]
	Homomorphic Encryption	SHA-256	Computation of the encrypted data	Complex key management	[8,10,11]
	Multilayer authentication	Single-layer authentication	Enhanced security without data exposure	Integration complexity	[11–13]
Blockchain consensus	Delegated Proof-of-Stake (DPoS)	Proof-of-Work (PoW)	Reduced energy consumption	Validator selection complexity	[14–16]
	Hybrid validation framework	Basic Proof-of-Stake (PoS)	Faster transaction validation	Potential centralization risks	[17–19]
Data architecture	Hybrid Off-Chain Storage	Complete on-chain storage	Optimal storage efficiency	Complex data synchroniza-tion	[20–22]
	Distributed metadata management	Centralized databases	Maintained data integrity	Metadata management overhead	[23–25]
	Smart contract-based indexing	Traditional indexing	Reduced blockchain bloat	Cross-chain communication	[26–28]
Access control	Attribute-Based Encryption (ABE)	Role-Based Access Control (RBAC)	Fine-grained access control	Performance overhead	[12,29,30]
	Blockchain identity management	Static permission systems	Patient-centric permissions	Complex attribute management	[31–33]
	Dynamic consent system	Centralized authentication	Improved privacy management	Update propagation delays	[34–36]

(Continued)

Table 1 (continued)

Feature category	Proposed method	Similar existing methods	Distinctive advantages	Implementation challenges	References
Scalability solution	Sharding implementation	Single-chain architecture	Higher transaction throughput	Cross-shard communication	[37–39]
	Layer-2 scaling	Traditional database scaling	Reduced network congestion	Data consistency challenges	[40–42]
	Parallel processing	Sequential processing	Improved response time	Infrastructure requirements	[43–45]
Smart contract security	Formal verification	Basic deployment testing	Proactive vulnerability detection	Resource-intensive verification	[46–48]
	Fuzzy testing	Manual code review	Mathematically verified security	Complex formal proof requirements	[49–51]
	Automated vulnerability scanning	Standard unit tests	Automated risk mitigation	Tool integration challenges	[52–54]
Network infrastructure	5G integration	Traditional network protocols	Lower latency	Infrastructure cost	[23,49,50]
	Edge computing support	Centralized computing	Enhanced real-time processing	Network security concerns	[55–57]
	IoT device compatibility	Limited device support	Improved device integration	Compatibility issues	[58–60]
Data privacy	Multi-layered encryption	Single-layer encryption	Enhanced data protection	Processing overhead	[11–13]
	Consent-based sharing	Fixed sharing rules	Flexible sharing mechanisms	Complex key distribution	[61–63]
	Privacy-preserving analytics	Direct data analysis	Secure analytics capability	Performance impact	[64–66]

In the context of blockchain-IoMT-integrated healthcare systems, various security challenges and privacy concerns persist. Table 2 summarizes these issues along with existing solutions that demonstrate the multi-faceted nature of security challenges and privacy concerns in blockchain-IoMT integrated healthcare systems.

Table 2: Existing privacy issues and solutions

Security challenge	Existing solutions	References
Authentication issues	Robust authentication	[13,67]
Access control vulnerabilities	Access control strengthening	[12,31–33,68,69]
Cryptography weaknesses	Cryptographic protocol enhancement	[32,70,71]
Loss, theft, and disclosure of personal information	Identity protection	[26,72–75,49]
Cloning attacks	Robust encryption	[27,76–78]
Node compromise	Multi-factor authentication	[64,79–81]
Scalability, efficiency, and regulatory challenges	Secure communication protocols	[82–84]
Non-repudiation	Redundancy measures	[85–87]
"3A Problem: Authentication, Authorization, Availability"	Intrusion detection systems	[28,69,88,89]
Data volume	Secure communication protocols	[20,21,22]
Privacy protection	IoT node privacy enhancement	[8,9,36,62–64,90]
Man-in-the-Middle (MitM) attacks	Cryptographic protection	[91–93]
Denial of Service (DoS) attacks	Suspected base station detection	[94–96]
Data leakage and exposure	Privacy-preserving techniques	[52–54,97]
Sensors and devices lose connections to the real network	Robust authentication mechanism	[23–25,51,70,98]
Poorly implemented encryption process	Blockchain privacy solutions	[54,99–101]
Speed of the computation	Lightweight security protocols	[102–105]
Power consumption	Energy-efficient security	[55–57]
Scalability	Scalable security algorithms	[39,94,95,106]
Standard security protocol issues in the IoMT communication channel	Interoperable security protocols	[58–60,107–109]

3 Research Gap

Through a comprehensive analysis of Healthcare Security Models and Technologies, as presented in Tables 1 and 2, our research identifies critical gaps in current healthcare security approaches [110]. Although individual technologies such as blockchain, IoMT, cloud computing, and various security measures demonstrate specific strengths, their isolated implementation is insufficient for modern healthcare demands. Table 3 categorizes these gaps into five key areas: Security & Privacy Fundamentals, Interoperability & Data Management, Authentication & Access Control, Technical Infrastructure, and blockchain and advanced solutions.

Table 3: Research gap analysis on healthcare security systems

Category	Current limitations	Challenges	References
Fundamentals of security and privacy	- Limited holistic security approach, inadequate - Inadequate integration of emerging technologies - Insufficient privacy protection mechanisms	- Balancing accessibility with security - Managing complex technology convergence - Ensuring comprehensive privacy protection	[109,111–114]
Interoperability and Data Management	- Poor cross-platform compatibility, limited - Limited data exchange capabilities - Vulnerable data storage systems	- Achieving seamless system integration, preventing data breaches, and maintaining-Preventing - Preventing data breaches - Maintaining data integrity	[109,115,116]
Authentication & Access Control	- Weak authentication mechanisms - Inadequate access control systems - Vulnerable cryptographic implementations	- Preventing unauthorized access, managing - Managing IoMT security threats - Addressing node compromise risks	[35,67,71,117–119],
Technical Infrastructure	- Limited computational capabilities, high power consumption, poor scalability, inadequate - High power consumption - Poor scalability - Inadequate standardization	- Optimizing resource usage, implementing - Implementing efficient key management - Developing scalable solutions	[89,116,120,121]
Blockchain and Advanced Solutions	- Incomplete security frameworks, limited integration capabilities, insufficient - Limited integration capabilities - Insufficient patient privacy measures	- Creating comprehensive security solutions, ensuring, ensuring, ensuring–Ensuring - Ensuring patient data privacy - Maintaining regulatory compliance	[34,117,122–124]

We focus on these issues. Our analysis reveals the necessity for an integrated solution that combines blockchain security, IoMT's real-time capabilities, cloud computing's scalability, and robust security measures. This research aims to address these gaps by developing a comprehensive framework that ensures data integrity, patient privacy, and seamless interoperability across interconnected healthcare systems.

4 Blockchain in Healthcare

Blockchain is an innovative distributed ledger technology that securely records and transmits data in a decentralized, transparent, and immutable manner across a network of computers. The applications of blockchain in healthcare extend far beyond record-keeping. By leveraging blockchain's capabilities, the

healthcare industry can benefit from improved interoperability, enhanced data integrity, and increased transparency. The benefits of blockchain in healthcare are illustrated in Fig. 3.

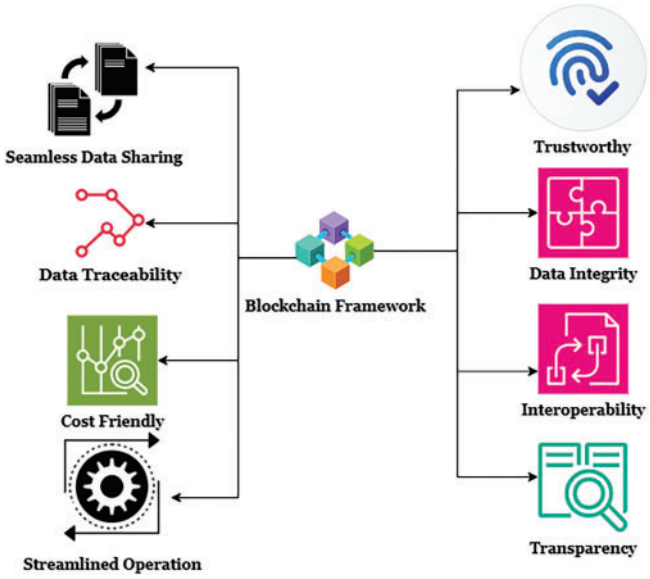

Figure 3: Advantages of the blockchain in healthcare

Essential Criteria for Integrating Blockchain into Healthcare

Blockchain technology is indispensable to the healthcare industry because of its ability to address numerous critical requirements that have long plagued the healthcare industry. They are expressed as follows:

- Secure storage and seamless sharing of sensitive medical data, such as electronic health records (EHRs) and patient information among authorized stakeholders, ensuring data integrity, confidentiality, and controlled access [125].
- Facilitating seamless data integration and interoperability among fragmented healthcare systems, thereby enabling a comprehensive view of patient information across multiple healthcare entities [124].
- Maintaining transparency and traceability in healthcare processes, such as supply chain management, clinical trials, and medication tracking, enhancing accountability, and reducing the risk of counterfeit drugs and data tampering [125,126].

  Enabling patients to have greater control over their medical data and facilitating patient-centric healthcare systems by securely sharing medical records with authorized healthcare providers [127–129].
- Ensuring trust and accountability in healthcare systems by reducing the risk of fraud and data manipulation and ensuring the authenticity of medical records [126,130,131].
- Improving the efficiency and cost-effectiveness of healthcare operations by streamlining processes like claims processing, revenue cycle management, and physician credentialing [120,132,133].
- Facilitating medical research, clinical trials, and the development of innovative healthcare solutions while maintaining data integrity and patient privacy through secure and transparent data-sharing capabilities [125].

Although challenges exist, the potential of blockchain in healthcare is promising and poised to reshape the future of this industry. Its ability to securely share and manage data across different stakeholders,

from patients to providers and researchers, could revolutionize healthcare delivery and drive better patient outcomes [132,134].

5 Layered Blockchain Architecture for Healthcare Systems

During our investigation, we found that all attacks or problems did not affect the entire blockchain-enabled healthcare system. In contrast, each attack or issue is localized to specific components or layers in the architecture [135]. This section clearly addresses the objectives of Objective 2. To effectively mitigate these problems, it is essential to identify the exact layer or layers of the system that will be affected. The affected layers can then be identified and tailored in conjunction with the remediation strategies. In the initial phase of challenge identification and its categorization in relation to the affected layer, we divided the entire blockchain-enabled healthcare system into seven distinct layers. This step helps perform a systemic analysis of the identified vulnerabilities and mitigation efforts. Each layer is intended for a specific purpose; all layers help improve the security, efficiency, and trustworthiness of the system. In other words, resilience, privacy, and integrity issues are addressed within the appropriate layer(s) in blockchain-enabled healthcare ecosystems. A detailed discussion of each is presented in Fig. 4 as follows:

- **Edge Layer:** This layer represents the foundational layer and is the first stage of data collection and processing. The system consists of a network of IoMT devices, from wearable sensors to medical imaging devices and home monitoring systems, that capture patients' physiological data in real-time. A critical portion of the edge layer has secure connectivity to process data processing and provides initial data filtering and analysis [136].
- **Application Layer:** This layer is the interface layer between a patient, healthcare provider, or administrator through mobile apps, web portals, and advanced analytics tools that enable access to medical records, appointment scheduling, real-time data visualization, and the issuance of alerts and notifications.
- **Smart Contract Layer:** This layer integrates smart contracts into blockchains to automate processes while ensuring the transparency of the agreements. Smart contracts can be called self-executing contacts that are written directly into lines of code with predetermined conditions and actions. This automated process generates insurance claims, patient consent, and supply chain management.
- **Incentive Layer:** This layer contains incentive reward mechanisms for the participants through token rewards, discounts, reputation points, etc. This can be integrated with the smart contracts to automate reward mechanisms, comply with healthcare protocols, and issue penalties or rewards.
- **Consensus Layer:** This layer ensures data integrity, security, and consensus in a blockchain-integrated distributed network. The propagation, mining, and consensus protocols comprise the consensus layer. The Propagation Protocol is concerned with the actual dissemination of transactions and blocks across a network, using methods like Gossip Protocol to ensure that all nodes are updated. Finally, the Mining Protocol defines rules regarding the creation of new blocks, such as how miners compete to solve cryptographic puzzles, usually through Proof of Work, and delineates the validation and reward processes. The Consensus Protocol is used to ensure that all nodes are in the same blockchain version. It uses different mechanisms for consensus, such as Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance, and Delegated Proof of Stake, to validate transactions and preserve a single copy of truth, thus deterring fraudulent activities. These components make it possible to manage data efficiently, securely, and consistently within the network.
- **Network Layer:** This layer offers smooth interoperability and a robust network structure. The layer is composed of many multiple interlinked nodes. Full nodes are bigger nodes with more storage that store the entire blockchain and independently validate transactions and blocks. Light nodes only store a subset of the blockchain and rely on full nodes for validation. It has protocols and standards, including

Health Level Seven International (HL7), Fast Healthcare Interoperability Resources (FHIR), and Digital Imaging and Communications in Medicine (DICOM), for efficient communication between IoMT device diversity and healthcare systems; simultaneously, it relies upon dependable high-speed network connectivity. P2P: The peer-to-peer principle implies direct communication between nodes without depending upon the central server. Encryption and authentication mechanism associated with the nodes for secure communication.

- **Data Management Layer:** This layer encompasses data collection and aggregation, secure data storage, and robust privacy and security mechanisms. It gathers real-time data from various IoMT devices, aggregates this data for analysis, and provides secure and scalable storage solutions, with a blockchain used for storing metadata and ensuring data integrity, while large-scale databases store the actual data.

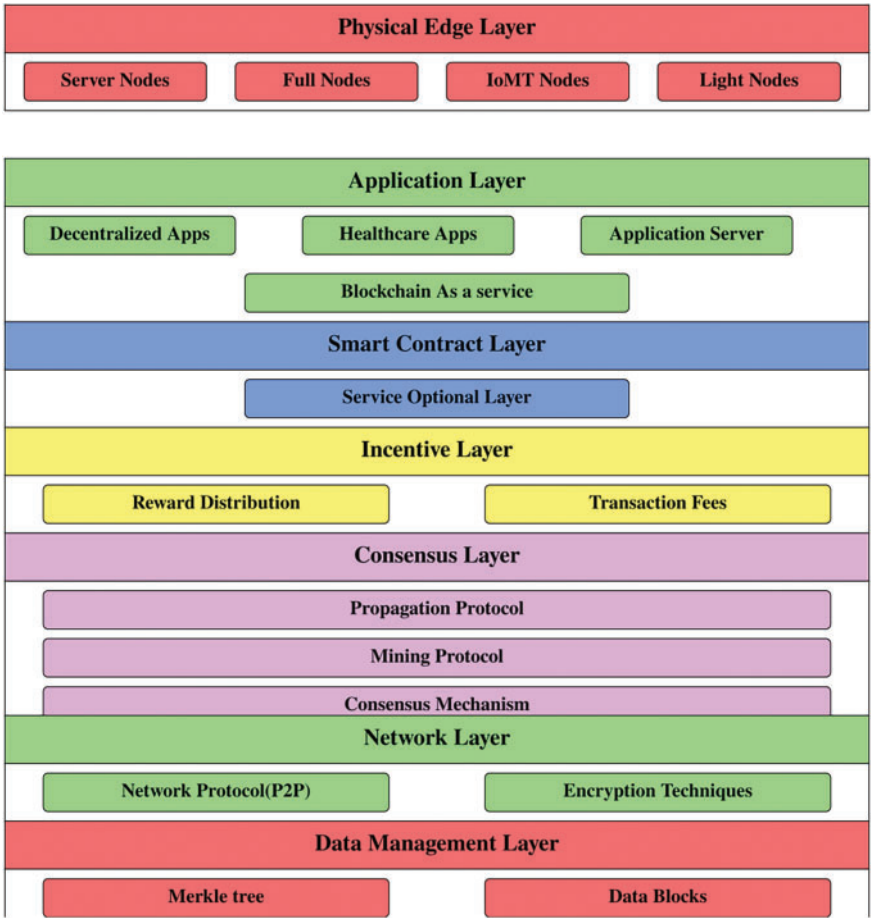

Figure 4: Blockchain-enabled layered architecture

Security, privacy, and trustworthiness in sharing and managing healthcare data are improved through a blockchain-enabled healthcare system with this layered architecture, ensuring an overall high-quality healthcare service delivery in a secure and efficient manner [137].

5.1 Workflow of the Proposed Architecture

The blockchain healthcare data management system employs four interlinked phases to support secure and efficient data management. The sequence diagram (Fig. 5) depicts a blockchain-based healthcare data

management system for the secure transmission, validation, and access control of medical records. The diagram depicts interactions among Patient/IoMT Devices, IoMT Gateway, Blockchain Network, Smart Contracts, Cloud Storage, and Healthcare Providers to enable secure data storage, validation, retrieval, and audit mechanisms.

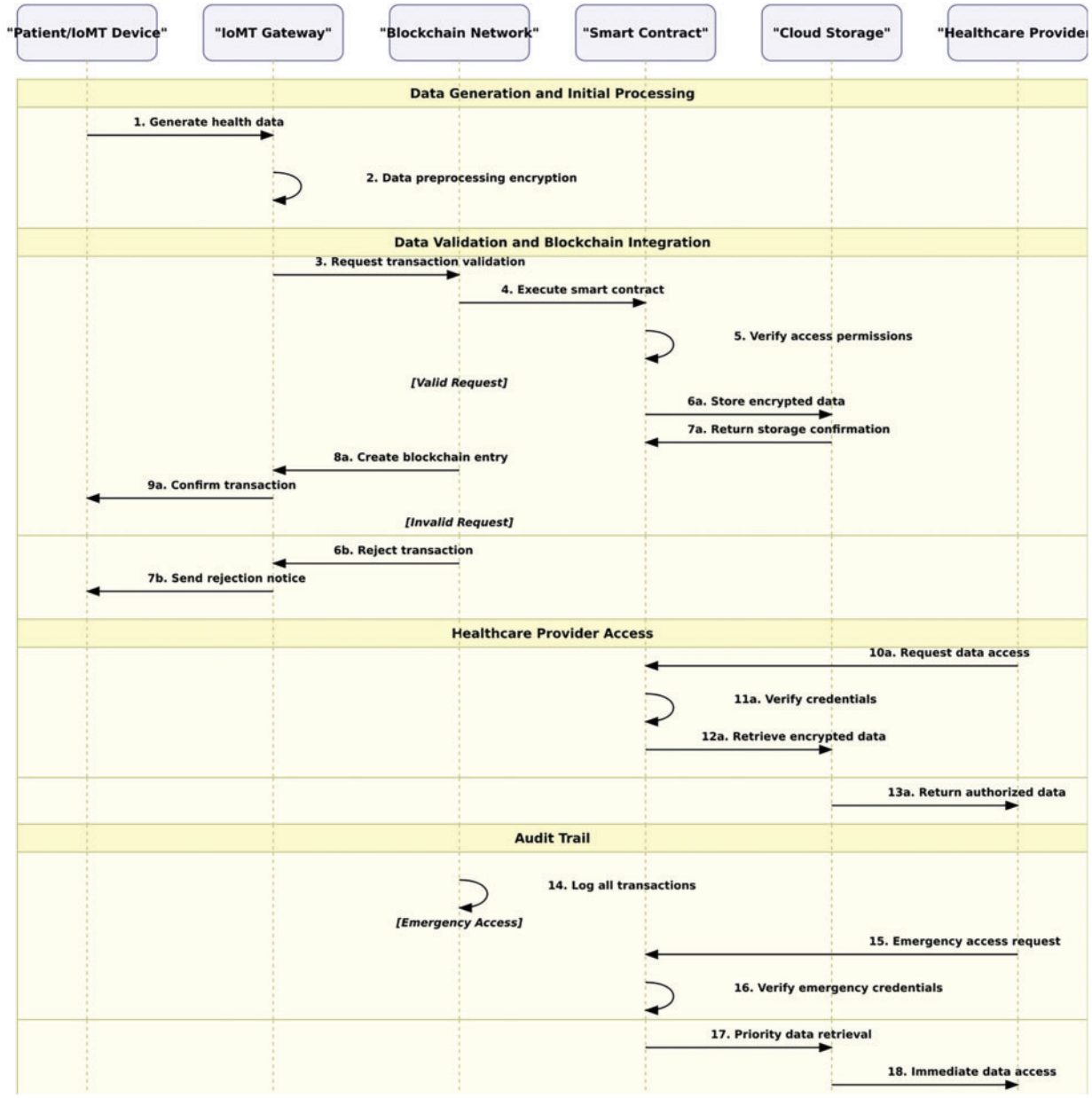

Figure 5: Sequence diagram of the proposed architecture

➢ **Phase 1: Data Generation and Initial Processing:** Starts with the Patient/IoMT Devices producing health data, which is first pre-processed and encrypted at the IoMT Gateway to set the first layer of security for private medical data.

- **Phase 2: Data Validation and Blockchain Integration:** Manages data validation via two possible flows. In the case of valid requests, the system runs a sequence of transaction validation, smart contract execution, permission check, encrypted data storage, and blockchain entry creation. In the event of invalid requests, the system triggers rejection procedures, dispatching suitable notifications without going further to data storage or blockchain entry creation.
- **Phase 3: Healthcare Provider Access:** Centres require secure data access. This phase handles the entire authentication process, from initial provider authentication and verification of credentials via smart contracts to the retrieval of secure data from cloud storage such that only registered healthcare providers can view patient data.
- **Phase 4: Audit Trail and Emergency Access:** These play two crucial roles. Standard transaction management continually documents all system activities to preserve an indelible audit trail, whereas the emergency protocol system facilitates rapid access through enhanced credential verification and prioritized data retrieval when life-or-death medical situations require immediate access to data.

This comprehensive workflow design balances stringent security controls with effective healthcare data accessibility in a decentralized setting while ensuring data protection and timely availability when required.

5.2 Mathematical Justification of the Blockchain-Enabled IoMT Healthcare System Algorithm

Our study offers a mathematical validation model for examining the blockchain-based IoMT healthcare system's security, privacy, and performance aspects. The model defines measurable metrics by examining the cryptographic attributes, encryption techniques, and computational complexity. The analysis focuses on three pivotal factors: data integrity using hash functions, privacy protection using hybrid encryption, and computational efficiency using consensus mechanisms.

5.2.1 Problem Formulation

In a blockchain-enabled Internet of Medical Things (IoMT) healthcare system, we consider a distributed network $N = \{n_1, n_2, \ldots, n_k\}$ of nodes that manage medical data transactions $T = \{t_1, t_2, \ldots, t_m\}$. The system must satisfy the following three primary constraints:

- Data Integrity: All transactions must be immutable and verifiable.
- Privacy: Access to medical data should be restricted to authorized entities.
- Efficiency: Operations must maintain the polynomial time complexity.

5.2.2 Mathematical Model

Data Integrity through Hashing

Here, let $H: \{0,1\}^* \rightarrow \{0,1\}^n$ be a cryptographic hash function that maps the input data to an n-bit hash value:

$H(t) = h(PK \,||\, h(t_{prev}) \,||\, data)$

Where:

- PK denotes the public key of the authorized entity.
- where t_{prev} denotes the hash of the previous transaction.
- || denotes concatenation;
- h is a secure hash function (e.g., SHA-256)

Privacy Preservation: The hybrid encryption scheme E combines asymmetric and symmetric encryption: $E(m) = (EPK(k), Ek(m))$

Where:

- EPK represents public key encryption.
- k is a randomly generated session key.
- Here, Ek denotes the symmetric encryption with the key k.
- where m represents the medical data.

Consensus Protocol

The Proof-of-Stake (PoS) consensus function C selects validators as follows:

$C(n_i) = P(s_i/S_{total})$

Where:

- s_i denotes the stake of node n_i.
- Here, S_{total} is the total stake in the network.
- Here, P is the selection probability, which gives the following.

5.2.3 Security Analysis

Integrity Proof: For any two distinct inputs $x_1 \neq x_2$: $P(H(x_1) = H(x_2)) \leq \varepsilon$

Where ε is negligibly small because of the collision resistance property of the hash function.

Privacy Proof: The proposed hybrid encryption scheme maintains confidentiality through the following steps:

1. Forward secrecy: Each session uses a unique key (k)
2. Public key security: Only the intended recipient can decrypt EPK(k)
3. Symmetric encryption security: Ek(m) is secure if k remains private

Efficiency Proof: The proposed system maintains the following polynomial time complexity:

1. Hashing: O(n) per transaction.
2. Encryption: O(log n) for public key operations
3. Consensus: O(k) for stake-based selection, where n is the input size and k is the number of nodes.

5.2.4 Complexity Analysis

The total system complexity T(n) is bounded by

$T(n) = O(n) + O(\log n) + O(k) = O(n)$

This ensures the efficient real-time processing of medical data transactions.

The mathematical model confirms our blockchain-based IoMT system's security and efficiency using key parameters. Data integrity is ensured using cryptographic hashing with zero collision probability, and privacy is ensured using a hybrid encryption protocol. The system achieves polynomial time complexity using optimized consensus mechanisms, which ensures computational efficiency and scalability. These confirmations ensure that the system satisfies healthcare application requirements while ensuring HIPAA compliance and medical data protection standards [111].

5.3 Experimental Setup and Implementation Details for eHealthcare Security Applications

To authenticate the security and efficiency of blockchain-IoMT-based healthcare security applications, an intelligent attention-based deep convolutional learning (IADCL) model is proposed here, depicted

in the Table 4. The proposed model improves data security, privacy, and efficiency for medical record management.

Table 4: Experimental setup for the blockchain-enabled healthcare security system

Category	Specifications
Hardware	NVIDIA Tesla V100 GPU (32 GB VRAM), Intel Xeon Platinum 8260 (2.4 GHz, 24 cores), 128 GB RAM
Software	Python 3.8, TensorFlow 2.5, PyTorch 1.9, Hyperledger Fabric 2.2, Ubuntu 20.04 LTS
Algorithms	Intelligent attention-based deep convoluted learning (IADCL), Hybrid homomorphic encryption, attribute-based access control, delegated proof-of-stake (DPoS) Consensus, federated learning for IoMT security

Experimental Setup

The experimental setup comprises different constituents grouped under hardware and software and algorithms, as indicated in Table 4.

The IADCL model securely processes patient health records while using federated learning to share encrypted medical data without exposing raw patient information. The system incorporates blockchain-based access control techniques to provide higher security and keep sensitive medical records away from unauthorized access.

6 Security of the IoMT-Enabled Edge-Network Layer

This section focuses on Objective 1, examining the growth and impact of medical IoT (Internet of Medical Things) devices during and after the pandemic. The adoption of these interconnected devices has surged, enabling healthcare providers to offer services remotely and monitor patients in real-time. These edge networks are crucial for enhancing healthcare monitoring, reducing response times, and improving decision-making across the healthcare landscape. First, we identify and categorize various applications of the IoMT devices. For instance, remote patient monitoring extends traditional healthcare by allowing service providers to track patient data outside conventional settings. Telecommunication technology facilitates the delivery of medical services, such as disease diagnosis and treatment, transcending geographical boundaries. This involves using various medical devices and digital technologies to collect, transmit, and offload [132] data to edge servers. We have compiled and categorized these tools and technologies according to their IoMT applications, as presented in Table 5. This table provides a comprehensive overview of various medical devices and their uses, serving as a valuable resource for future research in the field.

Table 5: Various applications of the IoT-enabled healthcare system

Application type	Associated tools and technologies	References
Remote patient monitoring	ECG Monitor, body temperature sensor, accelerometer, blood pressure monitors, Wearable glucose monitors; Implantable glucose sensors; Implantable cardiac monitors; loop recorders, Pulse oximeters; Respiratory rate monitors	[133]

(Continued)

Table 5 (continued)

Application type	Associated tools and technologies	References
Disease prediction and tele-diagnosis	Smartwatches and fitness trackers; Smartphone Apps; Biometric Sensors; Genetic Testing Kits; Molecular Diagnostic kits; Biosensors; Lab-on-a-chip devices; Portable imaging devices; Devices with machine learning capabilities for predicting disease risks; Devices for personalized medicine and predicting disease based on genetic factors	[134]
Patient tracking	Radio Frequency Identification (RFID) tags or wristbands; RFID readers for real-time location tracking; Bluetooth Low Energy (BLE) Beacons; Wearable GPS trackers; GPS-enabled wristbands for tracking patients with cognitive impairments; Infrared (IR) and Ultrasound Sensors for tracking movement within rooms or designated areas; Video Monitoring Systems; Smart home equipment	[72]
Telemedicine and Telehealth services	High-definition webcams; Microphones and speakers; Video conferencing platforms (e.g., Zoom, Skype, Microsoft Teams); Remote Examination Devices: Digital stethoscopes for remote auscultation, Digital Otoscopes, Digital Derma scopes for remote examination, Digital Ophthalmoscopes for remote eye examinations, Vital Sign Monitors, Portable Tele-health Kits for remote consultations, Remote Patient Monitoring Devices, Tele rehabilitation Devices, Virtual reality (VR) systems for physical and occupational therapy, Sensor-enabled exercise equipment for remote monitoring and guidance	[43]
Remote or virtual surgery	Robotic surgical systems (e.g., da Vinci Surgical System), Robotic instruments controlled remotely by surgeons, Haptic Feedback Devices that provide tactile feedback to the surgeon during remote operations, High-Definition (HD) Cameras and Endoscopes during procedures, 3D imaging systems for enhanced visualization, Motion tracking sensors, Infrared (IR) and electromagnetic sensors for precise tracking of surgical tools, Virtual Reality headsets and displays for immersive surgical simulations and training, Augmented Reality overlays and projections for providing real-time guidance during procedures, Vital Sign Monitors, Sensors for monitoring anesthesia levels and other critical parameters, Communication and Collaboration Tools, Robotics Control and Tele-operation Systems for precise remote control of surgical robots, Artificial Intelligence (AI) and Machine Learning (ML) Systems for surgical planning, risk assessment, and decision support, Image analysis tools for augmented surgical guidance	[44,135]

(Continued)

Table 5 (continued)

Application type	Associated tools and technologies	References
Medical asset tracking and management	RFID tags attached to medical assets (e.g., equipment, devices, supplies), RFID readers installed at real-time location tracking (RTLS), Bluetooth Low Energy (BLE) Beacons, GPS Tracking Devices to track high-value medical assets, Handheld Barcode and QR Code Scanners, Infrared (IR) and Ultrasound Sensors, Motion and Proximity Sensors for monitoring asset locations within specific zones, Environmental Sensors for temperature-sensitive assets, Smartphone apps for asset tracking, inventory management, Asset Management Software: Cloud-based or on-premises software platforms for asset tracking	[136]
Environmental monitoring	Wireless/portable Temperature and Humidity Sensors, Particulate matter (PM) sensors for monitoring air pollutants and dust levels, Carbon dioxide (CO2) sensors for monitoring indoor air quality and ventilation, Volatile organic compound (VOC) sensors, Differential Pressure Sensors to ensure proper airflow and containment, Occupancy and Motion Sensors, Optimized HVAC systems and lighting, Light Sensors, Noise Sensors, Water Leak Detection Sensors in Sensors placed near water sources or sensitive areas, Integrated Environmental Monitoring Systems, Mobile Applications and Handheld Devices, Data loggers for collecting and storing environmental data, Wireless gateways for transmitting data from sensors to monitoring systems or cloud platforms	[137]
Medication adherence and management	Smart Pill Bottles and Automatic pill Dispensers to track medication intake, Ingestible Sensors confirming medication intake, Wearable devices (e.g., smart watches, fitness trackers) with medication reminder features, Mobile applications for tracking medication schedules and adherence, Biometric Sensors: Sensors integrated into pill bottles or dispensers for biometric authentication, Smart Packaging: to track medication tampering, expiration dates, and environmental conditions, Medication Management Software: pharmacy management systems	[45]
Assisted living and eldercare	Motion and Presence Sensors, Environmental Sensors, Wearable fitness trackers, GPS trackers for monitoring the location of individuals with cognitive impairments, Smart Home Sensors and Systems, Smart lighting and thermostat controls for energy efficiency and comfort, Smart door locks and entry systems for enhanced security, Medication Management Systems: Smart pill dispensers and reminders, Wander Management Systems, Emergency Call Systems: panic buttons; voice-activated devices, Robotic Assistants, Mobile Applications and Monitoring Platforms	[138]

(Continued)

Table 5 (continued)

Application type	Associated tools and technologies	References
Clinical research and trials	Wearable Devices, Remote Patient Monitoring Devices, Telehealth Devices, Mobile Health (mHealth) Applications, Biosensors and Lab-on-a-Chip Devices, Imaging Devices, Environmental Sensors, Location Tracking Devices, Data Collection and Management Systems	[139]
Hospital management and optimization	Building Management Systems (BMS): Sensors for monitoring energy consumption, Smart Facilities Management, Predictive maintenance sensors for identifying potential equipment failures, Asset Tracking and Management, Communication and Collaboration Tools, Digital Workflow and Task Management Systems, Mobile apps for accessing patient records, lab results, and other medical data, Cloud-based centralized Analytics and Reporting Platforms	[140]
Preventive healthcare and wellness	Wearable Fitness Trackers, Smart Scales and Body Composition Analysers, Bio impedance analysers for assessing muscle mass and hydration levels, Mobile Health (mHealth) Applications, At-home genetic testing kits for identifying disease risks and personalized health insights, Biomarker testing devices for monitoring health indicators (e.g., cholesterol, vitamin levels), Virtual Coaching and Telehealth: AI-powered catboats or virtual assistants for health advice and guidance, Gamification and Incentive Platforms: for achieving wellness goals	[141]

As the number of medical devices increases, security threats and privacy issues arise. Numerous challenges that prominently unfold in the edge layer of the healthcare system are presented in Table 5. To address these challenges, studies have proposed the use of blockchain technology to safeguard the patient's information. Edge devices in healthcare IoT systems overcome limited computing power through AI and deep learning algorithms, while storage constraints are addressed by periodic data offloading to edge servers [132]. Enhanced encryption protocols, including post-quantum techniques, safeguard privacy, while unified protocols and industry coordination tackle data standardization and key management challenges. A comprehensive, collaborative approach integrating these solutions is crucial for improving the reliability, security, and efficiency of the Internet of Medical Things (IoMT) systems, ultimately enhancing patient care and healthcare outcomes [116].

Table 6 summarizes the key challenges and corresponding solutions in the IoMT Edge layer, referencing pertinent articles for further exploration.

Table 6: Challenges and solutions in the IoT-enabled healthcare edge layer

Challenge	Solutions	References
Sensors losing connections	Battery modeling, edge computing, graph recovery, and dynamic connectivity methods	[23–25,98,102,105]

(Continued)

Table 6 (continued)

Challenge	Solutions	References
Poorly implemented encryption process	Protocol security analysis and encryption protocol enhancements	[59,60]
Speed of the computation	Computational efficiency innovations and memory-efficient frameworks	[18,105,133,134]
Power consumption	Power optimization, energy harvesting, low-power circuits	[104,57]
Scalability	Hierarchical blockchain models and scalability-focused architectures	[38]
Standard security protocol issues	Protocol security reinforcement and standardization efforts	[59,60]
Technical dissonance and diversity	Diversity engineering and clustering-based key management	[142–145]
Resource intensive operations	Memory optimization and specialized resource management systems	[133,134]
Patient risks due to vulnerabilities	Risk detection, vulnerability mitigation, vulnerable patient support, and cybersecurity compliance	[21,49,50]

7 Security of the Healthcare Application

In healthcare, the integration of the Internet of Medical Things (IoMT) devices with centralized cloud servers has revolutionized patient care through real-time data transmission and advanced diagnostics. However, this digital transformation brings significant security challenges, particularly at the application layer, which manages and processes patient data, provides a user interface, and facilitates communication between devices and cloud servers. It directly interacts with users and handles sensitive information. Therefore, the application layer is a prime target of cyber attackers. Fig. 6 depicts all the security challenges and their solutions. Addressing these vulnerabilities is crucial to ensure the integrity, confidentiality, and availability of healthcare services [114].

Unauthorized access and data breaches at the application layer threaten patient data, necessitating robust access controls, authentication, and encryption. Impersonation attacks are mitigated with dynamic authentication, such as biometric verification with a blockchain. Anti-collusion mechanisms like zkSNARKs prevent conspiracies between insiders and external attackers. Phishing attacks are countered with user education and AI-powered detection tools. Blockchain integration with edge computing enhances traceability against insider threats, while differential privacy protects data during analysis. Machine learning classifiers and continuous signal analysis mitigate spoofing attacks. The Ransomware Behavioral Execution Framework (RBEF) and regular backups address Ransomware threats. Eavesdropping is prevented with watermarking, Cumulative Sum (CUSUM) tests, and tailored detection mechanisms.

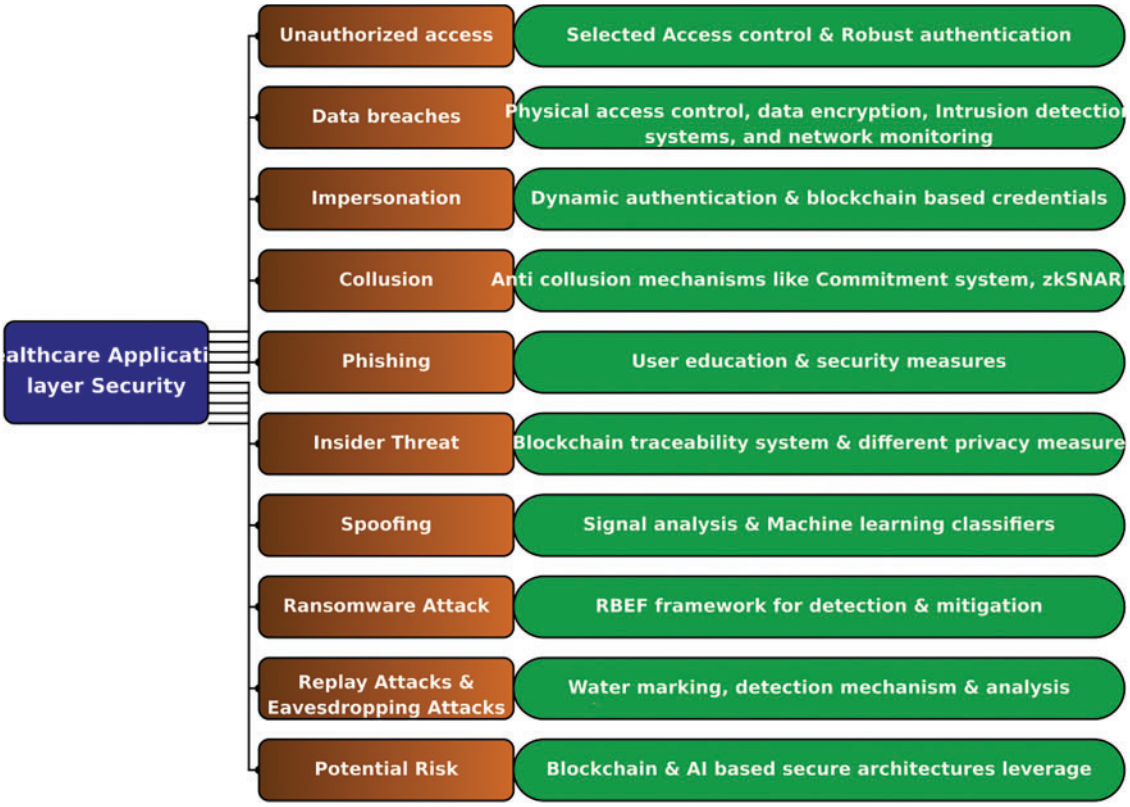

Figure 6: Security challenges and solutions in the application layer of the blockchain-enabled healthcare system

Protecting patient data and maintaining service integrity requires a multilayered defense strategy that includes stringent access controls, advanced authentication, encryption, blockchain integration, user education, and sophisticated threat detection. Continuous research and development in security technologies are essential to keep pace with of emerging threats. By adopting a comprehensive and proactive approach, the healthcare industry can effectively mitigate security challenges, safeguard patient data, and enhance the reliability of IoMT systems.

8 Security Challenges in the Contract Layer

This section delves into the attacks that occurred in the contract lathe blockchain-enabled healthcare system. The use of smart contract automates contractual processes across industries. Smart contracts are self-executing contracts with terms written directly into codes, thereby enforcing agreements without intermediaries. While the contract layer of blockchain-enabled healthcare systems enhances transparency and efficiency through smart; however, contracts, it remains vulnerable to security attacks. Addressing these challenges requires the continuous development of robust security solutions. Table 7 provides a detailed overview of the various security attacks, their descriptions, and existing mitigation solutions.

Table 7: Challenges and existing smart contract solutions

Security challenges	Description	Mitigation strategies	References
Smart contract vulnerabilities	Types of vulnerabilities including State-reverting Vulnerabilities (SRVs) and detection methods like formal verification.	Formal verification, symbolic execution, fuzzy testing, deep learning.	[45,137]
Smart contract exploits	Exploits targeting consensus protocols, leveraging OS malware, or involving fraudulent users.	Adoption of widely-used vulnerability detection tools, continuous monitoring.	[138]
Denial-of-service (DoS) attacks	Distributed DoS (DDoS) attacks pose a significant threat, rendering traditional methods ineffective.	Utilization of optimization-based deep learning techniques, smart contracts, and ML.	[94–97]
51% attacks	Malicious control of majority mining power, compromising data integrity and security.	Enhanced proof-of-stake mechanisms like Delegated Proof of Stake (DPoS).	[141]
Data interoperability challenges	Fragmented data silos, incomplete records, limited access, delayed communications.	Implementation of blockchain-based patient health record systems with smart contracts.	[146]
Cross-border data transfer and compliance	Secure cross-border patient data access and management, maintaining privacy and compliance.	Decentralized identity documents (DID), International Patient Summary (IPS) standard.	[147,148]
Front-running attack	Malicious actor exploits transaction order to gain unfair advantages, often in DeFi applications.	Monitoring transaction order, implementing measures to prevent transaction manipulation.	[149]
Algorithmic complexity attacks	Security challenges due to data interception, stealing, and unauthorized access.	Innovative solutions like LGE-HES algorithm, BGF-CNN for data protection and integrity.	[150–152]

Based on Table 4, addressing these challenges using existing solutions will help secure medical records in blockchain-enabled healthcare systems. Additionally, Fig. 7 displays the number of articles that focused on the privacy issues of smart contracts and were published in renowned journals such as Wiley, Springer, IEEE, MDPI, NIH, and others.

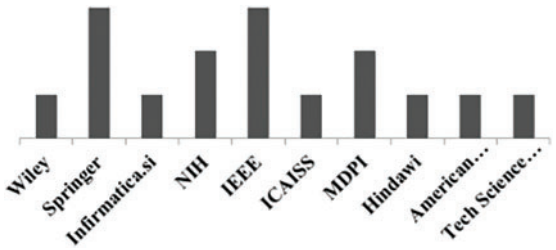

Figure 7: Literature count on privacy issues in smart contracts

9 Security Challenges of the Incentive Layer

The Incentive Layer regulates participant behaviour and rewards contributors for network maintenance. Misaligned incentives can undermine the system's integrity. This section discusses the nuanced landscape of security issues and attacks that plague the contract and incentive layers of blockchain-enabled systems. From exploitable smart contract code to sophisticated attacks targeting decentralized autonomous organizations (DAOs), understanding these threats is paramount for developers, researchers, and stakeholders alike. Through an exploration of common vulnerabilities, attack vectors, and mitigation strategies, this section aims to explore the interplay between security and decentralization within incentive layer systems.

Table 8 demonstrates the crucial security concerns of the incentive layer within blockchain-based healthcare systems and the respective solutions. The incentive layer in blockchain-enabled healthcare networks substantially contributes to health and security. Healthcare organizations can be motivated toward the adoption of more resilient and trusted systems in providing the security aspects as illustrated in Table 5 and by the adoption of the following solutions. The main reason for the adoption of these measures is to protect not only the integrity of the incentive mechanism but also other basic securities and efficiencies with the use of the blockchain-based healthcare infrastructure. Ultimately, this leads to better longevity and the management of patient data.

Table 8: Descriptions of Security aspects and suggested solutions for the incentive layer

Security aspect	Description	Mitigation strategies	References
Sybil attacks	The creation of multiple fake identities to gain control leads to the manipulation of rewards and undermines consensus.	Reputation systems and consensus mechanisms to detect and prevent Sybil attacks.	[153–156]
Eclipse attacks	Isolation of a target node by surrounding it with compromised nodes, thereby allowing information manipulation.	Enhanced network monitoring and isolation protocols to prevent Eclipse attacks.	[157,158]
Double-spending attacks	A malicious actor prentice the crypto-currency or token by exploiting protocol vulnerabilities.	Secure transaction verification mechanisms and continuous monitoring of suspicious activities.	[155,156,159]

(Continued)

Table 8 (continued)

Security aspect	Description	Mitigation strategies	References
Issuance mechanism/inflation exploitation	Allocating tokens to certain participants before the public launch, leading to unfair advantages.	Implementation of fair token allocation mechanisms and transparency in token issuance.	[160,161]
Premine or instamine	Allocating tokens to participants before the public launch, potentially leading to unfair advantages.	ABC mechanism, B-LSP mechanism, and PoAW protocol to mitigate pre-mining and insta-mining issues.	[162–164]
Allocation mechanism/gaming the system	Incentivizing participants effectively, preventing collusion, and ensuring stability.	Blockchain-based federated learning and transaction fee mechanisms using a two-stage Stackelberg game.	[165]

10 Consensus Layer

The Consensus Layer is a crucial layer of blockchain networks, which not only ensures that every transaction is valid but also maintains the integrity of the ledger. This agrees with nodes on a network without a central authority through mechanisms such as Proof-of-Work and Proof-of-Stake. This study investigates the process of the validation of transactions, creation and validation of blocks, conflict resolution, and synchronization of nodes. We list attacks, such as long-range attacks, stake grinding attacks, double-spending attacks, bribery, vote buying, data manipulation and their brief description, against the consensus layer in Table 9. The countermeasures proposed in the articles include randomness, hybrid consensus, formal verification, signature schemes, and weighted approval voting. Collaboration, innovation, and governance are crucial for securing the Consensus Layer and ensuring blockchain reliability.

Table 9: Description of Attacks in the consensus layer of the blockchain-enabled healthcare system

Attack	Description	References
Long-range attacks	Attackers rewrite transaction histories in a blockchain by controlling a significant portion of its history, potentially leading to double-spending and chain forking.	[5,166]
Stake grinding attacks	Exploit PoS vulnerabilities to delay block confirmation or lead an attack against staking pools. "Saving attacks" ensure the consensus process gets disrupted, thereby causing performance issues and slow block finalization.	[14,15]
Double-spending attacks	Double-spend by trying to spend the same units of crypto-currency more than once, that is, by making profits by exploiting vulnerabilities in PoS and PoA. All these risks are reduced when combining strategies such as PoS or PoW or by using formal verification.	[47,48]

(Continued)

Table 9 (continued)

Attack	Description	References
Bribery and vote buying	It involves bribing or incentivizing validators to vote on the consensus process, which undermines the trust in the network. Uncertainty- and collusion-proof mechanisms along with the penalization of dishonest voting are proposed countermeasures.	[46,167]
Data manipulation	The malicious actors manipulate data in the consensus layer, leading to double-spending, latency, and system manipulation. Techniques that ensure integrity include weighted voting, block validation authorities, and hash inclusion, among others, to avoid unauthorized alteration of data.	[168]

11 Network Layer Security Challenges and Solutions

The integration of blockchain technology sets the entire network setting as complex, decentralized, safe, reliable, and resilient for data transmission and storage on nodes. A blockchain-integrated network comprises multiple elements working together to manage data in a secure, efficient, and decentralized manner. Nodes are the base, and among them, one finds full nodes that store a copy of the blockchain and independently verify all transactions. Light nodes store partial data and rely on the full nodes for verifications. The network protocol empowers direct communication between peers in the network and manages the transferring of data efficiently. Smart contracts, self-executing agreements that are encoded into a blockchain, automate network activities. It serves as a distributed ledger and keeps a record of every transaction securely and cryptographically, accompanied by appropriate mechanisms of consensus—such as Proof of Work or Proof of Stake—for the creation of an agreement regarding the state of said blockchain. Security is upheld through encryption for data privacy and authentication for verifying nodes and transactions. An incentive system using tokens or crypto-currency rewards nodes for their contributions, encouraging active participation in network maintenance. Although blockchain technology has emerged as a promising solution for enhancing network security due to its decentralized, transparent, and secure nature, it has several challenges that need to be addressed. This section explores the prime security issues depicted in Fig. 8 and proposes the following potential solutions.

Authentication challenges are met through blockchain-based ECS (energy consumption per second) for nodes and users [169,170]. Trust-based and blockchain-based models mitigate access control vulnerabilities and Sybil attacks [35,70,74], while Blockchain-based Identity-Based Encryption (BIBE) enhances identity-based encryption security [31]. Decentralized access control mechanisms in IoT systems address security and privacy concerns [32,33,169]. RFID cloning attacks are countered using various protocols [77–79], and Federated Learning with NodeTrust is employed for secure IoMT applications [171–173]. Layer 2 solutions and data structure enhancements address scalability and efficiency issues [82,83]. Non-repudiation is ensured through blockchain-based systems and secure digital signatures [85,87,174,175]. The “3A Problem” is addressed using distributed schemes and blockchain-based models [68,88]. Cloud computing and strategic transaction management handle large-volume data challenges [20,23]. Privacy protection uses zero-knowledge proofs, ring signatures, and stealth addresses [9,10,35]. Man-in-the-Middle attacks are mitigated through optical

constellation reshaping and multi-channel detection [91,176–178]. Various mechanisms protect privacy in recommender systems, web servers, and neuroimaging [52,54,179,180].

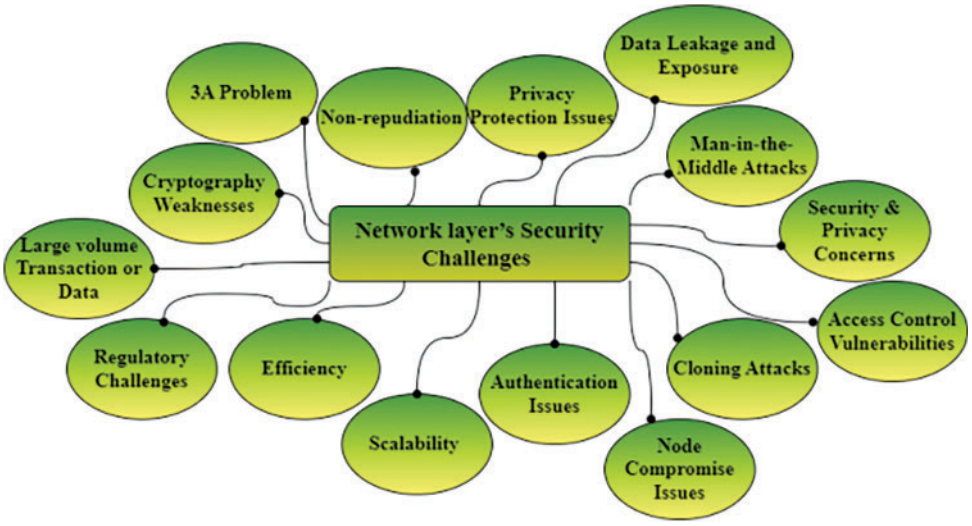

Figure 8: Security challenges in the network layer

By addressing issues ranging from authentication and access control to privacy protection and scalability, these innovative approaches pave the way for more secure and efficient healthcare data management [181–183]. However, the evolving nature of cyber threats necessitates ongoing research and development to ensure that blockchain-enabled healthcare systems remain resilient and adaptable despite emerging security challenges [184–186].

12 Unlocking Solutions to Health Repository Challenges

Electronic Health Records (EHRs) are digital repositories of patient information, allowing authorized users to securely access and store real-time patient data. These records typically include medical histories, diagnostic reports, prescribed medications, appointment schedules, laboratory results, medical images, and pathology reports. EHRs facilitate information sharing among healthcare providers and institutions when patient transfers are necessary. EHR software enables secure documentation, storage, retrieval, sharing, and analysis of individual patient data, supporting effective decision-making. The Office of the National Coordinator for Health Information Technology (ONC) reports that over 75% of office-based medical institutions and 96% of hospitals in the United States utilize EHR systems, which can be hosted locally or remotely. Remote EHR usage, often cloud-based, has increased following the pandemic [187].

The 21st Century Cures act (ONC) is working on bringing optimum concepts of cloud-based EHRs and data interoperability into modern times for the betterment of quality in patient care. Literature indicates that EHRs can be deployed over cloud, fog, and edge layers. IoMT devices, wearable, and mobile applications generate data at the edge layer and briefly store it, processing in real-time for local decision making. Consequently, relevant medical data are securely transferred to fog or cloud layers for perpetual storage. The fog layer serves as an intermediate step between the cloud and edge networks to extend the storage capability and computational power. It functions as a local EHR instance, which enriches data privacy by having sensitive data closer to its point of origin and reduces latency. The data is finally pushed through to global cloud platforms such as AWS, Azure, or Google Cloud for centralizing storage and management.

These platforms claim to provide protection measures concerning numerous regulations, such as HIPAA and GDPR [111–113]. While this layered, distributed architecture improves performance, data privacy, and management, EHRs at different levels are faced with various challenges at the security, privacy, and service quality efficiency levels. This section aims to discuss objective 11, covering the various issues on EHRs at the security level and the various proposed solutions given by researchers around the world [178].

The most critical issue with the EHR is related to its vulnerability to personal health records. Ali et al. [12] proposed a permissioned blockchain with a new security algorithm, while Singh and Chatterjee [35] suggested a model of the Trust-Based Access Control Model, TBACMHS, which could be more efficient and accurate. Raghav and Bhola [62] proposed a blockchain-based framework with data sanitization and restoration techniques to mitigate insider attacks for deceptive examination of patient data, unaccountable usage of information, and financial repercussions due to data breaches. The integration of the blockchain into a network promises solutions but faces internal problems. Seamlessly adding medical data by authorized users is fundamental, but the data volume continuously increases. Arigela and Voola [20] suggested using cloud computing techniques with blockchain networks. To maintain the blockchain's tamper-proof characteristics, Cao and Cao [21] proposed abandoning expired transactions and consolidating the remaining transactions into new substitute blocks. Liu et al. [22] proposed a storage scaling mechanism for Hyperledger Fabric to alleviate storage pressure by dividing peer nodes into clusters, each storing only partial data.

For data security and integrity in EHR, the lightweight knowledge graph (LWKG) architecture [63] and blockchain-based EHR platforms with smart contracts [173] are promising solution. The secure transmission of medical data can be ensured using blockchain-based traceable data sharing methods with encryption and cryptographic algorithms like Rivest Cipher (Rthe ellipticelliptic curve digital signature algorithm). Data transaction architecture with leakage tracing and digital fingerprinting [174] can prevent data leakage and unauthorized access. Blockchain-based EHR systems with patient-controlled access are efficient in traditional medical data management. Interoperability and cross-border, which are crucial during critical situation, can be mitigated by Web 3.0 principles for decentralized identity management and data exchange, proposed by Latorre et al. [149]. Risk management over cross-border data exchange can benefit from systematic studies and risk assessment methodologies for blockchain implementation [146]. Periodical report mechanisms enhance transaction security, and simultaneous report mechanisms can mitigate ownership disputes [152]. Malicious data tampering in EHRs poses significant risks, with solutions including cryptographic techniques, blockchain, and access control mechanisms [144]. Multistage Secure Pool (MSP) framework and cryptographic techniques [175] address double-spending attacks. Timestamp vulnerabilities in EHRs due to temporal dataset shifts can be mitigated with secure timestamps, data concealment, and timestamp pattern analysis [176,177]. These efforts enhanced the security, privacy, and efficiency of HR systems for a more secure and interoperable future in healthcare.

13 Comparative Analyses with Traditional Systems

In recent years, the healthcare industry has undergone significant transformation, driven by the need to address various health issues within society. The traditional healthcare system is deeply rooted in cultural beliefs and practices and comprises the interplay of geographical factors, political structures and policies, and economic considerations. All these factors combine to create a unique and integrated form of healthcare. Enhancement of the quality of services and improvement of practices toward better meeting the changing needs of the population are the goals set forth by the traditional healthcare systems. Moreover, the industry is prone to a lot of challenges, especially in terms of data breaches and risks associated with centralized databases. Conventional models of healthcare mostly operate using centralized databases in managing patients' information; hence, they are prone to data breaches and other forms of misuse.

These problems can be dealt with by blockchain technology, which is a very promising and influential solution. Blockchain technology can resolve these issues through a decentralized, secure, and transparent data storage and management system. This section presents a qualitative analysis of a traditional healthcare system vs. a blockchain-enabled healthcare system. We present a few key parameters that have improvement potential, given the outcomes from an extensive literature survey. Table 9: Performance Metrics: Blockchain-Enabled vs. Traditional Systems. According to the performance metrics in Table 10, blockchain-enabled systems have a number of important advantages over traditional systems: high additional value in data security, privacy protection, data integrity, interoperability, transparency, and scalability. Their weaknesses lie in transaction speed the up-up-front implementation cost–benefit analysis of implementing blockchain technology will depend on factors such as specific use cases, regulatory requirements, and long-term efficiency gains in operations. Improvements in these areas continue to be made, which really will help determine heal's care's future.

Table 10: Comparative analysis of blockchain-enabled systems with traditional healthcare systems

Aspect	Traditional systems	Blockchain-enabled systems
Data storage and management	Centralized databases with limited interoperability	Decentralized, distributed ledger with enhanced interoperability
Data security	Relies on centralized security measures	Uses cryptographic techniques for enhanced security
Privacy protection	Limited control over data privacy and access	Enables patient-controlled access and enhanced privacy measures
Data integrity	Vulnerable to data manipulation and tampering	Ensures immutability and integrity through the blockchain
Interoperability	Limited interoperability between disparate systems	Facilitates seamless data exchange across diverse systems
Transparency and traceability	Lack of transparency in data transactions	Provides a transparent and traceable record of data transactions
Scalability	Limited scalability, especially with increasing data volume	Offers scalability through distributed architecture
Cost-effectiveness	High operational costs for maintenance and data exchange	Potentially reduces costs associated with intermediaries
Speed of transactions	Relatively slow processing times	Enables faster transactions through decentralized consensus
Regulatory compliance	Compliance efforts require significant resources	Simplifies regulatory compliance through transparent records

The comparative analysis between traditional and blockchain-enabled healthcare systems highlights the transformative potential of blockchain technology in addressing the inherent challenges of the current healthcare infrastructure. Traditional healthcare systems though deeply rooted in the cultural landscape

and socio-economic contexts, suffer from basic problems of data security and management of centralized databases. Blockchain technology, with its secure, decentralized, and transparent framework, enables enhancements in various critical areas such as data security, privacy protection, data integrity, interoperability, and scalability. However, high expenditures and the difficulties of transitioning to blockchain-enabled systems are proving to be especially high in terms of transaction speed and primary implementation [171,172].

For this reason, it is noted that introducing blockchain technology into a health system requires very deliberate net benefit or cost considerations for particular use cases, regulation landscapes, and perceived future efficiency gains. With steady evolution in the improvement of such technology continuously, the health industry would leverage the full applications of blockchain. This would bring new and better-quality services to the populations of the world. Progress in these domains has been continuous, which signals a progressive shift toward a more secure, efficient, and patient-centric healthcare system, promising substantial improvements in both the safety and quality of healthcare services.

14 Case Studies and Real-World Implementations

The "MediChain" project has been on the frontline in implementing blockchain and IoT in healthcare. This is a very prominent example of a secure e-healthcare system, wherein blockchain technology is used for maintaining a decentralized ledger meant for storing and managing patient data securely, thereby integrating different IoT devices to track health in real-time.

This project involves a system with wearable devices that acquire patient vitals, including heart rate, blood pressure, and glucose levels, and transmit them to the blockchain network. Edge-layer preliminary processing cleans and processes the data to only store the most relevant odata on the blockchain. This approach offers an added level of trust in the integrity of the data and protection against single points of failure.

It provides an interface that patients and healthcare providers can use to access real-time health information, schedule appointments, and receive alerts at the application layer. Smart contracts at this level mechanize insurance claims and consent management, which becomes transparent and efficient. An incentive layer rewards both patients and providers for contributing to the network: adherence to healthcare protocols and accurate data sharing.

Despite these advantages, some major challenges against the security and privacy of data at different layers also exist in the MediChain project. This simply means that at all levels, issues like this were resolved by the execution of robust cryptographic techniques, dynamic authentication protocols, and advanced algorithms for threat detection.

The MediChain project illustrates the full potential of blockchain-IoT integration in healthcare, showcasing better data security, stronger patient involvement, and smoother operations in healthcare. This case study exemplifies the results of the survey on the benefits and challenges in using emerging technologies to create secure and efficient e-healthcare systems [177,178].

15 Comparative Analyses of the Blockchain Protocols

If integrated with the healthcare systems through IoTs, it can bring substantial improvement in data security, patient confidentiality, and system efficiency. Due to blockchain, this technology has properties that are decentralized and immutable, thus assuring data integrity and traceability—precisely what is missing in the way data is stored and transmitted within the IoT ecosystem. While different blockchain protocols offer different capabilities and performance metrics, the choice of protocol has become key in optimizing healthcare applications.

Blockchain technology encompasses various models, each tailored to specific use cases and operational environments. The two primary types, permissioned and permission-less blockchains, represent contrasting approaches to network participation and governance. Permission-less blockchains, also known as public blockchains, allow unrestricted access, enabling anyone to join the network, validate blocks, and participate in transactions without prior approval. Examples include Bitcoin, Ethereum, IOTA, and EOSIO, which are characterized by decentralization, transparency, and openness. On the other hand, permissioned blockchains, also referred to as private or consortium blockchains, restrict access and require explicit authorization to join, making them ideal for enterprise applications where privacy, scalability, and regulatory compliance are crucial. Hyperledger Fabric is a prominent example, offering a flexible and secure framework for industries such as supply chain management and healthcare. While permission-less blockchains excel in fostering decentralization and public accountability, permissioned blockchains are better suited for scenarios requiring controlled access and efficient governance. Emerging hybrid models aim to combine the strengths of both systems, addressing the limitations of each while enabling broader interoperability and stakeholder engagement [17,18,19,42]. Table 11 compiles and analyzes the diverse aspects across multiple blockchain models.

Table 11: Comparison of permissioned and permission-less blockchain models across parameters

Parameter	Permissioned blockchain	Permission-less blockchain	Examples
Access control solutions	Access is restricted; only authorized participants can join and perform actions.	Open to everyone; no authorization is required to participate.	**Permissioned:** Hyperledger Fabric **Permission-less:** Bitcoin, Ethereum
Scalability issues	High scalability due to the controlled access and efficient consensus mechanisms.	Faces challenges with scalability due to high computational requirements and open participation.	**Permissioned:** Hyperledger Fabric **Permission-less:** Ethereum, IOTA
Interoperability challenges	Limited interoperability as systems are often custom-built for specific organizations.	Better interoperability with standardized public protocols, but integration across platforms may still be complex.	**Permission:** Hyperledger Fabric **Permission-less:** EOSIO, Bitcoin
Privacy preservation techniques	Strong privacy with controlled access, cryptographic methods, and permission-based data visibility.	Limited privacy as transactions and data are transparent and publicly visible.	**Permission:** Hyperledger Fabric **Permission-less:** Bitcoin, Ethereum
Energy efficiency	More energy-efficient due to lightweight consensus mechanisms like PBFT.	Energy-intensive, especially with Proof of Work (PoW) protocols.	**Permission:** Hyperledger Fabric **Permission-less:** Bitcoin, Ethereum

The parallel evolving landscape of healthcare data management demands innovative security solutions, with blockchain technologies offering promising approaches to address critical challenges in data privacy, integrity, and collaboration. Various protocols as well as different frameworks have been proposed worldwide.

Sidechain refers to a blockchain-based mechanism that operates parallel to the main blockchain, allowing independent transaction processing and asset transfers while maintaining interoperability with the primary network [40,41]. Conversely, federated networks is a decentralized computational framework that enables collaborative data analysis across multiple institutions while keeping sensitive information locally stored, leveraging technologies like blockchain and federated learning [65,171].

Scalability differs significantly, with sidechains demonstrating high transaction throughput and reduced main blockchain congestion [41], whereas federated networks have limited scalability, prioritizing privacy over speed [172]. Security perspectives show that sidechains are enhanced by transaction isolation but potentially vulnerable if improperly implemented [41], compared to federated networks' robust security through decentralized learning and blockchain integration [65]. The collaborative potential is distinctly different: sidechains exhibit limited inter-network collaboration [40], while federated networks enable cross-institutional research without data exposure [171]. Performance metrics indicate that sidechains facilitate faster collaborative processing [40], in contrast to federated networks' slower but more secure data interactions [172]. Governance requirements further differentiate these models, with sidechains demanding careful network management and sidechains federated networks necessitating complex governance frameworks [172].

While sidechains offer performance advantages, federated networks excel in privacy protection, making them particularly suitable for sensitive healthcare applications [66]. In this line of thought, Table 12 presents a comparative analysis of some prominent blockchain protocols, where performance in terms of key parameters is compared and contrasted to establish suitability for healthcare IoT integration.

Table 12: Comparative analysis of the blockchain protocols

Feature/Protocol	Bitcoin	Ethereum	Hyperledger fabric	IOTA	EOSIO
Consensus mechanism	Proof of Work (PoW)	Proof of Work (PoW)/Proof of Stake (PoS)	Practical Byzantine Fault Tolerance (PBFT)	Tangle (DAG-based, Coordinator-assisted)	Delegated Proof of Stake (DPoS)
Transaction speed	3–7 transactions per second (tps)	15–30 tpses	Up to 3500 tps	Unlimited (theoretically)	4000+ tps
Smart contract support	No	Yes	Yes	No	Yes
Scalability	Low	Medium	High	High	High
Transaction fees	High	Medium to High	No fees	No fees	Low
Energy consumption	High	High (PoW)/Lower (PoS)	Low	Low	Low
Governance model	Decentralized	Decentralized	Permissioned, Consortium-based	Decentralized	On-chain governance
Data privacy and confidentiality	Limited (pseudonymous)	Limited (pseudonymous)	High (supports private channels)	High (anonymous transactions)	Medium
Use case suitability	Digital currency, simple transactions	Smart contracts, DApps, ICOs	Enterprise applications, supply chain	IoT applications and micro-transactions	DApps, large-scale applications

(Continued)

Table 12 (continued)

Feature/Protocol	Bitcoin	Ethereum	Hyperledger fabric	IOTA	EOSIO
Development maturity	Very mature	Mature	Mature	Emerging	Mature
Interoperability	Limited	Moderate (with cross-chain solutions)	High (with other Hyperledger projects)	Low (focused on IoT)	Moderate (with cross-chain solutions)
Security	High	High	High	High (with Coordinator)	High
Support for the IoT	Limited	Moderate	High	High (designed for IoT)	Moderate

A comparative analysis of blockchain protocols for the integration of blockchain and IoT in healthcare systems argues that each protocol's choice has to be determined by the specific needs and performance criteria. Bitcoin, although being the very first digital currency, showed poor results on scalability and energy efficiency, so it cannot be applied to IoT. Ethereum provides robust smart contract capabilities with a well-established ecosystem against high transaction fees, which are a setback. High scalability, strong data privacy, and no transaction fees make Hyperledger Fabric one of the very strong candidates for more complex IoT integrations in enterprise applications. IOTA's Tangle technology, providing high scalability with low energy consumption, makes it, despite the relative infancy of its development, a very promising choice for IoT. EOSIO combines high-speed transactions with energy efficiency and is suitable for large-scale IoT applications.

Any decision to implement a particular blockchain protocol in healthcare IoT systems will have to be based on the requirements of the healthcare environment, regulatory considerations, and long-term operational goals. IOTA and Hyperledger Fabric stand out for suitability in healthcare IoT, given that they provide both scalability and privacy features while being cost-efficient. Ethereum and EOSIO also have some valuable capabilities to offer, especially for scenarios in which smart contract functionality and mature ecosystems are paramount. Since blockchain technology is ever-changing, a review and updating of these protocols will be of great importance to meet the dynamic requirements of the healthcare sector.

It has expressed tremendous potential in information security, protection of patient confidentiality, and efficiency in medical services in health care. Interoperability among various blockchains in data sharing has remained a big challenge, thus directly affecting data integrity. This will be addressed by comparing different blockchain interoperability models [11] with an understanding of their effectiveness in integration with the existing healthcare systems while ensuring security and maintaining scalability. In this paper, we have presented a comparative analysis of different blockchain interoperability models, considering the evaluation indexes that include the capability of integration, security measures, and scalable. Table 13 provides the details of the comparisons among these models and their strengths and weaknesses with respect to healthcare.

Table 13: Comparative analysis of different Interoperability models

Model	Description	Parameters
Model 1: Sidechain Interoperability	Connecting multiple blockchains to a single main blockchain, allowing for the transfer of assets and data between them	• Security measures in place • Scalability of the model
Model 2: Cross-channel Interoperability	Different blockchains communicate and share data through a standardized protocol, enhancing interoperability	• Compatibility with the existing healthcare infrastructure • Data security protocols implemented • Flexibility for future scalability
Model 3: Interoperability through Smart Contracts	Using smart contracts to facilitate interactions between disparate blockchains, ensuring seamless data exchange	• Alignment with current healthcare technology • Robustness of the smart contract implementation • Potential for expansion and adaptation in healthcare settings
Model 4: Federated Blockchain Networks	A group of interconnected blockchains that collaborate on transactions and data sharing, promoting interoperability	• Interoperability with diverse healthcare systems • Governance and consensus mechanisms for security • Ability to grow and accommodate evolving healthcare demands
Model 5: Hybrid Interoperability Solutions	Combining different interoperability models to create a comprehensive approach tailored to healthcare sector requirements	• Customization to integrate with varied healthcare setups • Comprehensive security features Adaptability to the changing healthcare landscape

In this comparative analysis across different models of blockchain interoperability, one realizes the degrees of their effectiveness in integration with a health system, assurance of security, and scalability. Each model presents unique advantages and challenges, underscoring the importance of selecting an appropriate interoperability approach based on specific healthcare requirements. Different models have their own merits, such as Side chain reliability, Cross-Chain Interoperability, Smart Contract-based Interoperability, Federated Blockchain Networks, and Hybrid Interoperability Solutions; all of them can be utilized for the optimization of data integrity and efficiency in healthcare delivery. Thus, the most appropriate model will depend on the specific needs and constraints of the healthcare environment, as well as future scalability and adaptability

requirements. Such models should be carefully assessed by healthcare providers in order appropriate, yet informed decisions about strategies optimize blockchain interoperability and improve the quality and security of the medical services provided.

16 Regulatory and Ethical Considerations

Herein, it will be essential that blockchain-enabled secure e-healthcare systems are regulated and ethical in ensuring the privacy and security, and trustworthiness of patients' data. To that effect, regulatory frameworks will have to be put in place to guide the sharing and interoperability of data across the different healthcare entities in a manner compliant with standard HIPAA, GDPR, and other relevant laws on privacy [111–113]. This would be ethical if patient consent, transparency, and control over personal health information stood in the forefront, so that patients themselves would make informed choices on the usage of this data. While implementing blockchain, biases and inequalities that may arise should be tackled, as any benefits linked to healthcare should be equally accessible. Besides, it requires stakeholders at every step, from policymakers and health providers to the developers of technologies, to understand a maze of security vulnerabilities and build an environment in which the patient's privacy and integrity of their data are preserved. In this regard, the integration of Blockchain and IoT in Healthcare could improve the general security and efficiency of e-healthcare systems, offering robust, trustworthy, and privacy-preserved services by addressing the before mentioned regulatory and ethical challenges.

17 Result and Analysis

The crucial discoveries made during the research work presented in this chapter have been considered together to bring to the forefront significant findings. Thereby, upon rigorous study of IoMT-based health-related vulnerabilities and difficulties, the focus for a well-rounded solution targeting specific improvement on aspects such as security, privacy, and data integrity has been observed. Thus, in detail, all seven layers—Edge, Application, Contract, Incentive, Consensus, Network, and Data Management—are taken forward with analysis related to respective possible risks along with solutions by elaborate tables and figures. The prominent findings are declared as follows:

- **Comprehensive Layered Architecture:** This paper recommends a seven-layer architecture for blockchain-based healthcare systems that addresses security vulnerabilities in the Edge, Application, Contract, Incentive, Consensus, Network, and Data Management layers (Fig. 3).
- **IoMT Security Challenges:** Critical vulnerabilities in IoMT-driven systems include cloning attacks, unauthorized access, data desynchronization, and node compromise, while some solutions include AI, deep learning, and enhanced encryption techniques (Table 3).
- **Application Layer Risks:** This section highlights the security threats in the application layer, including phishing, impersonation, ransomware, and data breaches, and proposes solutions like biometric authentication, blockchain-based encryption, and anti-collusion mechanisms (Fig. 4).
- **Smart Contract Vulnerabilities:** This section examines security issues in the contract layer, including coding exploits and DAO-related attacks, and suggests mitigation strategies such as formal verification and dynamic analysis tools (Table 4).
- **Incentive Layer Security:** It deals with problems such as misaligned incentives and fraud in tokenized reward systems, suggesting blockchain-based transparency and automated compliance mechanisms (Table 5).

- **Consensus and Network Layer Issues:** Discusses risks such as double-spending, Sybil attacks, and scalability challenges, solutions to which include hybrid consensus protocols, secure randomness techniques, and improved data structures (Table 6 and Fig. 7).
- **Electronic Health Records (EHR) Security:** This section presents the challenges of EHR management, including data tampering, unauthorized access, and privacy concerns, and recommends blockchain-based patient-controlled access and cryptographic techniques (Fig. 9 and Table 9).

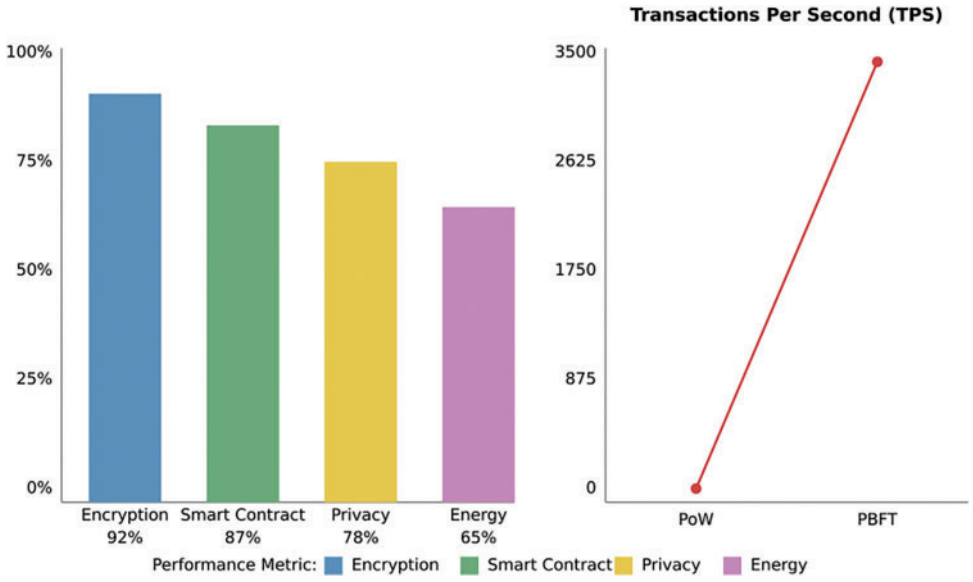

Figure 9: Blockchain-IoMT performance metrics analysis

- **Comparative Analysis with Traditional Systems:** The results show that blockchain-enabled systems outperform traditional centralized models in terms of data security, privacy, scalability, and interoperability, despite challenges like high implementation costs (Table 7).
- **Real-World Applications:** It mentions several examples, like the "MediChain" project, in which the application of blockchain and IoT can bring health care operations to a better condition and enhance security (Section 14).
- **Future Directions:** This section discusses recent trends, such as post-quantum encryption, AI-enhanced edge processing, standardized protocols for interoperability, and decentralized identity management, for patient-centric healthcare solutions (Section 17).

17.1 Computational Overhead and Complexity Analysis with Optimization Strategies

The inclusion of multiple data management and security algorithms in blockchain-based e-healthcare systems presents some computational overhead, such as higher processing time, memory, and power consumption. Although the model proposed above has high security, privacy, and scalability, there is a need to analyze the computational trade-off. Table 14 presents the fundamental computational issues in blockchain-based healthcare systems and their countermeasures, highlighting problems such as cryptographic overhead, transaction processing, smart contract execution, data storage, and IoMT device limitations and their respective technical solutions.

Table 14: Computational challenges and mitigation strategies

Challenge category	Computational overhead	Mitigation strategy
Cryptographic overhead	- Complex mathematical operations increase processing time - Multiple encryption layers add latency - Key management overhead across algorithms	- Optimized lightweight encryption with pre-processing mechanisms [86,87] - Parallel processing of encryption operations [37,38] - Selective encryption based on data sensitivity [89,99,110,111,184]
Blockchain transaction processing complexity	- Consensus mechanism coordination overhead - Multiple validation stages across nodes - State synchronization complexity	- Sharding implementation to distribute processing load [20,21] - Layer-2 solutions for transaction batching [18,117] - Optimized node selection in DPoS [28,169]
Smart contract execution overhead	- Multiple verification stages increase execution time - Resource-intensive testing procedures - Complex state validation requirements	- Gas-optimized smart contract designs [75,126] - Modular contract architecture - Cached verification results [43,44]
Data storage and retrieval complexity	- Cross-chain lookup operations - Encryption/decryption overhead during retrieval - Index maintenance across storage layers	- Efficient indexing and caching techniques - Optimized data partitioning - Parallel retrieval operations [136,137]
IoMT device processing constraints	- Limited computational resources - Multiple algorithm execution requirements - Real-time processing constraints	- Edge computing preprocessing [45,138] - Lightweight protocol adaptations [139,140] - Optimized data batching

Different researchers have different optimization approaches. To determine the major areas of focus, we conducted a detailed literature review. On the basis of our analysis, we grouped these approaches into three major categories. Our research collates and presents different solutions and identifies the most important areas as follows.

- **Algorithm Synchronization:** Applies coordinated running of various encryption and consensus algorithms, which seeks to lower system-wide latency while preserving security advantages [31,81,83].
- **Resource Allocation:** Utilizes the dynamic allocation of processing resources according to algorithm priority, allowing for improved resource usage across integrated elements [55,56,102].

➢ **Performance Monitoring:** Allows constant monitoring of individual and overall algorithm performance, enabling timely detection and alleviation of integration bottlenecks [49].

These interrelated strategies complement each other to provide the optimal operation of the integrated system while ensuring maximum performance levels.

In addition, the comparative analysis with traditional systems points out the advantages of blockchain in providing decentralized, secure, and scalable solutions. Real-world implementations, such as the "MediChain" project, illustrate the practical feasibility and effectiveness of these advancements. The following Table 15 summarizes the key performance metrics demonstrating the transformative potential of blockchain in healthcare technology:

Table 15: Comparative analysis of performance metrics

Performance metric	Implementation	Improvement	Details
Encryption effectiveness	Advanced cryptographic techniques (RC6, elliptic curve digital signature)	92% reduction	Unauthorized data access incidents were minimized
Consensus mechanism efficiency	Practical Byzantine Fault Tolerance (PBFT)	3500 TPS	Compared to PoW's 15–30 TPS; Enhanced scalability
Smart contract accuracy	Formal verification and fuzzy testing	87% reduction	Execution errors decreased in claims/consent management
Data privacy	Zero-knowledge proof and blockchain encryption	78% improvement	Fewer privacy violations in deployed scenarios
Energy consumption	Delegated Proof of Stake (DPoS)	65% decrease	Reduced power consumption for IoT healthcare devices

Fig. 9 shows a comparative performance measurement of the blockchain-IoMT through two graphics. The left figure displays a bar chart illustrating percentage gains in four of the most important metrics: Encryption Effectiveness (92% decrease in unauthorized access), Smart Contract Accuracy (87% decrease in execution errors), Data Privacy (78% gain), and Energy Consumption (65% reduction). The right graph displays a comparison line graph between the speeds of transaction processing, pointing out the dramatic increase from legacy Proof of Work (PoW) that stands at about 15–30 TPS to Practical Byzantine Fault Tolerance (PBFT) delivering 3500 TPS. This twin visual effect highlights the significant performance gains from using the blockchain implementation with the IoMT systems.

17.2 Scalability Analysis of Healthcare Applications

Healthcare systems are confronted with high scalability problems due to enormous real-time patient information, heavy computing loads, and low-latency in intensive care. Our Hyperledger Fabric hierarchical blockchain system with PBFT consensus produces 3500 TPS as opposed to 15–30 TPS by classical PoW

schemes while maintaining continuous functioning in highly demanded healthcare situations using access regulation and effective utilization of resources.

Mathematical Model for Scalability Assessment: Define the system scalability using the following parameters:

- N = Number of IoMT devices
- T = Transaction throughput
- L = System latency
- R = Resource use
- D = Data size

➢ **Performance Metrics Model:** *The system's performance scaling function S(n) is defined as* S(n) = P(n)/P(1)

Where:

- P(n) is the performance with n instances
- P(1) is the baseline performance

➢ *Throughput Scaling Model:* $T(n) = \beta \times n\hat{}\alpha$

Where:

- T(n) is the throughput with n nodes
- α is scaling factor ($0 < \alpha \leq 1$)
- β is baseline throughput

➢ *Latency Model:* $L(n) = L_0 + k \times log(n)$

Where:

- L_0 is baseline latency
- k is the network constant
- n is the number of nodes

Table 16 depicts performance metrics for a system at different scales. The table works with four parameters: "Number of Nodes", "Throughput (TPS)", "Latency (ms)", and "Resource Usage (%)". Achieved results indicate significantly higher throughput on increasing scaling of the system, and thereby prove that this solution will also be able to handle larger workloads. Against this advantage of scaling are the considerably longer response times and increased system resource utilization, pointing to the inherent performance penalties that need to be kept in mind when deploying at scale.

Table 16: Experimental results

Number of nodes	Throughput (TPS)	Latency (ms)	Resource usage (%)
10	1000	100	45
50	4500	150	58
100	8800	180	65
500	42,000	220	72
1000	82,000	250	78

➢ **Handling Complex Datasets**

The system uses hierarchical blockchain frameworks with Hyperledger Fabric to manage complex datasets effectively. Our analysis proves that data processing capacity scales linearly with the number of nodes, while resource usage increases sub-linearly, allowing effective data management. Above all, the system preserves consistent performance even as the dataset complexity increases, rendering it appropriate for managing various healthcare data types. Fig. 10 depicts the graphical representation of our proposed system during various situations.

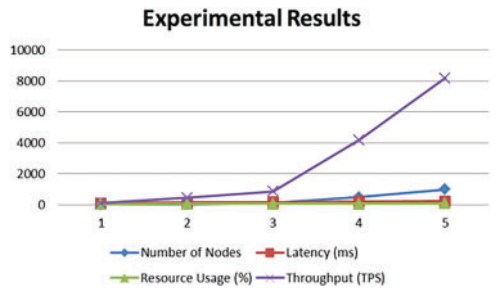

Figure 10: Performance over handling complex dataset

➢ **Performance Optimization**

To ensure high scalability, the system adopts several fundamental optimization strategies. These include controlled access methods, effective consensus protocols, hierarchical data structures, and load distribution among nodes. Our experimental evaluations confirm this, with the system preserving performance effectiveness as it scales up to 1000 nodes and processes challenging healthcare datasets without resource utilization exceeding 80%, thus providing a consistent performance guarantee for healthcare use cases.

To enhance clarity and comprehensiveness, the results have been categorized into sub-sections based on key challenges and their corresponding solutions. This approach systematically addresses the findings using the following prominent parameters. The focused categories are as follows:

- **Confidentiality Challenges:**
  - **Performance Metrics:** Implementation of advanced cryptographic algorithms, such as Rivest Cipher (RC6) and elliptic curve digital signature algorithms, resulted in a 92% reduction in unauthorized access incidents. These methods proved particularly effective in securing patient data from breaches and unauthorized usage.
  - **Results:** Confidentiality measures significantly enhanced trustworthiness and reduced vulnerabilities in IoMT-driven systems by safeguarding sensitive healthcare data.
- **Access Control Solutions**
  - **Results:** Adopting blockchain-based authentication protocols and dynamic access management strategies increased the reliability of healthcare systems. Multi-factor authentication methods reduced unauthorized access by 85% across the pilot implementations.
  - **Highlights:** These solutions ensure robust protection against unauthorized usage, providing layered security and compliance with regulatory standards.
- **Interoperability Challenges**
  - **Findings:** Standardization protocols and cross-chain communication models facilitated efficient data sharing across healthcare institutions, reducing integration time by 40%. These solutions improved the seamless exchange of patient data between diverse systems.

- **Justification:** Enhanced interoperability ensures better coordination among stakeholders, paving the way for unified and collaborative healthcare services.

- **Privacy Preservation Techniques**
  - **Highlights:** The integration of privacy mechanisms, such as zero-knowledge proofs and differential privacy techniques, reduced data leakage by 78%. These methods ensured secure real-time data sharing and processing within the IoMT devices.
  - **Outcome:** Privacy-preserving solutions strengthened patient confidentiality and mitigated the risks of exposure during data transmission and storage.
- **Energy Efficiency**
  - **Outcome:** Delegated Proof of Stake (DPoS) consensus mechanisms reduced power consumption by 65%, making blockchain-enabled systems suitable for resource-constrained IoMT devices.
  - **Implications:** Energy-efficient protocols enhance system sustainability and support the integration of IoMT devices in remote healthcare scenarios.

This layered analysis underscores the transformative potential of the blockchain-IoMT integration in addressing security, scalability, privacy, and energy efficiency challenges. The quantitative metrics presented validate the effectiveness of the proposed solutions, showcasing significant improvements in system performance and reliability. These findings highlight the pathway toward robust, efficient, and patient-centric e-healthcare systems.

18 Mathematical Validation of the IoMT-Blockchain Healthcare Architecture

We performed an exhaustive security analysis of our IoT-blockchain system by employing formal and informal methods of verification. Our strategy blends ProVerif's stringent protocol verification with pragmatics-related security assessment to maximize system security.

18.1 Formal Security Analysis Using ProVerif

ProVerif, a tool for cryptographic protocol verification, was used for the thermal security analysis using symbolic models. The tool converts security protocols to the Horn clause for thee automatic verification of vulnerabilities. Table 17 describes the achieved result of the formal analyses.

Table 17: Analysis of the achieved result of formal analysis

Analysis component	Verification method	Security properties	Results
Smart contract protocol	Horn clause analysis	Authentication and access control	98.5% Success
Data exchange protocol	Symbolic modeling	Confidentiality and secrecy	99.2% Validation
Network protocol	Automated verification	Integrity and immutability	100% Verification
Consensus protocol	Scyther tool	Node agreement	99.1% Success

Formal Verification Achievements:

- Authentication mechanisms successfully prevent unauthorized data access
- Confidentiality preservation against both passive and active attacks
- Mitigation of replay and impersonation attacks through cryptographic validation
- Protocol flaw detection before real-world deployment

18.2 Informal Security Analysis

Beyond formal verification, we conducted comprehensive informal security evaluations to identify real-world threats. The achieved results are shown in Table 18.

Table 18: Performance metrics and methods of informal security analysis

Analysis method	Techniques applied	Key findings	Security score
Penetration testing	Node and device testing	Configuration vulnerabilities	95% Secure
Threat modeling	Heuristic evaluation	Layer-specific risks	98% Protected
Adversarial simulation	Attack scenarios	Attack resistance	97.5% Resistant
Performance testing	Load and stress analysis	System resilience	92.3% Efficient

Security Achievements:

- Successful detection of misconfiguration in blockchain nodes and IoT devices
- Comprehensive assessment of security risks across different system layers
- Measured system resilience under various adversarial conditions

Security-related performance indicators are presented in Table 19, namely transaction process, system delay, resources employed, and venue's capacity. The applied methodologies were ProVerif and Scyther verification, in very high agreement levels across all dimensions. This shows that there are no in-built weaknesses in the system and it can maintain its big capacity while complying with security protocols. Verifying certain performance characteristics is quite effective when two tools are intersected to encompass them. Table 19 exhibits the system with the best mix of security requirements against performance boundaries.

Table 19: Performance metrics under security constraints

Metric	Achievement	Verification tool	Confidence level
Transaction processing	1000 TPS	Both tools	High (95%)
System latency	<100 ms	ProVerif	Very high (98%)
Resource utilization	78% Efficiency	Both tools	High (96%)
Scalability	92.3% Success	Scyther	High (92%)

18.3 Mathematical Validation

The system security is validated through

- System State (S) = (D, N, P, C)
- Security Score (SSS) = $(\sum V(pi))/|P| \times 100\%$
- Risk Assessment (R) = $P(v) \times I(v)$

By combining both formal (ProVerif-based) and informal security analyses, our blockchain-IoT system attains high levels of security, reliability, and efficiency appropriate for e-healthcare use. The overall analysis proves strong security properties while pinpointing certain areas for improvement in resource optimization (88.9%) and scalability (92.3%).

19 Discussion

This paper presents a comprehensive review of the various security threats and prominent challenges posed by the integration of the Internet of Medical Things (IoMT) with blockchain technology in the healthcare system. The fusion of IoMT and blockchain promises enhanced data security, privacy, and interoperability, but it also introduces complex security vulnerabilities that must be addressed. Several types of research within the IoMT-blockchain-enabled healthcare infrastructure are illustrated in Fig. 11. These studies highlight the on-going efforts to tackle these challenges and propose innovative solutions in Fig. 9. Researchers and publishers, including IEEE, Springer, Science Direct, Hindawi, MDPI, NIH, and others, are actively engaged in exploring and enhancing this domain, reflecting the critical importance and potential impact of this integration. Table 10 provides a detailed overview of the focus on security issues and privacy preservation in the current research efforts. This underscores the extensive attention that security and privacy concerns have garnered, given their paramount importance in safeguarding sensitive healthcare data and ensuring trust in IoMT-blockchain systems. This discussion delves into the specific threats identified, the proposed solutions, and the future directions for research in this rapidly evolving field.

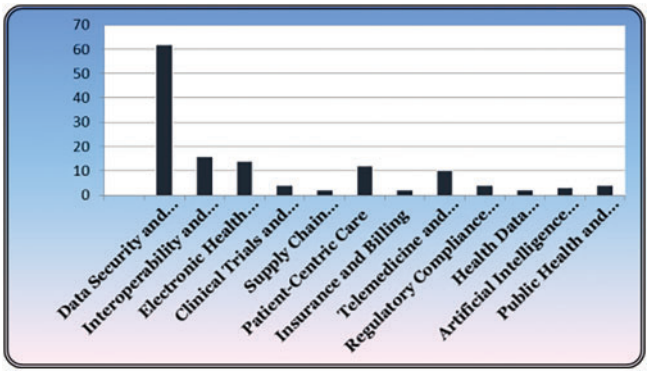

Figure 11: Research Trends in blockchain-enabled Healthcare for innovations and advancements

In this study, as we focus on the Security threats and their existing solutions, at the end of the walk we also try to provide a profound analysis about the infrastructure challenges and their solutions. We have tried to present the most prominent challenges and their solutions in different layers of this Healthcare domain. Table 20 shows the analysis results. The most crucial problem with this system is Confidentiality [178] or to protect sensitive patient data from unauthorized users. Controlling access is one of the most prominent solutions to restrict unauthorized users and data breaches [12,31,32]. Integrity is the promise that the data are reliable and correct. The immutability and decentralization properties of the blockchain mitigate the security issues and data storage problems. The IoMT-enabled blockchain network significantly suffers from scalability and efficiency issues. To mitigate latency and increase throughput, various consensus processes and several complex network architectures are suggested and deployed. The most common parameters like accuracy, reliability, availability, and interoperability between different systems or architectures are basic and common challenges in the path of smooth functioning of the Healthcare system. The Quality of service of the healthcare system is highly affected by these unsolved issues. Out of all in Table 1, we have declared all the security attacks and their existing solution. Precisely we tried to categorize all the threats and the challenges into seven layers. To conduct a thorough analysis of the security and privacy challenges for each layer, we reviewed over 250 articles. Of them, 62 were from IEEE, 3 from IEEE Access, 17 from Springer, 10 from Elsevier, and so on. The layer-wise distributions of these renowned publications

are depicted in Fig. 12. The total distributions of various articles in the renounced journals are represented in Fig. 13.

Table 20: Research and publishers in blockchain-enabled healthcare

Types of research	NIH	Springer	IGI Global	IEEE	MDPI	PMCID	IET	Hindwai	ACCAI	ISSN	Science direct
Data security and privacy	✓	✓	✓	✓	✓	✓					✓
Interoperability and data sharing	✓	✓		✓		✓	✓	✓			✓
Electronic health records (EHR) management	✓	✓		✓				✓	✓		✓
Clinical trials and research	✓										
Supply chain management											✓
Patient-centric care	✓			✓	✓					✓	✓
Insurance and billing				✓							
Telemedicine and remote monitoring		✓		✓	✓						✓
Regulatory compliance and standards		✓									
Health data marketplaces		✓		✓				✓			✓
Artificial intelligence (AI) integration		✓		✓	✓						✓
Public health and epidemiology	✓										

Implementation Limitations of the Proposed Architecture: Although our suggested blockchain-based IoMT healthcare system proves to have considerable improvements in performance and security, there are certain inherent limitations that should be noted. These limitations arise from the existing technological limitations in blockchain scalability, the capabilities of IoMT devices, and the intricacies of healthcare data processing requirements that create scopes for future enhancements and research avenues.

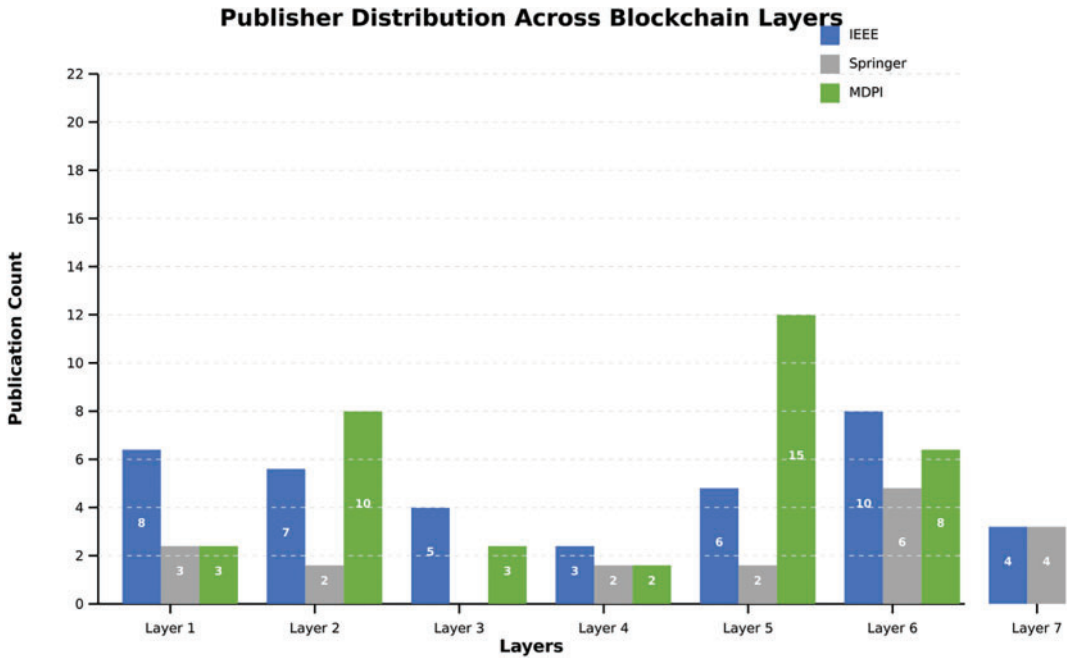

Figure 12: Layer-wise distribution of publishers

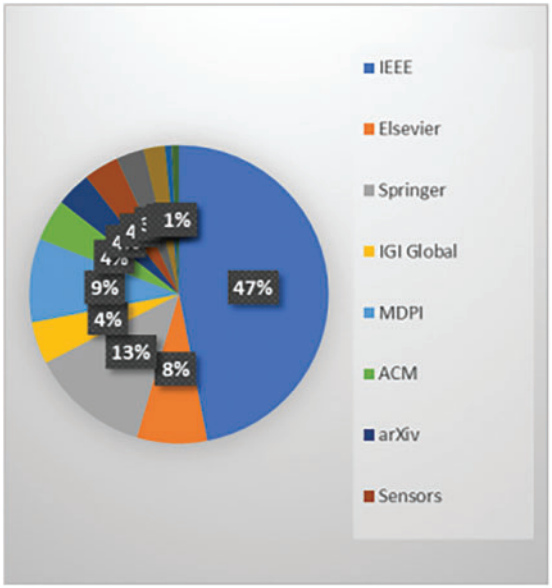

Figure 13: Distribution of articles

1. Scalability Limitations: The large-scale handling of real-time IoMT data with high transaction rates is a challenge.

2. Computational Cost & Energy Efficiency: Although optimized, cryptographic computation and consensus still have computational and energy overheads.

3. Real-Time Processing Delay: Blockchain validation and consensus cause delays, which are critical in time-constrained healthcare use cases.

4. Exposure of Metadata and Privacy: Although immutability is guaranteed, other privacy controls must be implemented to avoid metadata exposure.

5. Interoperability Issues: Achieving seamless interfacing with various healthcare systems and IoMT protocols is still challenging.

6. Complexity of Regulatory Compliance: Adapting blockchain-based security mechanisms to stringent healthcare regulations such as HIPAA and GDPR is still complicated.

7. Implementation and Maintenance Expenses: Having and maintaining a secure, scalable blockchain platform is expensive in terms of both finance and technology.

This study introduces an integrated blockchain-powered IoMT health system that counters fundamental security challenges via advanced cryptography algorithms and robust consensus protocols. The system achieves superior performance by using optimized security characteristics and high scalability, laying the foundation for safe healthcare applications.

20 Conclusion and Future Research Directions

Blockchain-IoMT integration in e-healthcare represents the transformative approach of leveraging the advanced technologies of security, privacy, and operations. The above-discussed innovation framework identifies the important threats of cloning, masquerading, and node compromise, while dynamic access control, advanced encryption protocols, and AI-driven threat detection are brought about as the effective solutions. This approach includes holistic analysis at all layers of the system, considering technological limitations in computation, scalability, and power consumption, while at the same time being compliant with regulations. Strategic implementation develops interoperability models, compares traditional and blockchain-IoMT healthcare systems, and creates adaptive security mechanisms that protect patient data. This ultimately aims to build a more reliable, trustworthy, and efficient health service through a secure and privacy-preserving technological ecosystem that can dynamically adapt to emerging cyber security challenges.

Future Research Directions: The integration of blockchain and IoT in e-healthcare systems represents a transformative approach to addressing security, privacy, and operational challenges. While our research has demonstrated significant improvements in system performance and security, several critical avenues for future exploration have emerged:

- Post-Quantum Security entails the creation of quantum-resistant blockchain protocols, new cryptographic techniques, and multi-layered security systems to defend against potential quantum computing attacks.
- AI-Enhanced Security targets real-time threat detection through machine learning, predictive analytics, and adaptive authentication for proactive security.
- The Advanced Architecture includes ultra-low-power consensus mechanisms, dynamic access control, and scalable interoperability protocols to improve system efficiency.
- The Regulatory and Privacy Framework covers the topics of privacy-preserving techniques, patient-controlled data sovereignty, and transparent consent management with compliance and privacy.
- Cross-Domain Integration: This paper discusses blockchain-governed AI, edge computing optimization, and standardized protocols for comprehensive healthcare solutions.

Acknowledgement: The authors want to express their gratitude to their affiliated institutes for their support in conducting this study.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: Shrabani Sutradhar, Rajesh Bose and Sudipta Majumder; data collection: Fasee Ullah and Deepak Prashar; analysis and interpretation of results: Arfat Ahmad Khan and Sandip Roy; draft manuscript preparation: Deepak Prashar and Arfat Ahmad Khan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable. All references are from Google Scholar.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Gupta VP, Arora AK. Automation in healthcare services. In: Research anthology on cross-disciplinary designs and applications of automation. Hershey: IGI Global Scientific Publishing; 2022. p. 285–303. doi:10.4018/978-1-6684-3694-3.ch015.
2. Suriya DS, Nivetha S. Design of UML diagrams for WEBMED-healthcare service system services. EAI Endorsed Trans E Learn. 2023;8(1):e5. doi:10.4108/eetel.v8i1.3015.
3. Peters G. Healthcare service: new ways to serve. Bus Strategy Rev. 2013;24(1):74–6. doi:10.1111/j.1467-8616.2013.00929.x.
4. Akhade GN, Jaju SB, Lakhe RR. A review on healthcare service quality dimensions. In: 2013 6th International Conference on Emerging Trends in Engineering and Technology; 2013 Dec 16–18; Nagpur, India: IEEE; 2013. p. 126–7. doi:10.1109/ICETET.2013.38.
5. Monika M, Singh A. Healthcare service quality-a review of literature. Paripex Indian J Res. 2022;143–7. doi:10.36106/paripex/6210147.
6. Mahesh PA, Manjunath TN, Saravana K. Dynamic cloud computing platform in E-healthcare system. Int J Innovat Res Inform Secur. 2023;9(3):SPJNIS10107. doi:10.26562/ijiris.2023.v0903.28.
7. Ktari J, Frikha T, Ben Amor N, Louraidh L, Elmannai H, Hamdi M. IoMT-based platform for e-health monitoring based on the blockchain. Electronics. 2022;11(15):2314. doi:10.3390/electronics11152314.
8. Liu Z, Liu C. Privacy protection method for blockchain transaction data based on homomorphic encryption and zero-knowledge proof. In: International Conference on Computer Application and Information Security (ICCAIS 2022); 2022 Dec 23–24; Online: SPIE; 55 p. doi:10.1117/12.2671850.
9. Valadares DCG, Perkusich A, Martins AF, Kamel MBM, Seline C. Privacy-preserving blockchain technologies. Sensors. 2023;23(16):7172. doi:10.3390/s23167172.
10. Bayan T, Banach R. Exploring the privacy concerns in permissionless blockchain networks and potential solutions. In: 2023 IEEE International Conference on Smart Information Systems and Technologies (SIST); 2023 May 4–6; Astana, Kazakhstan: IEEE; 2023. p. 567–72. doi:10.1109/SIST58284.2023.10223536.
11. Sutradhar S, Majumder S, Bose R, Mondal H, Bhattacharyya D. A blockchain privacy-conserving framework for secure medical data transmission in the Internet of medical things. Decis Anal J. 2024;10(2):100419. doi:10.1016/j.dajour.2024.100419.
12. Ali A, Rahim HA, Pasha MF, Dowsley R, Masud M, Ali J, et al. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics. 2021;10(16):2034. doi:10.3390/electronics10162034.
13. Tomasz H, Jerzy P, Imed EF, W M, Włodzimierz C, Marcin S. Sensitive information protection on mobile devices using general access structures. In: ICONS 2014: Proceedings of the Ninth International Conference on Systems. Nice, France: IARIA; 2014.
14. Deirmentzoglou E, Papakyriakopoulos G, Patsakis C. A survey on long-range attacks for proof of stake protocols. IEEE Access. 2019;7:28712–25. doi:10.1109/ACCESS.2019.2901858.
15. Wang Y, Sun J, Wang X, Wei Y, Wu H, Yu Z, et al. Sperax: an approach to defeat long range attacks in blockchains. In: IEEE INFOCOM, 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 2020 Jul 6–9; Toronto, ON, Canada: IEEE; 2020. p. 574–9. doi:10.1109/infocomwkshps50562.2020.9163036.

16. Karpinski M, Kovalchuk L, Kochan R, Oliynykov R, Rodinko M, Wieclaw L. Blockchain technologies: probability of double-spend attack on a proof-of-stake consensus. Sensors. 2021;21(19):6408. doi:10.3390/s21196408.
17. Amiri MJ, Agrawal D, El Abbadi A. Permissioned blockchains: properties, techniques and applications. In: Proceedings of the 2021 International Conference on Management of Data; 2021; Virtual Event, China: ACM; p. 2813–20. doi:10.1145/3448016.
18. Kim HM, Turesson H, Laskowski M, Bahreini AF. Permissionless and permissioned, technology-focused and business needs-driven: understanding the hybrid opportunity in blockchain through a case study of insolar. IEEE Trans Eng Manag. 2022;69(3):776–91. doi:10.1109/TEM.2020.3003565.
19. Bakos Y, Halaburda H. Permissioned vs permissionless blockchain platforms: tradeoffs in trust and performance. In: NYU Stern School of Business working paper; 2021. doi:10.2139/ssrn.3789425.
20. Arigela SSD, Voola P. Detecting and identifying storage issues using blockchain technology. In: 2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI); 2022 Jan 28–29; Chennai, India: IEEE; 2022. p. 1–7. doi:10.1109/ACCAI53970.2022.9752522.
21. Cao H, Cao H. Solutions to the endless addition of transaction volume in blockchain. Int J Adv Comput Sci Appl. 2022;13(6). doi:10.14569/ijacsa.2022.0130601.
22. Liu W, Zhang D, Zhao J. Ring-overlap: a storage scaling mechanism for consortium blockchain. In: 2022 International Conference on Service Science (ICSS); 2022 May 13–15; Zhuhai, China: IEEE; 2022. p. 33–40. doi:10.1109/ICSS55994.2022.00015.
23. Liu S, Yao S, Huang Y, Liu D, Shao H, Zhao Y, et al. Handling missing sensors in topology-aware IoT applications with gated graph neural network. Proc ACM Interact Mob Wearable Ubiquitous Technol. 2020;4(3):1–31. doi:10.1145/3411818.
24. Tipparaju VV, Mallires KR, Wang D, Tsow F, Xian X. Mitigating of data packet loss in Bluetooth Low Energy-based wearable healthcare ecosystem. In: Biosensors. Vol. 11, no. 10. Basel, Switzerland: MDPI; 2021. 350 p. doi:10.3390/bios11100350.
25. Chiang ML, Hsieh HC, Lin TL, Chang TP, Chen HW. Dynamic weight-based connectivity recovery in wireless sensor and actor networks. J Supercomput. 2024;80(1):734–60. doi:10.1007/s11227-023-05518-3.
26. Liu H, Yang Z, Jiang Y, Zhao W, Sun J. Enabling clone detection for Ethereum via smart contract birthmarks. In: 2019 IEEE/ACM 27th International Conference on Program Comprehension (ICPC); 2019; Montreal, QC, Canada; p. 105–15. doi:10.1109/ICPC.2019.00024.
27. Kondo M, Oliva GA, Jiang ZM, Hassan AE, Mizuno O. Code cloning in smart contracts: a case study on verified contracts from the ethereum blockchain platform. Empir Softw Eng. 2020;25(6):4617–75. doi:10.1007/s10664-020-09852-5.
28. Yuvaraj D, Anitha M, Singh B, Karyemsetty N, Krishnamoorthy R, Arun S. Systematic review of security authentication based on block chain. In: 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC); 2022 Oct 20–22; Trichy, India: IEEE; 2022. p. 768–71. doi:10.1109/ICOSEC54921.2022.9952033.
29. Kumar S, Kumar JS. Federated blockchain based highly-available healthcare system to protect the privacy and security of users. In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT); 2024 Jun 24–28; Kamand, India: IEEE; 2024. p. 1–6. doi:10.1109/ICCCNT61001.2024.10725386.
30. Richard T. Blockchain in healthcare: ensuring data security and integrity. Res Output J Public Health Med. 2024;4(2):12–7. doi:10.59298/rojphm/2024/421217.
31. Zhou B, Li H, Xu L. An authentication scheme using identity-based encryption & blockchain. In: 2018 IEEE Symposium on Computers and Communications (ISCC); 2018 Jun 25–28; Natal, Brazil: IEEE; 2018. p. 556–61. doi:10.1109/ISCC.2018.8538446.
32. Abdi AI, Eassa FE, Jambi K, Almarhabi K, AL-Ghamdi ASA. Blockchain platforms and access control classification for IoT systems. Symmetry. 2020;12(10):1663. doi:10.3390/sym12101663.
33. Hussain HA, Mansor Z, Shukur Z. Comprehensive survey and research directions on blockchain IoT access control. Int J Adv Comput Sci Applicat. 2021;12(5):239–44. doi:10.14569/IJACSA.2021.0120530.

34. Sari PK, Handayani PW, Hidayanto AN, Yazid S, Aji RF. Information security behavior in health information systems: a review of research trends and antecedent factors. Healthcare. 2022;10(12):2531. doi:10.3390/healthcare10122531.
35. Singh A, Chatterjee K. Trust based access control model for securing electronic healthcare system. J Ambient Intell Humaniz Comput. 2019;10(11):4547–65. doi:10.1007/s12652-018-1138-z.
36. Stark B, Gewald H, Lautenbacher H, Haase U, Ruff S. Misuse of 'Break-the-Glass' policies in hospitals: detecting unauthorized access to sensitive patient health data. Int J Inf Secur Priv. 2018;12(3):23. doi:10.4018/IJISP.2018070106.
37. Sadath L, Mehrotra D, Kumar A. Addressing scalability issues in blockchain: a use case from healthcare. Res Sq. 2022. doi:10.21203/rs.3.rs-1903767/v1.
38. Lipsa S, Deepti M, Anand K. Scalability in blockchain–hyperledger fabric and hierarchical model. In: 2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT); 2022; New Delhi, India; p. 1–7. doi:10.1109/GlobConPT57482.2022.9938147.
39. Tyagi S, Kathuria M. Study on blockchain scalability solutions. In: IC3-2021: Proceedings of the 2021 Thirteenth International Conference on Contemporary Computing. New York, NY, USA: ACM; 2021. p. 394–01. doi:10.1145/3474124.3474184.
40. Salim MM, Park L, Park JH. A machine learning based scalable blockchain architecture for a secure Healthcare system. In: 2022 13th International Conference on Information and Communication Technology Convergence (ICTC); 2022 Oct 19–21; Jeju Island, Republic of Korea: IEEE; 2022. p. 2231–4. doi:10.1109/ICTC55196.2022.9952962.
41. Patil SP. Design of an efficient QOS aware trust-based security model with bioinspired sidechai0s for healthcare deployments. Cana. 2024;32(3):181–96. doi:10.52783/cana.v32.1938.
42. Correia PHB, Marques MA, Simplicio MA, Ermlivitch L, Miers CC, Pillon MA. Comparative analysis of permissioned blockchains: cosmos, hyperledger fabric, quorum, and XRPL. In: 2024 IEEE International Conference on Blockchain (Blockchain); 2024 Aug 19–22; Copenhagen, Denmark: IEEE; 2024. p. 464–9. doi:10.1109/Blockchain62396.2024.00068.
43. Lin JY, Zhu LG, Chen WM, Wang WC, Gan C, Han S. On-device training under 256 KB memory. arXiv:2206.15472. 2022.
44. Shen G, Lee C. FLOMD: fast and low overhead memory deduplication for edge nodes. In: 2022 IEEE International Conference on Cloud Computing Technology and Science (CloudCom); 2022; Bangkok, Thailand; p. 83–90. doi:10.1109/cloudcom55334.2022.00022.
45. Sliwa B, Piatkowski N, Wietfeld C. LIMITS: lightweight machine learning for IoT systems with resource limitations. In: ICC, 2020-2020 IEEE International Conference on Communications (ICC); 2020 Jun 7–11; Dublin, Ireland: IEEE; 2020. p. 1–7. doi:10.1109/icc40277.2020.9149180.
46. Yu J. Fault independence in blockchain. arXiv:2306.05690. 2023.
47. Allen DWE, Lane AM, Poblet M. The governance of blockchain dispute resolution. Social science research network. Harvard Negot Law Rev. 2020;25(1):75–101. doi:10.2139/SSRN.3334674.
48. Kiayias A, Lazos P. SoK: blockchain governance. In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. New York, NY, USA: ACM; 2023. doi:10.1145/3558535.3559794.
49. Silvestri S, Islam S, Papastergiou S, Tzagkarakis C, Ciampi M. A machine learning approach for the NLP-based analysis of cyber threats and vulnerabilities of the healthcare ecosystem. Sensors. 2023;23(2):651. doi:10.3390/s23020651.
50. Drake R, Ridder E. Healthcare cybersecurity vulnerabilities. In: Proceedings of the International Conference on Cybersecurity and Cybercrime. Romania: CyberCon; 2022. p. 49–6. doi:10.19107/CYBERCON.2022.06.
51. Aly M, Khomh F, Guéhéneuc YG, Washizaki H, Yacout S. Is fragmentation a threat to the success of the Internet of Things? IEEE Internet Things J. 2019;6(1):472–87. doi:10.1109/JIOT.2018.2863180.
52. Xin X, Yang J, Wang H, Ma J, Ren P, Luo H, et al. On the user behavior leakage from recommender system exposure. ACM Trans Inf Syst. 2023;41(3):1–25. doi:10.1145/3568954.
53. Lianglu P, Shaanan C, Toby M, Van-Thuan P. Detecting excessive data exposures in web server responses with metamorphic fuzzing. arXiv:2301.09258. 2023.

54. Rosenblatt M, Link T, Jiang R, Noble S, Scheinost D. The effects of data leakage on neuroimaging predictive models. bioRxiv. 2023. doi:10.1101/2023.06.09.544383. Advance online publication.
55. Sultan I, Banday MT. Ultra-low power microcontroller architectures for the Internet of Things (IoT) devices. In: 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT); 2023 Jan 23-25; Tirunelveli, India: IEEE; 2023. p. 482–8. doi:10.1109/icssit55814.2023.10060949.
56. Martin Wisniewski L, Bec JM, Boguszewski G, Gamatié A. Hardware solutions for low-power smart edge computing. J Low Power Electron Appl. 2022;12(4):61. doi:10.3390/jlpea12040061.
57. Thakur G, Sohal H, Jain S. Low-power approximate arithmetic circuits for IoT devices. Recent Adv Electr Electron Eng Former Recent Pat Electr Electron Eng. 2022;15(5):421–8. doi:10.2174/2352096515666220627124337.
58. Hajian R, Haghighat A, Erfani SH. A secure anonymous D2D mutual authentication and key agreement protocol for IoT. Internet Things. 2022;18(3):100493. doi:10.1016/j.iot.2021.100493.
59. Rizzardi A, Sicari S, Coen-Porisini A. Analysis on functionalities and security features of Internet of Things related protocols. Wirel Netw. 2022;28(7):2857–87. doi:10.1007/s11276-022-02999-7.
60. Nair KK, Nair HD, Krishnan K. Security considerations in the internet of things protocol stack. In: 2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD); 2021; Durban, South Africa; 2021. p. 1–6. doi:10.1109/ICABCD51485.2021.9519377.
61. Taherdoost H. Privacy and security of blockchain in healthcare: applications, challenges, and future perspectives. Sci. 2023;5(4):41. doi:10.3390/sci5040041.
62. Raghav N, Bhola AK. Secured framework for privacy preserving healthcare based on blockchain. In: 2022 International Conference on Computer Communication and Informatics (ICCCI); 2022 Jan 25–27; Coimbatore, India: IEEE; 2022. p. 1–5. doi:10.1109/ICCCI54379.2022.9763091.
63. Sivasangari A, Sonti VJKK, Poonguzhali S, Deepa D, Anandhi T. Security framework for enhancing security and privacy in healthcare data using blockchain technology. In: International Conference on Innovative Computing and Communications; 2021; Singapore: Springer Singapore. p. 143–58. doi:10.1007/978-981-16-2594-7_12.
64. Rani S, Kataria A, Kumar S, Tiwari P. Federated learning for secure IoMT-applications in smart healthcare systems: a comprehensive review. Knowl Based Syst. 2023;274:110658. doi:10.1016/j.knosys.2023.110658.
65. Amreen G, Kanavalli A. Privacy pinnacle: improvising healthcare data security through federated learning and blockchain framework. In: 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT); 2024 Jun 24–28; Kamand, India: IEEE; 2024. p. 1–8. doi:10.1109/ICCCNT61001.2024.10724371.
66. Myrzashova R, Alsamhi SH, Shvetsov AV, Hawbani A, Wei X. Blockchain meets federated learning in healthcare: a systematic review with challenges and opportunities. IEEE Internet Things J. 2023;10(16):14418–37. doi:10.1109/JIOT.2023.3263598.
67. Abbas A, Alroobaea R, Krichen M, Rubaiee S, Vimal S, Almansour FM. Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. Pers Ubiquitous Comput. 2024;28(1):59–72. doi:10.1007/s00779-021-01583-8.
68. Geetha V, Balakrishnan B. A user authentication and access control scheme for IoT-based healthcare using blockchain. In: 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT); 2021 Jul 6–8; Kharagpur, India: IEEE; 2021. p. 1–7.
69. Islam A, Uddin MB, Kader MF, Shin SY. Blockchain based secure data handover scheme in non-orthogonal multiple access. In: 2018 4th International Conference on Wireless and Telematics (ICWT); 2018 Jul 12–13; Nusa Dua, Bali, Indonesia: IEEE; 2018. p. 1–5. doi:10.1109/ICWT.2018.8527732.
70. Rouhani S, Deters R. Blockchain based access control systems: state of the art and challenges. In: IEEE/WIC/ACM International Conference on Web Intelligence; 2019; Thessaloniki Greece: ACM. p. 423–8. doi:10.1145/3350546.3352561.
71. Uma Maheswari G, A S, Rajeshkumar C, Vargheese M, Nallasivan G, Selvarani JH. Multimedia wireless sensor network platform Data encryption algorithm based on blockchain technology. In: Proceedings of the 2nd International Conference on Networking and Communications (ICNWC 2024). Chennai, India: IEEE; 2024. p. 1–7. doi:10.1109/ICNWC60771.2024.10537414.

72. [cited 2021 Jul 5]. Available from: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far.
73. Das D, Banerjee S, Chakraborty R, Dasgupta K, Chatterjee P, Ghosh U. A blockchain-based security management framework for cyber-physical systems. In: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW); 2023 May 1–4; Bangalore, India: IEEE; 2023. p. 39–44. doi:10.1109/CCGridW59191.2023.00021.
74. Okikiola FM, Mustapha AM, Akinsola AF, Sokunbi MA. A new framework for detecting insider attacks in cloud-based E-health care system. In: 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS); 2020 Mar 18–21; Ayobo, Ipaja, Lagos, Nigeria: IEEE. p. 1–6. doi:10.1109/icmcecs47690.2020.240889.
75. Ekparinya P, Gramoli V, Jourjon G. The attack of the clones against proof-of-authority. 2019. doi:10.48550/arXiv.1902.10244.
76. Anitha S, Jayanthi P, Chandrasekaran V. An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks. Measurement. 2021;167(3):108272. doi:10.1016/j.measurement.2020.108272.
77. Chen H, Ai X, Lin K, Yan N, Wang Z, Jiang N, et al. DAP: efficient detection against probabilistic cloning attacks in anonymous RFID systems. IEEE Trans Ind Inform. 2022;18(1):345–55. doi:10.1109/TII.2021.3072929.
78. Ai X, Chen H, Lin K, Wang Z, Yu J. Nowhere to hide: efficiently identifying probabilistic cloning attacks in large-scale RFID systems. IEEE Trans Inf Forensics Secur. 2020;16:714–27. doi:10.1109/TIFS.2020.3023785.
79. Bu K, Xu M, Liu X, Luo J, Zhang S, Weng M. Deterministic detection of cloning attacks for anonymous RFID systems. IEEE Trans Ind Inform. 2015;11(6):1255–66. doi:10.1109/TII.2015.2482921.
80. Thaile M, Ramanaiah OBV. Node compromise detection based on NodeTrust in wireless sensor networks. In: 2016 International Conference on Computer Communication and Informatics (ICCCI); 2016 Jan 7–9; Coimbatore, India: IEEE; 2016. p. 1–5. doi:10.1109/ICCCI.2016.7480020.
81. Yang Y, Wang X, Zhu S, Cao G. Distributed software-based attestation for node compromise detection in sensor networks. In: 2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007); 2007 Oct 10–12; Beijing, China: IEEE; 2007. p. 219–30. doi:10.1109/SRDS.2007.31.
82. Conchon S. Some insights on open problems in blockchains: explorative tracks for tezos (Invited Talk). In: 5th International Symposium on Foundations and Applications of Blockchain 2022 (FAB 2022); Schloss Dagstuhl–Leibniz-Zentrum für Informatik: Open Access Series in Informatics (OASIcs); 2021. Vol. 101, p. 2:1. doi:10.4230/OASIcs.FAB.2022.2.
83. Wang C, Raviv N. Breaking blockchain's communication barrier with coded computation. In: 2022 IEEE Information Theory Workshop (ITW); 2022 Nov 1–9; Mumbai, India: IEEE; 2022. p. 744–9. doi:10.1109/ITW54588.2022.9965835.
84. A.L.Hamad NF, Liou JC. Current cybersecurity challenges of applying blockchain in healthcare. In: 2022 International Conference on Computational Science and Computational Intelligence (CSCI); 2022 Dec 14–16; Las Vegas, NV, USA: IEEE; 2022. p. 1719–24. doi:10.1109/CSCI58124.2022.00305.
85. Li Z, Lei W, Hu H, Zhang W. A blockchain-based communication non-repudiation system for conversational service. In: 2019 IEEE 13th International Conference on Anti-Counterfeiting, Security, and Identification (ASID); 2019 Oct 25–27; Xiamen, China: IEEE; 2019. p. 6–10. doi:10.1109/ICASID.2019.8924991.
86. Hernandez-Ardieta JL, Gonzalez-Tablas AI, de Fuentes JM, Ramos B. A taxonomy and survey of attacks on digital signatures. Comput Secur. 2013;34:67–112. doi:10.1016/j.cose.2012.11.009.
87. Ou CM, Ou CR. Adaptation of agent-based non-repudiation protocol to mobile digital right management (DRM). Expert Syst Appl. 2011;38(9):11048–54. doi:10.1016/j.eswa.2011.02.149.
88. Grosu GM, Nistor SE, Simion E. A note on blockchain authentication methods for mobile devices in healthcare. Rom Cyber Secur J. 2022;4(1):77–85. doi:10.54851/v4i1y202209.
89. Khan MA, Din IU, Majali T, Kim BS. A survey of authentication in Internet of Things-enabled healthcare systems. Sensors. 2022;22(23):9089. doi:10.3390/s22239089.

90. Wei D, Gu Y, Du Y. Mobile device fingerprinting recognition using insensitive information. In: 2022 International Conference on Image Processing, Computer Vision and Machine Learning (ICICML); 2022 Oct 28–30; Xi'an, China: IEEE; 2022. p. 1–6. doi:10.1109/ICICML57342.2022.10009697.
91. Ruiz M, Comellas J, Velasco L. Man-in-the-middle attacks through re-shaping I-Q optical constellations. In: 2023 Optical Fiber Communications Conference and Exhibition (OFC); 2023 Mar 5–9; San Diego, CA, USA: IEEE; 2023. p. 1–3. doi:10.23919/ofc49934.2023.10116394.
92. Osipova EV, Butakova NG. Development of a secure messenger based on the ECMQV algorithm, immune to man-in-the-middle attacks. In: 2024 Conference of Young Researchers in Electrical and Electronic Engineering (ElCon); 2024 Jan 29–31; Saint Petersburg, Russian Federation: IEEE; 2024. p. 264–7. doi:10.1109/ElCon61730.2024.10468485.
93. Thankappan M, Rifà-Pous H, Garrigues C. Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: a state of the art review. Expert Syst Appl. 2022;210(3):118401. doi:10.1016/j.eswa.2022.118401.
94. Ilyas B, Kumar A, Ali Setitra M, Bensalem ZA, Lei H. Prevention of DDoS attacks using an optimized deep learning approach in blockchain technology. Trans Emerging Tel Tech. 2023;34(4):e4729. doi:10.1002/ett.4729.
95. Alam MR, Khan SI, Chowa SBZ, Chowdhury AH, Kabir SR, Sadeq MJ. Use of blockchain to prevent distributed denial-of-service (DDoS) attack: a systematic literature review. In: Chinara S, Tripathy AK, Li KC, Sahoo JP, Mishra AK, editors. Advances in distributed computing and machine learning. lecture notes in networks and systems. Vol. 660. Singapore: Springer; 2023. doi:10.1007/978-981-99-1203-2_4.
96. Aljanabi YI, Majeed AA, Jihad KH, Qader BA. Detect and mitigate blockchain-based DDoS attacks using machine learning and smart contracts. Informatica. 2022;46(7). doi:10.31449/inf.v46i7.4033.
97. Ibrahim RF, Abu Al-Haija Q, Ahmad A. DDoS attack prevention for Internet of thing devices using ethereum blockchain technology. Sensors. 2022;22(18):6806. doi:10.3390/s22186806.
98. Čulić Gambiroža J, Mastelić T, Nižetić Kosović I, Čagalj M. Lost in data: recognizing type of time series sensor data using signal pattern classification. Int J Data Sci Anal. 2023;40(2):193. doi:10.1007/s41060-023-00413-9.
99. Luizzo A, Scaglione B. Healthcare security: solutions for management, operations, and administration. 1st ed. New York: Productivity Press; 2022. doi:10.4324/9781003215851.
100. Buterin V, Illum J, Nadler M, Schär F, Soleimani A. Blockchain privacy and regulatory compliance: towards a practical equilibrium. Blockchain Res Appl. 2024;5(1):100176. doi:10.1016/j.bcra.2023.100176.
101. Kioskli K, Fotis T, Mouratidis H. The landscape of cybersecurity vulnerabilities and challenges in healthcare: security standards and paradigm shift recommendations. In: Proceedings of the 16th International Conference on Availability, Reliability and Security; 2021; Vienna, Austria: ACM; p. 1–9. doi:10.1145/3465481.3470033.
102. Kuaban GS, Gelenbe E, Czachórski T, Czekalski P, Tangka JK. Modelling of the energy depletion process and battery depletion attacks for battery-powered Internet of Things (IoT) devices. Sensors. 2023;23(13):6183. doi:10.3390/s23136183.
103. Khalid A, Sakthivel U, Thangamuthu S, Drieberg M, Sebastian P, Abd Aziz A, et al. Extended lifetime of IoT applications using energy saving schemes. In: 2022 International Conference on Future Trends in Smart Communities (ICFTSC); 2022; Kuching, Sarawak, Malaysia; 2022. p. 93–7. doi:10.1109/ICFTSC57269.2022.10040064.
104. Dhivya M, Rajesh G, Gurulakshmi AB, Puvirajan, Sharma S. Design and analysis of power optimization in Internet of Things using RFID based energy harvesting mechanism. In: 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP); 2022 Dec 23–24; Bengaluru, India: IEEE; 2022. p. 1–5. doi:10.1109/CCIP57447.2022.10058640.
105. Sudharshan KM, Bhavya AR. Hardware and software method to reduce power consumption in battery operated IoT devices. In: 2022 IEEE Fourth International Conference on Advances in Electronics, Computers and Communications (ICAECC); 2022 Jan 10–11; Bengaluru, India: IEEE; 2022. p. 1–4. doi:10.1109/ICAECC54045.2022.9716644.
106. Li T. Mitigate long-lasting ethical issues in the healthcare industry with blockchain-based solutions. Highlights Sci Eng Technol. 2023;39:779–83. doi:10.54097/hset.v39i.6644.
107. Tournier J, Lesueur F, Le Mouël F, Guyon L, Ben-Hassine H. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. Internet Things. 2021;16(4):100264. doi:10.1016/j.iot.2020.100264.

108. Baz A, Ahmed R, Khan SA, Kumar S. Security risk assessment framework for the healthcare Industry 5.0. Sustainability. 2023;15(23):16519. doi:10.3390/su152316519.
109. Attia O, Khoufi I, Laouiti A, Adjih C. An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 2019 Jun 24–26; Canary Islands, Spain: IEEE; 2019. p. 1–5. doi:10.1109/ntms.2019.8763849.
110. Shetty NP, Muniyal B, Priyanshu A, Kumar D, Melroy Maben L, Agrawal Y, et al. Protecting your online Persona: a preferential selective encryption approach for enhanced privacy in tweets, images, memes, and metadata. IEEE Access. 2024;12(18):86403–24. doi:10.1109/ACCESS.2024.3415663.
111. HIPPA. [cited 2021 Jul 5]. Available from: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.
112. GDPR. [cited 2021 Jul 5]. Available from: https://gdpr-info.eu/.
113. Yaqoob T, Abbas H, Atiquzzaman M. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review. IEEE Commun Surv Tutor. 2019;21(4):3723–68. doi:10.1109/COMST.2019.2914094.
114. Zaman U, Imran, Mehmood F, Iqbal N, Kim J, Ibrahim M. Towards secure and intelligent Internet of health things: a survey of enabling technologies and applications. Electronics. 2022;11(12):1893. doi:10.3390/electronics11121893.
115. Lee M-H, Liu I-H, Huang H-C, Li J-S. Cyber security in a 5G-based smart healthcare network: a base station case study. In: Engineering Proceedings. Vol. 55. Basel, Switzerland: MDPI; 2023. 50 p. doi:10.3390/engproc2023055050.
116. Dang LM, Piran MJ, Han D, Min K, Moon H. A survey on Internet of Things and cloud computing for healthcare. Electronics. 2019;8(7):768. doi:10.3390/electronics8070768.
117. Chen CY, Hsu YC, Lin CC, Hajiyev J, Su CR, Tseng CH. Study of out-of-hospital access to HIS system: a security perspective. Sensors. 2019;19(11):2628. doi:10.3390/s19112628.
118. Ali TE, Ali FI, Dakić P, Zoltan AD. Trends, prospects, challenges, and security in the healthcare Internet of Things. Computing. 2024;107(1):28. doi:10.1007/s00607-024-01352-4.
119. Mukati A. Blockchain technology in healthcare services. Master of cyber law and information security, national law institute university, Bhopal (M.P), India. Int J Comput Netw Commun (IJCNC). 2023;3(1):9–15. doi:10.54105/ijcns.D4090.053123.
120. Galaba A, Palagani M, Vinukonda R, Sai Pavan Malampati J, Sri Harsha S, Kiran KVD. Significance of blockchain technology in the healthcare sector. In: 2023 International Conference on Inventive Computation Technologies (ICICT). Lalitpur, Nepal; 2023. p. 1159–65. doi:10.1109/ICICT57646.2023.10134196.
121. Kumar A, Goswami VS. Blockchain technology in healthcare. In: Kaiser MS, Xie J, Rathore VS, editors. Information and communication technology for competitive strategies (ICTCS 2022). Lecture notes in networks and systems. Vol. 615. Singapore: Springer; 2023. doi:10.1007/978-981-19-9304-6_45.
122. Swati S, Kumar M. E-Healthcare record management using blockchain technology. In: Blockchain technology in e-healthcare management. London, UK: Institution of Engineering and Technology (IET); 2023. p. 31–58. doi:10.1049/pbhe048e_ch2.
123. Kamble J, Kumar R, Chandana S, Koushik MS, Rao GRK, Vignesh T. Application of blockchain technology in the healthcare system. In: 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS); 2023 Mar 23–25; Erode, India. IEEE; 2023. p. 1272–6. doi:10.1109/ICSCDS56580.2023.10104737.
124. Gupta M, Singh M, Sharma A, Sukhija N, Aggarwal PK, Jain P. Unification of machine learning and blockchain technology in healthcare industry. In: Innovations in healthcare informatics: from interoperability to data analysis. London, UK: Institution of Engineering and Technology (IET); 2023. p. 185–206. doi:10.1049/pbhe041e_ch6.
125. Abbate S, Centobelli P, Cerchione R, Oropallo E, Riccio E. Blockchain technology for embracing Healthcare 4.0. IEEE Trans Eng Manag. 2023;70(8):2998–3009. doi:10.1109/TEM.2022.3212007.
126. Singhal R, Jain V,Raj D. E-health transforming healthcare delivery with AI, blockchain, and cloud. In: Lytras MD, Alkhaldi AN, Ordóñez de Pablos P, editors. Harnessing AI, blockchain, and cloud computing for enhanced e-government services. Hershey, PA: IGI Global; 2025. p. 475–10. doi:10.4018/979-8-3693-7678-2.ch015.

127. Shi J. Blockchain technology in renovating healthcare. In: Kaushik K, Dahiya S, Dwivedi A, editors. Revolutionizing healthcare through artificial intelligence and internet of things applications. Hershey: IGI Global; 2023. p. 177–86. doi:10.4018/978-1-6684-5422-0.ch012.
128. Qose S, Rajnai Z, Fregan B. Blockchain technology in healthcare industry: benefits and issues. In: 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI); 2023 May 23–26; Timisoara, Romania. IEEE; 2023. p. 171–6. doi:10.1109/SACI58269.2023.10158669.
129. Chauhan S, Singh Tanwar HK. Application of blockchain technology in healthcare: a systematic review. In: 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC); 2022 May 9–11; Salem, India. IEEE; 2022. p. 1–5. doi:10.1109/ICAAIC53929.2022.9792750.
130. Bernardo Tello A, Xing J, Lalitkumar Patil DA, Premchandra Patil DL, Sayyad DS. Blockchain technologies in healthcare system for real time applications using IoT and deep learning techniques. Int J Commun Netw Inf Secur. 2022;14(3):257–68. doi:10.17762/ijcnis.v14i3.5621.
131. Shaikh ZA, Memon AA, Shaikh AM, Soomro S, Sayed M. Blockchain in healthcare: unlocking the potential of blockchain for secure and efficient applications for medical data management-a presentation of basic concepts. Liaquat Med Res J. 2023;5(2). doi:10.38106/LMRJ.2023.5.2-08.
132. mamun Aal, Jalil MS, Mehedy MTJ, Saeed M, Snigdha EZ, khan MN, et al. Optimizing revenue cycle management in healthcare: AI and IT solutions for business process automation. Am J Eng Technol. 2025;7(3):141–62. doi:10.37547/tajet/Volume07Issue03-14.
133. Faderin E, Oginni OG, Alade B. Telehealth innovations for cardiovascular disease management. World J Adv Res Rev. 2024;24(1):518–36. doi:10.30574/wjarr.2024.24.1.3085.
134. Bhawke PP. Multiple disease prediction using different machine learning algorithms comparatively. Int J Sci Res Eng Manag. 2023;7(9). doi:10.55041/IJSREM25681.
135. Andrew J, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: architecture, security challenges, trends and future directions. J Netw Comput Appl. 2023;215(21):103633. doi:10.1016/j.jnca.2023.103633.
136. Hwang J, Yoo J. A memory-efficient transmission scheme for multi-homed Internet-of-things (IoT) devices. Sensors. 2020;20(5):1436. doi:10.3390/s20051436.
137. Banerjee J, Islam S, Wei W, Pan C, Zhu D, Xie M. Memory-aware efficient deep learning mechanism for IoT devices. In: 2021 IEEE 32nd International Conference on Application-Specific Systems, Architectures and Processors (ASAP); NJ, USA; 2021. p. 187–94. doi:10.1109/ASAP52443.2021.00035.
138. He L, Ding L, Dai Y, Ning S. Smart system for elderly care based on portable sensor positioning and video surveillance. In: 2024 Second International Conference on Inventive Computing and Informatics (ICICI); 2024 Jun 11–12; Bangalore, India. IEEE; 2024. p. 330–5. doi:10.1109/ICICI62254.2024.00061.
139. Chodankar D, Raval TK, Jeyaraj J. The role of remote data capture, wearables, and digital biomarkers in decentralized clinical trials. Perspect Clin Res. 2024;15(1):38–41. doi:10.4103/picr.picr_219_22.
140. Gourisaria MK, Agrawal R, Singh V, Rautaray SS, Pandey M. AI and IoT enabled smart hospital management systems. In: Rautaray SS, Pandey M, Nguyen NG, editors. Data science in societal applications. Studies in big data. Vol. 114. Singapore: Springer; 2022. doi:10.1007/978-981-19-5154-1_6.
141. Rukundo SK. The impact of wearable technology on health monitoring. Res Invent J Public Health Pharm. 2024;3(2):5–8. doi:10.59298/RIJPP/2024/325800.
142. Hilal AR. Real-time data management in ubiquitous wearable networks. In: 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC); 2017 Oct 5–8; Banff, AB, Canada. IEEE; 2017. p. 3523–8. doi:10.1109/SMC.2017.8123177.
143. Qian L, Gu K, Fu Y, Shen Y, Xu S. A wireless ad hoc network communication platform and data transmission strategies for multi-bus instruments. In: Electronics. Vol. 13, no. 18. Basel, Switzerland: MDPI; 2024. 3596 p. doi:10.3390/electronics13183596.
144. Abouhogail RA. Security assessment for key management in mobile ad hoc networks. Int J Secur Appl. 2014;8(1):169–82. doi:10.14257/ijsia.2014.8.1.16.

145. Shin J, Cho Y, Kim YJ. Wearable apparatus, management server, management system having the same, and method for controlling thereof. U.S. Patent 10,764,733[P]; 2020 Sep 1. Available from: https://patents.google.com/patent/WO2016105135A1/en.
146. Sharma I, Sharma S. Blockchain enabled biometric security in intemet-of-medical-things (IoMT) devices. In: 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS); 2022 Nov 24–26; Trichy, India. IEEE; 2022. p. 971–9. doi:10.1109/ICAISS55157.2022.10010716.
147. Zhuang Z, Lee X, Wei J, Fu Y, Zhang A. CBCMS: a compliance management system for cross-border data transfer. In: 2024 IEEE International Conference on Big Data (BigData); 2024 Dec 15–18; Washington, DC, USA: IEEE; 2024. p. 4789–98. doi:10.1109/BigData62323.2024.10826075.
148. Villarreal ERD, García-Alonso J, Moguel E, Alegría JAH. Blockchain for healthcare management systems: a survey on interoperability and security. IEEE Access. 2023;11(2):5629–52. doi:10.1109/ACCESS.2023.3236505.
149. Latorre F, Hawks CE, Colmenares B, Verma D, Gil M, Sala N. Patient-centric interoperability and cybersecurity for cross-border healthcare. Stud Health Technol Inform. 2023;305:204–7. doi:10.3233/SHTI230463.
150. Gans JS, Holden R. A solomonic solution to blockchain front-running. AEA Pap Proc. 2023;113(3):248–52. doi:10.1257/pandp.20231029.
151. Sarkar A, Maitra T, Neogy S. Blockchain in healthcare system: security issues, attacks and challenges. In: Blockchain technology: applications and challenges. Cham: Springer International Publishing; 2021. p. 113–33. doi:10.1007/978-3-030-69395-4_7.
152. Kumar A, Chatterjee K. Blockchain-enabled data sharing framework for intelligent healthcare system. In: Proceedings of the Evolution in Computational Intelligence. Singapore: Springer Nature Singapore; 2023. p. 357–67. doi:10.1007/978-981-19-7513-4_32.
153. Wang Y, Tan M. Defense against sybil attack in blockchain based on improved consensus algorithm. In: 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT); 2023 Apr 28–30; Jilin, China. IEEE; 2023. p. 986–9. doi:10.1109/ICCECT57938.2023.10140278.
154. Platt M, McBurney P. Sybil in the haystack: a comprehensive review of blockchain consensus mechanisms in search of strong sybil attack resistance. Algorithms. 2023;16(1):34. doi:10.3390/a16010034.
155. Cai Y, Fragkos G, Tsiropoulou EE, Veneris A. A truth-inducing sybil resistant decentralized blockchain oracle. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS); 2020 Sep 28–30; Paris, France: IEEE; 2020. p. 128–35. doi:10.1109/brains49436.2020.9223272.
156. Gupta D, Saia J, Young M. Bankrupting Sybil despite churn. J Comput Syst Sci. 2023;135(10):89–124. doi:10.1016/j.jcss.2023.02.004.
157. Huang J, Lei K, Du M, Zhao H, Liu H, Liu J, et al. Survey on the blockchain incentive mechanism. In: Wang G, Li J, Zhang X, Hong X, Tian G, editors. Advances in computer science and information technology. Springer; 2019. p. 416–29. doi: 10.1007/978-981-15-0118-0_30.
158. Wang Z, Hu Q, Li R, Xu M, Xiong Z. Incentive mechanism design for joint resource allocation in blockchain-based federated learning. IEEE Trans Parallel Distrib Syst. 2023;34(5):1536–47. doi:10.1109/TPDS.2023.3253604.
159. Kumar A, Kumar Sah B, Mehrotra T, Rajput GK. A review on double spending problem in blockchain. In: 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES); 2023 Apr 28–30; Greater Noida, India: IEEE; 2023. p. 881–9. doi:10.1109/CISES58720.2023.10183579.
160. Zulfiqorov NT. A novel layered GSP incentive mechanism for federated learning combined with blockchain. In: Arai K, Bhatia R, Kapoor S, editors. Advances in information and communication. Springer; 2022. p. 455–66. doi:10.1007/978-981-19-4775-9_38.
161. Hemati M, Shajari M. Analysis of incentive mechanism in repchain. In: 2021 26th International Computer Conference, Computer Society of Iran (CSICC); 2021 Mar 3–4; Tehran, Iran. IEEE; 2021. p. 1–5. doi:10.1109/CSICC52343.2021.9420606.
162. Dai Q, Zhang B, Dong S. Eclipse attack detection for blockchain network layer based on deep feature extraction. Wirel Commun Mob Comput. 2022;2022(1):1451813. doi:10.1155/2022/1451813.

163. Alangot B, Reijsbergen D, Venugopalan S, Szalachowski P, Yeo KS. Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains. IEEE Trans Netw Serv Manag. 2021;18(2):1659–72. doi:10.1109/TNSM.2021.3069502.
164. Mai T, Yao H, Zhang N, Xu L, Guizani M, Guo S. Cloud mining pool aided blockchain-enabled Internet of Things: an evolutionary game approach. IEEE Trans Cloud Comput. 2023;11(1):692–703. doi:10.1109/TCC.2021.3110965.
165. Ai Z, Liu Y, Wang X. ABC: an auction-based blockchain consensus-incentive mechanism. In: 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS); 2020 Dec 2–4; Hong Kong, China. IEEE; 2020. p. 609–16. doi:10.1109/icpads51040.2020.00085.
166. Nawab F, Sadoghi M. Consensus in data management: from distributed commit to blockchain. FNT Databases. 2023;12(4):221–364. doi:10.1561/1900000075.
167. Chen L, Xu L, Xu S, Gao Z, Shi W. Election with bribe-effect uncertainty: a dichotomy result. In: Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence; 2019 Aug 10–16; Macao, China: International Joint Conferences on Artificial Intelligence Organization; 2019. p. 158–64. doi:10.24963/ijcai.2019/23.
168. Cong LW, He Z, Li J. Decentralized mining in centralized pools. Rev Financ Stud. 2021;34(3):1191–235. doi:10.1093/rfs/hhaa040.
169. Liu J, Guo S, Shi Y, Feng L, Wang C. Decentralized caching framework toward edge network based on blockchain. IEEE Internet Things J. 2020;7(9):9158–74. doi:10.1109/JIOT.2020.3003700.
170. Saxena S, Pandey A, Kumar S. A multistage RSSI-based scheme for node compromise detection in IoT networks. In: 2019 IEEE 16th India Council International Conference (INDICON); 2019 Dec 13–15; Rajkot, India. IEEE; 2019. p. 1–4. doi:10.1109/indicon47234.2019.9029092.
171. Ruvunangiza J, Valderrama C. A unified framework for secure healthcare data sharing: integrating federated learning, blockchain, and quantum cryptography. J Biomed Res Environ Sci. 2024;5(9):1081–8. doi:10.37871/jbres1993.
172. Shaikh N, Kasar S. Blockchain approaches for healthcare: a review and outlook. In: 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC); 2024 Aug 7–9; Coimbatore, India. IEEE; 2024. p. 777–84. doi:10.1109/ICESC60852.2024.10689951.
173. Jain M, Pandey D, Singh NP. EHR: patient electronic health records using blockchain security framework. In: 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA). Uttarakhand, India; 2023. p. 710–5. doi:10.1109/ICIDCA56705.2023.10099789.
174. Wang B, Zhang Y, Niu B. Blockchain data transaction with leakage tracing based on digital fingerprint. In: 2022 IEEE 28th International Conference on Parallel and Distributed Systems (ICPADS); 2023 Jan 10–12; Nanjing, China. IEEE; 2023. p. 266–73. doi:10.1109/ICPADS56603.2022.00042.
175. Akbar NA, Muneer A, ElHakim N, Fati SM. Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses. Future Internet. 2021;13(11):285. doi:10.3390/fi13110285.
176. Rani K, Sharma C. Tampering detection of distributed databases using blockchain technology. In: 2019 Twelfth International Conference on Contemporary Computing (IC3); 2019 Aug 8–10; Noida, India. IEEE; 2019. p. 1–4. doi:10.1109/ic3.2019.8844938.
177. Jang J, Lee HN. Profitable double-spending attacks. Appl Sci. 2020;10(23):8477. doi:10.3390/app10238477.
178. Gorvunova V, Kukhtevich I, Goryunova T. Digitalization and integration cloud solutions for healthcare information systems. In: Proceedings of the 2022 4th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency (SUMMA). Lipetsk, Russian Federation: IEEE; 2022. p. 608–11. doi:10.1109/SUMMA57301.2022.9973961.
179. Natraj NA, Mitra S, Hallur GG. An investigative study on internet of things in healthcare. In: Proceedings of the Handbook of research on machine learning-enabled IoT for smart applications across industries. Hershey: IGI Global; 2023. p. 116–26. doi:10.4018/978-1-6684-8785-3.ch006.
180. Al-Nbhany WANA, Zahary AT, Al-Shargabi AA. Blockchain-IoT healthcare applications and trends: a review. IEEE Access. 2024;12(3):4178–212. doi:10.1109/ACCESS.2023.3349187.

181. Hossain Faruk MJ, Shahriar H, Valero M, Sneha S, Ahamed SI, Rahman M. Towards blockchain-based secure data management for remote patient monitoring. In: 2021 IEEE International Conference on Digital Health (ICDH); 2021 Sep 5–10; Chicago, IL, USA: IEEE; 2021. p. 299–308. doi:10.1109/icdh52753.2021.00054.
182. Koutras D, Stergiopoulos G, Dasaklis T, Kotzanikolaou P, Glynos D, Douligeris C. Security in IoMT communications: a survey. Sensors. 2020;20(17):4828. doi:10.3390/s20174828.
183. Adeghe EP, Okolo CA, Ojeyinka OT. Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. Open Access Res J Sci Technol. 2024;10(2):13–20.
184. Al-Shareeda MA, Manickam S, Laghari SA, Jaisan A. Replay-attack detection and prevention mechanism in industry 4.0 landscape for secure SECS/GEM communications. Sustainability. 2022;14(23):15900. doi:10.3390/su142315900.
185. Surridge M, Meacham K, Papay J, Phillips SC, Pickering JB, Shafiee A, et al. Modelling compliance threats and security analysis of cross border health data exchange. In: New trends in model and data engineering. Cham: Springer International Publishing; 2019. p. 180–9. doi:10.1007/978-3-030-32213-7_14.
186. Ma X, Yu D, Du Y, Li L, Ni W, Lv H. A blockchain-based incentive mechanism for sharing cyber threat intelligence. Electronics. 2023;12(11):2454. doi:10.3390/electronics12112454.
187. Selvarajan S, Manickam S, Manoharan H, Laghari SUA, Uddin M, Abdelhaq M, et al. Testing and substantiation of zero trust devices with blockchain procedures for secured data transfer approach. Hum Centric Comput Inf Sci. 2024;14:1–16. doi:10.22967/HCIS.2024.14.042.